HOW MUCH DEAD-HAND CONTROL IS TOO MUCH? WHY BIOMETRIC DATA PRIVACY LAWS NEED EXPANDING

Gavin Elliott[*]

Biometric data privacy laws are meant to prevent certain harms envisioned by the legislature in the drafting process. The state legislatures that have passed and are currently drafting these laws consider their constituencies' discomfort with unforeseen downstream consequences of biometric data collection by companies and the potential for repeated fraud due to the immutability of biometric identifiers. In response to their constituencies' concerns, legislatures have passed laws that protect biometric identifiers in these two contexts.

This legislation stops short of its intended purpose by not extending the same protections to the deceased. This gap leaves the deceased vulnerable to cybercriminals and unintended downstream consequences alike. However, this Comment argues the right of control and right to private action created in biometric privacy legislation creates a property interest in biometric identifiers bringing this within the realm of estate planning. Estate planners in the states that have enacted biometric privacy legislation can protect the decedent's privacy while managing the risk of post-mortem fraud.

---

* J.D. Candidate, Texas Tech University School of Law, 2024; Bachelor of Science in Business Administration, University of Tulsa, 2021. I would like to thank Miguel Escobar for his guidance and perspective, Christine Vanderwater for her editorial guidance, and my friends and family for their constant encouragement and support thoughout the research and writing process.

I. WHAT ARE BIOMETRIC IDENTIFIERS AND WHY SHOULD WE CARE?

Any human characteristic that can be measured can be a biometric identifier.[1] The most recognizable biometric identifiers are physical identifiers and include fingerprints and facial structures.[2] Every person has these features, but every person's fingerprints and facial structure are unique to that person.[3] The second biometric identifier discussed in this comment is the behavioral identifier.[4] These identifiers measure characteristics like unconscious gestures or reactions to external stimuli.[5] A person's gait or how they react to a certain image is just as unique as that person's fingerprint.[6]

Physical biometric identifiers are most often used to replace user-generated passwords.[7] These characteristics are hard to replicate and provide an easy method to secure devices and accounts.[8] These characteristics are immutable and unique, but if a cybercriminal or identity thief were to acquire an individual's fingerprint or facial geometry, they would have access to all the devices and accounts that identifier secured.[9] The immutability of biometric identifiers exposes the individuals who employ them to secure their private information to repeated instances of fraud.[10]

These biometric identifiers are measures of inherently private information.[11] The technology utilizing these identifiers continues to advance, and as new applications are found for both behavioral and physical biometric identifiers, consumer concerns must be carefully considered.[12] There are only a few states with regulations for biometric identifiers in place.[13] Moving forward, regulations for this intersection between individual privacy and security should balance the individual's privacy concerns with the corporation's need for security.[14]

---

1. *Biometrics: definition, use cases, latest news,* THALES (Jan. 27, 2022), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics [https://perma.cc/BEX6-PBCD].
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. Maria Korolov, *What is biometrics? 10 physical and behavioral identifiers that can be used for authentication*, CSO (Feb. 12, 2019), https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html [https://perma.cc/M5QS-4ECV].
8. *Id.*
9. *Id.*
10. *Id.*
11. *Id.*
12. *See id.*
13. Molly DiRago et al., *A Fresh "Face" of Privacy: 2022 Biometric Laws*, JD SUPRA (Apr. 6, 2022), https://www.jdsupra.com/legalnews/a-fresh-face-of-privacy-2022-biometric-3041578/ [https://perma.cc/3RYE-SKZN].
14. *See* Korolov, *supra* note 7.

A. Biometric Identifiers in Pop-culture

Season two of the show Black Mirror starts with an episode called "Be Right Back," which involves the different ways people deal with grief with an underlying theme of techno-paranoia.[15] Within the first few minutes of the episode, an expecting mother has been left a widow after moving into a new cottage in the country.[16] At the husband Ash's funeral, a friend of Martha's, the widow, tells her about a grieving service that allows the living to keep in touch with the dead.[17]

This grieving service turns out to be an artificial intelligence (AI) program that mimics the deceased based on their social media profile.[18] The AI program starts by chatting with Martha via instant message, but as the episode progresses, Martha feeds the program videos and images of Ash and eventually acquires an android for the program to inhabit.[19] The android is a perfect replica of Ash, but Martha becomes concerned when she notices a lack of Ash's negative personality traits and unquestioning compliance when she orders the replica to jump off a cliff.[20]

Admittedly, "Be Right Back" is dramatized science fiction, but there are several real-world instances of the dead "coming back to life" via technology.[21] In 2012, Snoop Dogg and Dr. Dre shocked the crowd at Coachella when they brought out a hologram of Tupac as part of their performance.[22] More recently, at Amazon's Summer 2022 re:MARS conference in Las Vegas, Amazon revealed a potential update to their Amazon Alexa software that would allow the device to mimic a deceased relative's voice.[23] All the program needs to work is one minute of a voice recording.[24]

B. Legislative History of Biometric Identifiers with an Emphasis on Protecting the Immutability and Privacy of These Characteristics

On July 20, 2022, the House Energy and Commerce Committee voted fifty-three to two to advance the American Data Privacy and Protection Act

---

15. *Black Mirror: Be Right Back* (Channel 4 television broadcast Feb. 11, 2013).
16. *Id.*
17. *Id.*
18. *Id.*
19. *Id.*
20. *Id.*
21. Shannon F. Smith, *If It Looks Like Tupac, Walks Like Tupac, And Raps Like Tupac, It's Probably Tupac: Virtual Cloning And Post-Mortem Right Of Publicity Implications*, 2013 MICH. ST. L. REV. 1719, 1722 (2013); Bobby Allyn, *Amazon's Alexa could soon speak in a dead relative's voice, making some feel uneasy*, NPR (June 23, 2022), https://www.npr.org/2022/06/23/1107079194/amazon-alexa-dead-relatives-voice [https://perma.cc/SU32-A2CH].
22. Smith, *supra* note 21.
23. Allyn, *supra* note 21
24. *Id.*

(ADPPA) to the full House of Representatives.[25] The ADPPA includes protections for biometric identifiers, which is the initial focus of modern data privacy laws.[26] The bill has several landmark compromises that allowed it to progress the furthest of any previous comprehensive federal data privacy framework.[27] Among those compromises is a right to control and a delayed right to private action.[28] The ADPPA was criticized on multiple sides for its preemption provision and right of private action.[29] A significant obstacle in the legislative session was Speaker Pelosi's refusal to compromise on the preemption provision that would preempt parts of the data privacy laws of her home state California.[30]

The drafters of the ADPPA have neglected to address a key group in their proposed legislation: the dead.[31] Even if this iteration of a federal privacy framework is not signed into law, federal legislation of its kind is imminent.[32] A federal framework would extend the right of control and the right of private action nationwide.[33] These property rights should allow individuals to utilize estate planning to leave a plan for their biometric identifiers after death.[34] The ADPPA did not receive the support it needed to make it out of the House of Representatives in the 117th legislative session.[35] Nonetheless, several states have taken it upon themselves to pass and enact their own biometric privacy legislation.[36] Individuals and estate planners in these states should take advantage of these rights to ensure the deceased's biometric identifiers are protected after death.[37]

State legislatures have passed data privacy laws with two major concerns in mind: (1) to protect their constituents from invasions of privacy and (2) to prevent harmful uses of biometric identifiers.[38] Companies who collect biometric data must protect their consumers' privacy by telling them

---

25. JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN PRIVACY AND PROTECTION ACT, H.R. 8152 (2022).

26. *See* 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).

27. H.R. 8152 (2022).

28. *Id.*

29. Margaret H. McGill, *Online privacy bill faces daunting roadblocks*, AXIOS (Aug. 4, 2022), https://www.axios.com/2022/08/04/online-privacy-bill-roadblocks-congress [https://perma.cc/236T-JTJK].

30. Joseph Duball, *Pelosi opposes proposed American Data Privacy and Protection Act, seeks new preemption compromise*, IAPP (Sept. 6, 2022), https://iapp.org/news/a/pelosi-rejects-proposed-american-data-privacy-and-protection-act-seeks-new-compromise/ [https://perma.cc/3RMD-VLC4].

31. Kate C. Ashley, *Data of the Dead: A Proposal for Protecting Posthumous Data Privacy*, 62 WM. & MARY L. REV. 649, 651 (2020).

32. Andrea Peterson, *Why experts have hope in the federal privacy bill–even if it doesn't pass*, THE REC. (Aug. 9, 2022), https://therecord.media/why-experts-have-hope-in-the-federal-privacy-bill-even-if-it-doesnt-pass/ [https://perma.cc/CSR9-DNBK].

33. H.R. 8152 (2022).

34. Ashley, *supra* note 31.

35. DiRago, *supra* note 13.

36. *Id.*

37. *See* discussion *infra* Part III.

38. *See* 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018).

the type of data they are going to collect and getting consent from the user.[39] The company must also tell the individual what they are planning to use the data for and if they do share the consumer's data, whom they shared the data with.[40] The legislatures passed these measures to ensure that companies would not misuse the personal biometric identifiers they collect, either by failing to adequately protect the biometric identifiers on file or by using the identifiers in any way not consented to in the original notice.[41]

The harmful use state legislatures envisioned when drafting data security legislation mainly refers to fraud.[42] The immutable nature of biometric identifiers makes it easier for digital fraudsters with access to biometric data not only to defraud once but multiple times.[43] An individual that has fallen victim to fraud via a compromised biometric identifier cannot easily change that identifier like they could a compromised password.[44] In addition to the harm suffered by an individual that has had his or her identity stolen, the use of stolen or compromised credentials is the most common cause of data breaches for companies in 2022, costing these companies an average of $4.5 million per breach.[45]

Biometric data privacy laws are meant to prevent certain harm envisioned by the legislature in the drafting process.[46] The state legislatures that have passed and are currently drafting these types of laws consider their constituencies' discomfort with unforeseen downstream consequences of biometric data collection by companies, as well as the potential for repeated fraud due to the immutability of biometric identifiers.[47] In response to their constituency's concerns, legislatures have passed laws that afford the living property rights in their biometric identifiers.[48] The right to control and the right to private action granted by data privacy legislation gives estate planners the authority to bring biometric identifiers into the deceased's estate as property.[49] The deceased deserve the same protections afforded to the living by biometric data privacy laws because they suffer the same harm as the living as a result of fraud or invasions of privacy.[50] Not including the

39. *See* CAL. CIV. CODE § 1798.100 (West 2018).
40. *See id.*
41. *See id.*
42. *See id.*
43. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
44. Korolov, *supra* note 7.
45. *Cost of a Data Breach Report 2022*, IBM CORP. (July 2022), https://www.ibm.com/downloads/cas/3R8N1DZJ [http://perma.cc/KM8N-YRM8].
46. *ACTEC Trust and Estate Talk: Biometric Recognition Cases*, AM. COLL. OF TR. AND EST. COUNS. (Feb. 23, 2021), https://actecfoundation.org/podcasts/biometric-information-privacy-act-cases-bipa/ [https://perma.cc/Y5TY-7YYY].
47. *Utah Joins California, Colorado, and Virginia With Omnibus Privacy Law*, PERKINS COIE (Mar. 31, 2022), https://www.perkinscoie.com/en/news-insights/utah-joins-california-colorado-and-virginia-with-omnibus-privacy-law.html [https://perma.cc/9GGN-LDLW].
48. *Id.*
49. *See* discussion *infra* Part III.
50. *See* discussion *infra* Part III.

deceased in this legislation leaves a gap in the law for companies and fraudsters to exploit.[51]

Below, this Comment will define what exactly biometric identifiers are and the difference between physical biometric identifiers and behavioral biometric identifiers.[52] From there, this comment will discuss the different laws implemented by state legislatures protecting these identifiers, and how each law, despite having different levels and methods of protection, has similar goals of protecting their constituents from repeated instances of fraud and unforeseen downstream consequences.[53] The logical next step from the legislation is adjudication, most of the jurisprudence for biometric privacy laws has taken place in Illinois and has resulted in interesting interpretations of when an injury occurs in the violation of this legislation.[54] Some federal and state statutes lend themselves to the push for posthumous privacy as well.[55]

This Comment then turns to argue that biometric privacy legislation misses its purpose if it is interpreted to ignore the whole class of biometric identifiers belonging to the deceased.[56] The deceased are just as susceptible, if not more so, to repeated instances of fraud and unforeseen downstream consequences that are the result of unregulated biometric identifiers.[57] The solution advocated by this Comment is that the right to control and right to private action afforded by biometric privacy legislation allows for biometric identifiers to be classified as property, thus bringing these characteristics within estate planning.[58] A classification as property would make biometric identifiers more similar to digital assets governed by the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) than a defamation cause of action.[59] However, reliance on a combination of biometric privacy legislation and the RUFADAA may not be sufficient protection.[60] Finally, this Comment addresses additional counterarguments and practical considerations for change.[61]

51. Ashley, *supra* note 31.
52. *See* discussion *infra* Part II.
53. *See* discussion *infra* Part II.
54. *See* discussion *infra* Part II.
55. *See* discussion *infra* Part II.
56. *See* discussion *infra* Part III.
57. *See* discussion *infra* Part III.
58. *See* discussion *infra* Part III.
59. *See* discussion *infra* Part III.
60. *See* discussion *infra* Part III.
61. *See* discussion *infra* Part III.

II. A BRIEF HISTORY ON BIOMETRIC IDENTIFIERS

A. What Are Biometric Identifiers?

Biometric identifiers are any physical or behavioral characteristics that can be measured.[62] These characteristics must be: universal, every person should have the characteristic; distinct, any two persons should be sufficiently different in terms of the characteristic; permanent, the characteristic should be unchanging over time; and collectible, meaning the characteristic can be measured quantitatively.[63] The ordinary consumer is most familiar and comfortable with physical biometric identifiers like fingerprints and facial geometry.[64] However, biometric identifiers are not limited to just physical measurable characteristics: behavioral biometrics measure characteristics like unconscious gestures, gait, or how an individual reacts to external stimuli.[65] While behavioral biometrics are not as immutable as physical biometrics, they can potentially reveal information people may want to keep private.[66] This information can range from sexual attraction deduced from pupil dilation to gender assigned at birth deduced from facial geometry and voice patterns.[67]

1. Physical Biometric Identifiers

The application of physical biometric identifiers is mostly limited to biometric authentication in a security context.[68] Biometric authentication is a process by which a person proves who they are through the use of a biometric identifier.[69] The biometric identifier of the individual is compared to a database of biometric identifiers, if the identifier presented by the individual matches an identifier in the database, then the identity of the individual is confirmed.[70] Biometric authentication can take the form of face scans to match facial geometry, thumb scans to match fingerprints, and voice verification to match voice prints.[71]

---

62. THALES, *supra* note 1.
63. ANIL K. JAIN, *Biometric Recognition: How Do I Know Who You Are?*, 3540 LNCS 1, 3 (2005).
64. THALES, *supra* note 1.
65. *Id.*
66. *Id.*
67. Aisling Ní Chúláin, *'Reading your mind': How eyes, pupils and heart rate could be used to target ads in the metaverse*, EURONEWS.NEXT (Mar. 12, 2021), https://www.euronews.com/next/2021/12/03/reading-your-mind-how-eyes-pupils-and-heart-rate-could-be-used-to-target-ads-in-the-metave https://perma.cc/3F3Q-QVXH]; Matthew B. Kugler, *From Identification to Identity Theft: Public Perception of Biometric Privacy Harms*, 10 UC IRVINE L. REV. 107, 110 (2019).
68. Kelly A. Wong, *The Face-ID Revolution: The Balance between Pro-Market and Pro-Consumer Biometric Privacy Regulation*, 20 J. HIGH TECH. L. 229, 235 (2020).
69. *Id.*
70. *Id.*
71. *Id.*

While the application of physical biometric identifiers is generally limited to biometric authentication, increases in the technology powering Virtual Reality (VR) headsets and increased metaverse application to the business world may be the method by which corporations begin to value behavioral biometrics.[72]

2. Behavioral Biometrics

Meta has marketed the metaverse as a new stage beyond the constraints of geography for business to take place.[73] They are giving businesses a platform where their team members can meet regardless of where they live.[74] The collection of biometric identifiers can even take place via something as commonplace as a laptop camera.[75] The COVID-19 pandemic has resulted in an increased percentage of the workforce working from home.[76] Many companies are looking for ways to manage the productivity of their workers that do not work out of the office.[77] Some companies track mouse movement and clicks to encourage productivity, but what if they used software to track an employee's heart rate via their laptop camera?[78]

This technology would allow a corporation to closely monitor their employees.[79] Once a baseline heart rate of the productive employee is set, the system can track any aberrations from the productive baseline and accurately report how many hours, minutes, and even seconds the employee engaged in productive work.[80] This one instance seems like a form of micromanagement, but the monitoring system could also gauge how employees interact with their peers and help create cohesive work units.[81] The application of heart rate monitoring is broad, but as the program records employees' reactions to different scenarios, the program will inevitably begin to compile a database

---

72. Rory Mir & Katitza Rodriguez, *If Privacy Dies in VR, It Dies In Real Life*, ELEC. FRONTIER FOUND. (Aug. 25, 2020), https://www.eff.org/deeplinks/2020/08/if-privacy-dies-vr-it-dies-real-life [https://perma.cc/7A2W-S2RZ].

73. Scott Stein, *Watching Me, Watching You: How Eye Tracking Is Coming to VR and Beyond*, CNET (Feb. 21, 2022), https://www.cnet.com/tech/computing/watching-me-watching-you-how-eye-tracking-is-coming-to-vr-and-beyond/ [https://perma.cc/V4FC-HRUY].

74. *Id.*

75. Natalia Martinez et al., *Non-Contact Photoplethysmogram and Instantaneous Heart Rate Estimation From Infrared Face Video*, 2019 IEEE International Conference on Image Processing (Aug. 26, 2019), https://ieeexplore.ieee.org/abstract/document/8803109 [https://perma.cc/2JMF-WVTP].

76. Kim Parker et al., *COVID-19 Pandemic Continues to Reshape Work in America*, PEW RSCH. CTR. (Feb. 16, 2022), https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/ [https://perma.cc/FY69-L6B5].

77. Skye Schooley, *5 Tools for Tracking Your Remote Staff's Productivity*, BUSINESS.COM (last updated Jan. 23, 2023), https://www.business.com/articles/11-tools-for-tracking-your-remote-staffs-productivity/ [https://perma.cc/7A75-7H84].

78. *See id.*; Martinez et al., *supra* note 75.

79. Martinez et al., *supra* note 75.

80. *See id.*

81. *See id.*

of behavioral biometric identifiers.[82] The employer could use this information to elicit particular unconscious responses from an individual.[83] The initial collection and application of behavioral biometric identifiers is a breach of an individual's privacy, and only a few states protect this class of information.[84] This collection of behavioral biometrics is being researched, and its application in the business environment may be what companies with a high percentage of work from home employees are looking for.[85]

The mechanics of VR and the technology's application in the metaverse allow for unprecedented behavioral biometric data collection.[86] VR headsets that utilize eye-tracking technology do so through infrared cameras.[87] While this technology is generally limited to the more expensive business-focused headsets, eye-tracking technology is the expected next step in consumer-focused VR headsets.[88] Eye tracking would allow companies that design and manufacture VR headsets to make the headsets sleeker and more power efficient by mimicking how the eye works by only rendering what the eye is focusing on in high definition.[89] Currently, the VR metaverse has a cartoonish feel, but eye tracking would allow for features like eye contact, making the experience more personal.[90]

There are two different levels of eye tracking in this context, both of which introduce privacy concerns for the architects of the metaverse.[91] One way to use eye tracking is the same way one would use a computer mouse, to drive a particular intention.[92] The other use is more invasive as it records "heat maps" of where the user is looking and how long the user is looking.[93] These recorded heat maps can then be categorized based on the reaction to the stimuli shown.[94] The concern is how these companies will manage this data responsibly.[95]

The collection of behavioral biometric identifiers via VR eye-tracking technology is not isolated.[96] Research shows that a person's heart rate can be collected from a laptop camera.[97] This technology is significant because behavioral biometrics share more information than their physiological

82. *See id.*
83. *See id.*
84. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018).
85. Martinez et al., *supra* note 75.
86. Ní Chúláin, *supra* note 67.
87. Stein, *supra* note 73.
88. *Id.*
89. *Id.*
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.*
96. Martinez et al., *supra* note 75.
97. *Id.*

counterparts.[98] State statutes passed in 2008 and 2009 do not consider or protect behavioral biometric identifiers.[99] However, behavioral biometric identifiers were considered in the ADPPA and newer state legislation and will most likely be included in future biometric privacy legislation.[100]

B. The Failure of the Federal Government to Enact a Federal Biometric Privacy Framework Has Led to the Implementation of Differing Standards in the Various States with Enforced Biometric Identifier Legislation

Despite the legislatures continuing progress in the legislative process, the ADPPA failed to gain enough traction in the 117th legislative session.[101] State legislatures realize it could take some time for their constituents to receive protections for their biometric identifiers at the federal level.[102] Instead of waiting for federal legislation, Utah has joined Virginia and Colorado in passing legislation giving their residents rights in their biometric identifiers, each becoming effective in 2023.[103]

These states will join Illinois, Texas, Washington, and California, adding to the growing number of states with enacted laws protecting their constituents' data privacy.[104] This newer legislation has had the benefit of watching how state and federal courts have interpreted biometric data privacy causes of action in Illinois, resulting in varying degrees of nuance in each state.[105] While there is some overlap, these laws are very complex, and the lack of a national standard means that companies operating in these different states will have to carefully adhere to the different laws in each state they operate in.[106]

While each state has a different tone and varies in the degree of responsibility it assigns companies and the rights it affords to its constituents, the state legislatures consistently recognize two specific harms of unregulated and unprotected biometric identifiers.[107] First, the immutability of biometric identifiers works to both the practicality of the identifiers for

98. Ní Chúláin, *supra* note 67; Kugler, *supra* note 67.
99. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
100. GAFFNEY ET AL., *supra* note 25.
101. Duball, *supra* note 30.
102. PERKINS COIE, *supra* note 47.
103. *Id.*
104. Natalie A. Prescott, *The Anatomy of Biometric Laws: What US Companies Need To Know in 2020*, NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020 [https://perma.cc/5RN2-4FS4].
105. Fredric D. Bellamy, *Looking to the future of biometric data privacy laws*, REUTERS (Apr. 6, 2022 9:13 AM), https://www.reuters.com/legal/legalindustry/looking-future-biometric-data-privacy-laws-2022-04-06/ [https://perma.cc/S45K-4YX6].
106. Brenna Goth, *Colorado Consumer Privacy Rules Add to Looming Business Mandates*, BLOOMBERG L. (Oct. 21, 2022), https://news.bloomberglaw.com/privacy-and-data-security/colorado-consumer-privacy-rules-add-to-looming-business-mandates [https://perma.cc/7XVJ-5E6Q].
107. *See id.*

authentication as well as one of the main vulnerabilities.[108] State legislatures recognize the advantages and risks of immutable biometric identifiers, and have drafted legislation allowing corporations to collect and use this data, but require minimum approved security protocols and restricts transfer to third parties.[109] Second, the unforeseen downstream consequences of collecting and using biometric identifiers make people meaningfully uncomfortable.[110] To ensure corporations stay within their constituents' comfort zones, legislatures have enacted laws that require corporations to gain consent when they collect biometric identifiers and to limit their use of the biometric identifiers to what was stated in the notice of consent.[111]

1. Prevent Harmful Uses

Many state legislatures recognize that the immutability of biometric identifiers poses unique problems for fraud and identity theft.[112] An individual that has had their biometric identifier misappropriated by a cybercriminal is at risk for repeated instances of fraud because they cannot change their biometric identifiers like they could a password.[113] Additionally, corporations that utilize biometric authentication for security purposes are exposed to data breach risks from fraudulent access via biometric identifiers.[114]

Scammers can use stolen biometric data in many different ways.[115] These biometric identifiers can be used to fool biometric scanners in high-value locations and to create fake identities for online platforms.[116] The most widespread avenue for these scammers is selling the identifiers to create fake identities.[117] Once identities are sold, a motivated individual can use the falsified credentials to take over accounts and compromise operations.[118]

Identity theft is not the only harm of biometric identifier-facilitated fraud.[119] Fraudsters or hackers can use biometric identifiers to access a company's secured database and facilitate a data breach.[120] The efficiency of

---

108. Bellamy, *supra* note 105.
109. Prescott, *supra* note 104.
110. Kugler, *supra* note 67.
111. *See* Goth, *supra* note 106.
112. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018).
113. Korolov, *supra* note 7.
114. *See* Peter Tsai, *Data Snapshot: Biometrics in the workplace commonplace, but are they secure?*, SPICEWORKS (Mar. 12, 2018), https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure [https://perma.cc/RUC9-ZP6R].
115. *How can scammers use biometric data?*, COVERY (June 21, 2022), https://blog.covery.ai/how-can-scammers-use-biometric-data/ [https://perma.cc/K4YY-X7GT].
116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*
120. *Cost of a Data Breach Report 2022*, *supra* note 45.

biometric authentication has proven to be an asset for companies looking to streamline security.[121] In a survey of IT professionals from North America and Europe conducted by Spiceworks, 62% of companies are already using biometric authentication with another 24% planning to deploy a system in the next two years.[122] The most common applications include authentication technology on phones and laptops, as well as time clock systems.[123] The top security concerns cited by these IT professionals run counter to the security concerns biometric authentication is implemented to prevent.[124] Of the respondents, 57% reported that their top security concern was the fact that biometric identifiers can be compromised or replicated, 48% cited the risks of stolen biometric data, and the top security concern of 35% of the respondents was the fact that biometric identifiers cannot be revoked or replaced.[125]

Data breaches are happening more frequently and on a larger scale.[126] In June 2015, the Office of Personnel Management for the United States reported that it had experienced a data breach.[127] 21.5 million individuals were affected by this breach, and 5.6 million of the records the agency lost were fingerprints of federal employees.[128] Governmental agencies are not the only entities at risk of suffering a data breach.[129] Executives at 88% of private and public companies now consider cybersecurity to be a direct threat to business operations instead of a problem for IT to handle.[130]

In IBM's annual Cost of a Data Breach Report for 2022, the use of stolen or compromised credentials was found to be the most common cause of data breaches.[131] Breaches using this data cost an average of $4.5 million per breach, taking 243 days to identify and another eighty-four days to contain.[132] IBM includes personally identifiable information in this category and defines a compromised record as "information that identifies the natural person or individual."[133]

---

121. Tsai, *supra* note 114.

122. *Id.*

123. *Id.*

124. *See id.*

125. *Id.*

126. Aaron Drapkin, *Data Breaches That Have Happened in 2023 So Far*, TECH.CO, https://tech.co/news/data-breaches-2022-so-far (last updated Jan. 23, 2023) [https://perma.cc/4J52-8RQ3].

127. *Cybersecurity Incidents*, U.S. OFFICE OF PERSONNEL MANAGEMENT, https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last visited Jan. 30, 2023) [https://perma.cc/RF3J-BKFR].

128. *Id.*

129. Steve King, *Gartner Research: Cybersecurity Leaders Losing Control in Distributed Ecosystem*, CYBER THEORY, https://cybertheory.io/gartner-research-cybersecurity-leaders-losing-control-in-a-distributed-ecosystem/ (last visited Mar. 29, 2023) [https://perma.cc/PX94-Z666].

130. *Id.*

131. *Cost of a Data Breach Report 2022*, *supra* note 45.

132. *Id.*

133. *Id.* at 55.

Companies like Facebook and Apple that collect biometric data can fall victim to a data breach as well.[134] Biometric identifiers are the epitome of personally identifiable information and are worth the most money after being acquired in a data breach.[135] As companies explore different methods to stop data breaches the immutability and efficiency of biometric identifiers have already been recognized.[136] However, the benefits of stolen or compromised credentials as a method to breach the databases of companies as well as their relative worth to scammers and fraudsters make the security of biometric identifiers collected by companies for authentication purposes tantamount.[137]

2. Data Security

The data security concern cited by state legislatures in the promulgation of biometric data privacy legislation relates to the individual's privacy.[138] The Illinois legislature acknowledged that while their constituents may be fine with biometric authentication in limited circumstances, their constituents were concerned with unforeseen downstream consequences of the collection and use of these identifiers.[139] Therefore, this legislation was enacted as a check on the corporations that collect and use biometric identifiers to ensure that their use of biometric identifiers stays within the bounds of their consumer's comfort zones.[140]

Beyond representing an identifier more innate and secure than a state-issued identifier like a Social Security number or driver's license, biometric identifiers have no real economic value.[141] Once aggregated, however, a database of biometric identifiers is considered an asset.[142] This became an issue for the Illinois Legislature in 2008 when Pay By Touch filed for bankruptcy.[143] Pay By Touch had a database of consumer fingerprints that the trustee for the bankruptcy had determined was an asset; Illinois wanted to prevent the sale of this database during the bankruptcy.[144]

To prevent the transfer of Pay By Touch's fingerprint database to a corporation that the owner of the fingerprint had never consented to give their

---

134. Drapkin, *supra* note 126.

135. *Cost of a Data Breach Report 2022*, *supra* note 45.

136. Tsai, *supra* note 114.

137. *Cost of a Data Breach Report 2022*, *supra* note 45.

138. *See e.g.*, 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018).

139. Kugler, *supra* note 67.

140. *Id.*

141. Ashley, *supra* note 31 at 658.

142. Kwabena A. Appenteng & Philip L. Gordon, *Biometric Privacy Case Before Illinois Supreme Court Could Open Litigation Floodgates*, LITTLER (Nov. 16, 2018), https://www.littler.com/publication-press/publication/biometric-privacy-case-illinois-supreme-court-could-open-litigation [https://perma.cc/WX86-7MRG].

143. *Id.*

144. *Id.*

fingerprint, Illinois passed the Biometric Identifier Privacy Act (BIPA).[145] BIPA was a landmark statute that is fundamentally a consumer protection law that regulates the collection, use, storage, and safeguarding of biometric information.[146] Illinois became concerned with the security of these identifiers because unlike a password or Social Security number that can be changed, these are biologically unique.[147] Once these identifiers are compromised the individual has no recourse and is at an increased risk of identity theft.[148]

Texas was the next state to enact legislation protecting data privacy in 2009.[149] The Texas Capture and Use of Biometric Identifier Act (CUBI) requires companies to give notice to consumers that they are collecting biometric data and their plans for the data they collect.[150] While the statutory violation fine is more burdensome than BIPA, CUBI does not provide consumers a private right of action.[151]

The California Consumer Privacy Act (CCPA), updated in 2020, is one of the more recent state laws protecting data privacy.[152] Modeled after the European Union's General Data Protection Regulation, it is the most expansive and protective regulation for biometric identifiers.[153] It is similar to BIPA in providing a right of private action and also gives residents more control over their data once collected.[154] These consumer rights include: the right to notice, the right to know, the right to delete, the right to opt out, the right to opt in for minors, and the right to non-discrimination.[155]

BIPA is preventative legislation both in the context of its enactment and in practical application.[156] The Illinois Legislature introduced the first data privacy legislation in response to the possibility that Pay By Touch's database of consumer biometric identifiers might be sold to a third party.[157] This unforeseen downstream harm is the common theme for biometric data privacy legislation.[158]

In a study done by Dynata, 1,029 people were surveyed to assess their comfort level with different uses of biometric identifiers.[159] The study found that the majority of the individuals surveyed were comfortable with biometric

145. *See* 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
146. ACTEC, *supra* note 46.
147. *Id.*; *see e.g.*, 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
148. *See e.g.*, 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
149. TEX. BUS. & COM. CODE ANN. § 503.001.
150. *Id.*
151. *Id.*
152. CAL. CIV. CODE § 1798.100 (West 2018).
153. *Id.*
154. *Id.*
155. CAL. CIV. CODE §§ 1798.105, .106, .110, .115, .120, .121, .125 (West 2018).
156. *See* 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); Kugler, *supra* note 67, at 132–33.
157. Appenteng & Gordon, *supra* note 142.
158. Kugler, *supra* note 67, at 134.
159. *Id.* at 138.

authentication to promote security.[160] These security measures included using either facial or fingerprint biometrics to unlock their phone or apps, and using voice biometrics to verify identity over the phone.[161] However, when asked about future applications of biometric identifiers, people were much more uncomfortable.[162] These future applications included using facial biometric identifiers to track people on public streets, detect photos of celebrities online, and link people's social media profiles across different sites.[163]

Using biometric identifiers in security applications makes a big difference in determining comfort levels: "58.9% of people were comfortable . . . using facial recognition to detect when people who were banned from the store, such as previously apprehended shoplifters, had entered."[164] In the same store and using the same technology, however, "only 25.8% were comfortable with the business using facial recognition to track customer interest for serving advertisements."[165]

The Dynata study and the Illinois Legislature's motivation in passing BIPA show the same sentiment.[166] While most acknowledge the security applications of biometric identifiers, people are meaningfully uncomfortable with the collection of certain biometric identifiers "even without specific threats of downstream consequences."[167] Actual specific harm is not necessary to protect an individual's rights, as one of the hallmarks of the privacy space is "the discovery of new uses for old information."[168]

C. The Jurisprudence of Biometric Data Privacy Causes of Action Indicates an Individual is Harmed by a Mere Violation of the Statute

In *Patel v. Facebook*, Patel sued Facebook via BIPA for collecting biometric identifiers from its users without giving them notice.[169] Facebook implemented a user template that identified its users in a posted photo and then would automatically tag those users in any future pictures they were in.[170] Facebook essentially captured the facial geometry of its users without their consent and assigned the user's biometric identifier to their profile.[171]

Practically every time Patel's image was included in a Facebook post, his facial geometry biometric identifier was run against the database of the

160. *Id.* at 139.
161. *Id.* at 140.
162. *Id.*
163. *Id.* at 140–141.
164. *Id.* at 140.
165. *Id.*
166. *See id.*; 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
167. Kugler, *supra* note 67, at 146.
168. *Id.*
169. Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019).
170. *Id.* at 1269.
171. *See id.* at 1268.

identifiers of every Facebook user in the database.[172] When Patel's facial geometry from the new Facebook post found its match in Facebook's database of biometric identifiers, his Facebook profile would automatically be tagged in a photo he may not have known of.[173] Patel and other Facebook users had no idea that their biometric identifiers were being collected from each post on Facebook.[174]

The Ninth Circuit Court of Appeals held this to be an invasion of privacy and, therefore, an actual injury.[175] On its face, this auto-tagging feature seems benign, and—the invasion of privacy aside—it may not cause real harm.[176] However, the scenario that the Ninth Circuit found concerning was the database maintained by Facebook in which any person with access could use a picture of an unknown person to not only identify the individual, but access their Facebook page and all the information posted there.[177]

The right to private action in BIPA has resulted in most of the jurisprudence interpreting biometric identifier privacy legislation taking place in Illinois.[178] The harmful uses of an individual's biometric identifiers by corporations mostly relate to violations of BIPA's written consent provision.[179] The relevant issue most of the cases turn on is whether technical violations of BIPA can constitute an injury-in-fact to the plaintiffs.[180]

In *Bryant v. Compass Group*, the plaintiff was required to prove that the violation of the written consent provision of BIPA was a sufficient harm to constitute an injury-in-fact.[181] Bryant argued that because she "was denied the opportunity to make informed consent as to the use, storage, and dissemination of her biometric information, she suffered a concrete injury."[182] The Seventh Circuit Court of Appeals applied the Supreme Court's analysis in *Spokeo, Inc. v. Robins* to determine whether an injury existed.[183] In *Spokeo*, the court held that while an injury must exist, the injury does not need to be tangible.[184] The Seventh Circuit held that Bryant suffered an invasion of privacy and that an invasion alone was sufficient harm.[185]

---

172. *See id.*
173. *See id.*
174. *See id.*
175. *Id.* at 1274.
176. *See id.*
177. *See id.*
178. *See* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619 (7th Cir. 2020); *see* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1210 (Ill. 2019); *see* Citizens Ins. Co. of Am. v. Cooler Screens, Inc., No. 1:22CV03800 (Ill. Cir. Ct. July 1, 2022).
179. ACTEC, *supra* note 46.
180. *Id.*
181. *Bryant*, 958 F.3d at 627.
182. ACTEC, *supra* note 46.
183. *Bryant*, 958 F.3d at 627.
184. Spokeo, Inc. v. Robins, 578 U.S. 330, 339–41 (2016).
185. *Bryant*, 958 F.3d at 627.

Likewise, the Illinois Supreme Court in *Rosenbach v. Six Flags* denied the defendant's argument that to be "aggrieved" under BIPA, the plaintiff must plead or prove additional consequences beyond the mere technical violation of the statute.[186] *Bryant* and *Rosenbach* set the precedent in Illinois that a violation of the consent provision of BIPA constitutes an injury-in-fact that will support a suit.[187] As BIPA continues to mature, the contours of the protections the law provides continue to take shape.[188]

A notable case filed in 2022, *Roberts v. Cooler Screens Inc.*, asks whether smart cooler screens that employ facial profiling systems to choose the advertisements displayed on smart cooler screens violate the BIPA requirement to provide information and obtain consent.[189] The system considers the shopper's age, gender, and emotional response and then displays the selection and advertisements that the program believes the shopper will most likely purchase.[190] This case may be difficult for the Illinois court as the smart coolers are collecting behavioral biometric identifiers which are not covered in BIPA.[191] However, gender and physical indicators of age are protected as physical biometric identifiers.[192] If Cooler Screens is allowed to circumvent BIPA protections by only collecting behavioral biometric identifiers, it might be a signal to the Illinois Legislature that they need to consider updating BIPA protections to include behavioral biometric identifiers.[193]

Another case, filed in Washington in 2022, asks whether a plaintiff can seek damages for an injury that has not happened yet.[194] Arthur J. Gallagher & Co. is a leading insurance brokerage, risk management, human resources, and benefits consulting company that the plaintiff alleged had received personally identifiable information and protected health information from its clients.[195] The company then suffered a data breach in June 2020, but it was not discovered until September.[196] The company then neglected to inform the plaintiffs of the breach until July 2021, nine months later.[197] In the end, the breach affected 72,835 people as of December 2021.[198] The plaintiffs seek damages, claiming that their personally identifiable information and protected health information are on the dark web and will inevitably lead to

186. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019).
187. *Id.*; *Bryant*, 958 F.3d at 627.
188. *See* ACTEC, *supra* note 46.
189. Roberts v. Cooler Screens Inc., No. 2022-CH-01824 (Ill. Cir. Ct. July 1, 2022).
190. *Id.*
191. *Id.*
192. *Id.*
193. *Id.*
194. *See* Copple v. Arthur J. Gallegher & Co., C22-0116-LK-SKV, 2022 WL 3357865, at *1 (W.D. Wash. Aug. 2, 2022).
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.*

attempts at identity theft by cybercriminals.[199]

Copple v. Arthur J. Gallagher & Co. will be interesting to follow as the plaintiff's attorneys have successfully transferred the suit to Illinois courts.[200] If the Illinois court follows the precedent set in *Bryant,* will it identify the transfer of personally identifiable information and protected health information as the harm suffered by the plaintiffs?[201] Or will the court attempt to assign a dollar amount to the breached information allegedly on the dark web in an attempt to recompense the plaintiffs for the forfeiture of their private information and the increased potential for identity theft?[202]

D. Federal and State Statutes Setting the Scene for a Right of Posthumous Privacy

It is generally accepted that the right to privacy lapses upon death.[203] How, then, can the deceased merit the same data security concern as the living regarding their biometric identifiers?[204] The right to privacy itself is a new concept established in *Griswold v. Connecticut* and has not yet enjoyed broad acceptance in its application to the living, much less to the dead.[205] In general, the rights of the living take precedence over the rights of the dead, but an essential concept of estate planning doctrine is carrying out the wishes of a decedent.[206] This often interferes with the rights of the living, whether it is leaving the evil oldest son out of the will and denying his inheritance, or honoring Hunter S. Thompson's last request to have his ashes shot out of a cannon.[207] Despite the ongoing debate, there are notable instances of the privacy rights of the dead being protected, two of which are federal statutes.[208]

The Health Insurance Portability and Accountability Act (HIPAA) provides for a posthumous right to privacy that could apply to biometric identifiers.[209] Per 45 C.F.R. Section 160.103, an individual's protected health information is safeguarded for fifty years after death.[210] This health

199. *Id.* at *5.

200. *Id.* at *1.

201. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 627 (7th Cir. 2020).

202. Kristin L. Bryan, et al., *JUST RELEASED: 2022 Q1 AI/Biometric Litigation Trends*, NAT'L L. REV. (Apr. 1, 2022), https://www.natlawreview.com/article/just-released-2022-q1-aibiometric-litigation-trends [https://perma.cc/2CSN-A899].

203. Tex. Att'y Gen. Op. No. OR-06114 (2021).

204. *See* discussion *infra* Section III.A.

205. *See* Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965).

206. *See Ashes of Hunter S. Thompson blown into sky*, N.Y. TIMES (Aug. 21, 2005), https://www.nytimes.com/2005/08/21/world/americas/ashes-of-hunter-s-thompson-blown-into-sky.html [https://perma.cc/7C65-UL5N].

207. *Id.*

208. 45 C.F.R. § 160.103; 5 U.S.C. § 552.

209. *See* 45 C.F.R. § 160.103(2)(iv).

210. *Id.*

information includes demographic information as well as personal information that

> (2) [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) [t]hat identifies the individual; or (ii) [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.[211]

While it may seem that the phrase "personal information . . . that identifies the individual" is dispositive, the main weakness of HIPAA is that it has not been interpreted by federal appeals courts to constitute a private right of action.[212] It is hard to claim a right if there is no method to vindicate the abuse of that right.[213]

There have been several attempts to use the Freedom of Information Act (FOIA) to gain access to personal and medical files and crime scene photos, namely pictures of a deceased individual.[214] The statute contains a provision exempting this type of information from public access as it "would constitute a clearly unwarranted invasion of personal privacy."[215]

Both of these rights have been established to protect the privacy rights of the survivors of the decedents.[216] However, while these statutes have the effect of protecting the rights of the dead, there is no language that specifically grants a posthumous right to privacy.[217]

1. Survivability Statutes

At common law, a tort action did not survive the death of the injured party or the tortfeasor.[218] It did not matter whether the suit was commenced before or after the death; the suit was barred at the death of either party.[219] The common law required that suit be brought by and against the parties to the alleged wrong.[220] That changed over time as states recognized the importance of redressing the estate for the injuries a decedent suffered while alive.[221] Each state individually adopted some form of a survivability statute,

---

211. *Id.*
212. Ashley, *supra* note 31.
213. *Id.*
214. 5 U.S.C. § 552(c)(6).
215. *Id.*
216. Ashley, *supra* note 31.
217. *Id.*
218. James D. Sumner Jr., *Choice of Law Governing Survival of Actions*, 9 HASTINGS L.J. 128, 129 (1958).
219. *Id.*
220. *Id.*
221. 1A TEX. JUR. 3D *Actions* § 212.

which led to a wide variance of the causes of action permitted to survive the death of the injured party.[222] Most states allow for the survival of personal injury actions and actions for injury to property, while only a few permit the survival of actions involving injury to reputation.[223]

Until 1985, Texas did not adopt legislation preserving a cause of action that did not abate due to the death of the harmed person.[224] The Texas Survival Statute (Survival Act) is often confused with its Wrongful Death Act, but the main difference is that the Survival Act "did not create a new cause of action, but kept alive the cause of action that the deceased might have had."[225] The practical effect of this cause of action was to allow a close third party to sue for punitive damages in place of the deceased.[226]

Survivability statutes set a precedent for the right to sue on a decedent's behalf.[227] These statutes add weight to existing federal laws, like HIPAA and FOIA, through implications of posthumous privacy.[228] The state legislation, while varied and nuanced, allow the decedent's estate to redress injury despite the death of the injured party.[229] While the motivation of these laws seems geared more toward ensuring the rights of a decedent's survivors, they still have the effect of protecting the decedent's rights.[230]

E. Property Theory and Biometric Identifiers

Property rights are often characterized as a bundle of sticks, some of the more prominent of which are the right to control, use, or exclude.[231] This applies to personal property as well as real property, the main distinction being whether the property is moveable.[232] If the object is not affixed to the land, it is more likely than not a form of personal property.[233]

State biometric privacy laws already assign the right to control to their constituents, such as the right to be informed of whether or not a corporation is collecting their biometric identifiers.[234] The user can then choose whether or not they consent to the collection of their data.[235] Similarly, the constituents of some states with effective biometric privacy laws can pursue

222. *Id.*
223. Sumner, *supra* note 218.
224. TEX. CIV. PRAC. & REM. CODE ANN. § 71.021.
225. Hofer v. Lavender, 679 S.W.2d 470, 476 (Tex. 1984).
226. TEX. CIV. PRAC. & REM. CODE ANN. § 71.021.
227. *Id.*
228. *See id.*
229. Sumner, *supra* note 218.
230. Ashley, *supra* note 31, at 674.
231. Jane B. Baron, *Rescuing the Bundle-of-Rights Metaphor in Property Law*, 82 U. CIN. L. REV. 57, 58 (2014), https://scholarship.law.uc.edu/uclr/vol82/iss1/2 [https://perma.cc/E7LL-W2ED].
232. *Id.*
233. *Id.*
234. *Id.*
235. *Id.*

private action against a corporation that violated the informed consent provision or any other violation of the law.[236] This serves as the basis for the argument that biometric identifiers are personal property, thus naturally falling within the confines of estate planning law allowing the executor or survivors of a decedent's estate to assert a cause of action under biometric privacy legislation on behalf of the deceased.[237]

III. ARGUMENT

Consider the following hypothetical scenario: A young college student who has been unable to find a partner through conventional means downloads a dating app recommended to them by their peers.[238] After several assurances that the app works best if the user utilizes all available features, the young student leaves several voice recordings in response to prompts they choose for their profile.[239] Unfortunately, one month later, the student suffers a fatal car accident.[240]

As the student's loved ones are putting their affairs in order, they notice several transactions on the student's credit cards after their death.[241] It turns out that the company that runs the dating app had been selling their client's information to a third party.[242] The third party was developing an AI time clock program that used an employee's voice print to clock them in and out of work.[243] The third party had suffered a data breach that included the college student's voice recordings uploaded to their dating profile.[244] A cybercriminal had then used those voice recordings to fool the voiceprint authentication software used by the deceased student's bank to claim they were the deceased college student requesting replacement credit cards.[245]

Luckily, the fraud was contained, but the student's loved ones became upset when they realized that the voiceprint was lost to the dark web and could be used for whatever purpose by anyone who purchased it there.[246] As Illinois residents, the student's loved ones had contacted an attorney after they had heard about the class action lawsuit against the dating app for the unconsented and uninformed transfer of biometric data in violation of state law, but were upset to learn that the student had to be alive to join the suit.[247]

---

236. *Id.* at 83.
237. *Id.* at 57.
238. Author's original thought; *see* Stein, *supra* note 73.
239. Author's original thought.
240. *Id.*
241. *Id.*
242. *Id.*
243. *Id.*
244. *Id.*
245. *Id.*
246. *Id.*
247. *Id.*

In the situation above, the deceased's estate lost control of the voiceprint of the college student.[248] Not only did an identity thief use the voiceprint to defraud the student's bank account, but the voiceprint is also floating on the dark web.[249] The survivors of the deceased have no idea when or how they would get the record back, or what other nefarious schemes the voiceprint may be used for.[250]

Had the student survived the car accident, they would be able to assert a cause of action against the dating app for the uninformed and unconsented transfer of biometric data to a third party under BIPA.[251] If the decedent's executor or survivors can prove that the transfer happened before the student's death, they may be able to still pursue their claim under Illinois's survivability statute.[252] However, a BIPA violation action brought by a decedent's estate is not likely to survive a motion for dismissal.[253]

The student has still suffered the same harm that their living counterpart would have suffered.[254] They were defrauded once and are exposed to repeated instances of fraud in the future.[255] Additionally, forfeiting their voiceprint to the dark web forces them to wait for some other unforeseen application of private information.[256] Allowing a decedent's estate to pursue a BIPA violation on the decedent's behalf may not be a perfect solution, but it retains the incentive of punishment for the deceased in addition to the living, thus evening the playing field.[257]

A. The Biometric Identifiers of the Dead are Subject to the Same Harms as Those of the Living

The collection and use of the biometric identifiers of the dead are currently unregulated and unprotected.[258] This gap in the law runs counter to the purpose of standing and proposed biometric data privacy legislation that ensures the individual's privacy through data security and prevents harmful uses of an individual's biometric identifiers.[259] The right to control and the right to private action are property rights that should painlessly bring the electronic record of an individual's biometric identifier within the scope of estate planning, allowing an authorized representative to assert the rights of

248. *Id.*
249. *Id.*
250. *Id.*
251. *Id.*
252. *Id.*
253. *Id.*; *see* 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
254. *Id.*
255. *Id.*
256. *Id.*
257. *Id.*
258. Ashley, *supra* note 31.
259. *Id.*

a decedent.[260] A comprehensive federal data privacy framework, like the one suggested by the ADAPPA, would extend these rights nationwide ensuring clarity of purpose.[261] Not addressing this gap leaves the biometric identifiers of the deceased vulnerable to downstream consequences and harmful uses of their biometric identifiers, nullifying the purpose of biometric data privacy laws.[262]

1. The Immutability of Biometric Identifiers Bring Value to Corporations and Cybercriminals While Exposing the Individual to the Risk of Repeated Identity Theft

Biometric identifiers are nothing new; what is new is the ability to collect and aggregate this data en masse.[263] As biometric identifiers have become more ubiquitous in society, the value of the biometric databases companies maintain has increased as well.[264] Multiple parties find value in biometric identifiers.[265] Individually, hackers or scammers will pay $180 for each record of a customer's personally identifiable information.[266] Corporations that collect their consumer's biometric data like Google and Meta have found value by aggregating the identifiers they collect and selling access to the data to advertisers.[267] These two parties are different in the ways they value and use biometric identifiers, but living consumers are protected from both in data privacy legislation.[268] The dead, however, are not, leaving corporations and fraudsters room to abuse their biometric identifiers.[269]

Post-mortem fraud is not a far-removed, conceptual harm; in 2012 ID Analytics released a study that found the "identities of nearly 2.5 million deceased Americans are used by fraudsters to commit identity theft each year."[270] Cybercriminals recognize the window of opportunity after an individual's death and use it to "open credit cards, apply for jobs under a dead person's name, and get state identification cards," the window only closes upon authorities updating their database regarding a new death.[271] This

260. Author's original thought; *see* notes 234–37 and accompanying text.

261. *See* discussion *supra* Part II.

262. Kugler, *supra* note 67.

263. THALES, *supra* note 1.

264. Kugler, *supra* note 67, at 118.

265. Aimee O'Driscoll, *30+ data breach statistics and facts*, COMPARITECH, https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/ (last updated Jan. 4, 2023) [https://perma.cc/27RU-HDN7].

266. *Id.*

267. Ashley, *supra* note 31.

268. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); CAL. CIV. CODE § 1798.100 (West 2018).

269. Ashley, *supra* note 31, at 650.

270. *Identity Theft and Tax Fraud: Hearing Before the H. Comm. on Ways and Means*, 112th Cong. 6 (2012) (statement of Rep. Sam Johnson, Chairman, Subcomm. on Social Security).

271. Gerry W. Beyer & Kerri G. Nipp, *Cyber Estate Planning And Administration* (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2166422 [https://perma.cc/U8T9-GWDP].

problem is exacerbated when criminals gain access to one or more of an individual's biometric identifiers.[272] As more Americans with online presence die each year, postmortem fraud will increase.[273]

Bringing biometric identifiers within estate planning via the right to control and right of private action lets estate planners mitigate the risk of post-mortem fraud.[274] This closes the window of opportunity cybercriminals have to commit identity theft or gain access to a company's servers to leak their data.[275] Excluding the dead's biometric identifiers from data privacy laws negates the preventative effect that incentivizes companies not to invade the privacy of their users.[276] It also allows for instances of fraud and identity theft on an individual level and is a reliable method by which a cybercriminal might gain access to a company and leak its data.[277]

2. The Purpose Drift that Characterizes Advances in Technology Will Likely Result in Unforeseen Downstream Consequences

It is worth acknowledging that BIPA was passed in response to the possibility that a bankrupt Pay By Touch might be required to sell its database of fingerprints as an asset.[278] Data privacy laws are a preventative measure; state legislatures have recognized the immutability and inherent private nature of biometric identifiers.[279] To not extend the same protection to the dead runs counter to the purpose of the law.[280]

As physical biometric identifiers become more ubiquitous in society, the argument for biometric privacy for privacy's sake becomes tenuous.[281] Apple has allowed consumers to unlock their phones using fingerprints since at least 2017, state governments collect fingerprints when they issue driver's licenses to residents, and recently TSA has implemented face scans that utilize facial geometry to confirm a traveler's identity.[282] While unique and immutable to every person, a fingerprint by itself exposes no personal information and chances are high that individuals that interact in modern society already have fingerprints recorded somewhere.[283]

---

272. Ashley, *supra* note 31.

273. *Identity Theft and Tax Fraud: Hearing Before the H. Comm. on Ways and Means*, 112th Cong. 6 (2012) (statement of Rep. Sam Johnson, Chairman, Subcomm. on Social Security).

274. Author's original thought.

275. Beyer & Nipp, *supra* note 271, at 3.

276. Ashley, *supra* note 31.

277. O'Driscoll, *supra* note 265.

278. Kugler, *supra* note 67.

279. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. 6 (2022); CAL. CIV. CODE § 1798.100 (West 2018).

280. Ashley, *supra* note 31.

281. Kugler, *supra* note 67.

282. *Id.*

283. *Id.*

While it may seem that facial geometry is a characteristic that the average person wants to keep private, the wish for privacy has not stopped social media companies from enjoying success in the United States.[284] In social media companies like Facebook and Instagram, the concept they sell revolves around users sharing pictures of themselves that often contain biometric identifiers.[285] Additionally, merely appearing in public may leave a recorded instance of an individual's facial geometry.[286]

The prevalence of the collection and use of physical biometric identifiers like fingerprints and facial geometry takes these characteristics out of the realm of private information into semipublic data.[287] Nonetheless, Americans are still concerned with the security of this semi-public data.[288] Biometric data privacy statutes like BIPA were not passed in response to specific harm, but instead because state legislatures recognized the importance of protecting their constituencies' privacy.[289] Consumers may be perfectly fine with their biometric identifiers being used in a specific context, but a change in the context may result in a change of approval.[290] Such is the result of the Dynata study, which found that the majority of the individuals polled were comfortable with the application of biometric identifiers to promote security.[291] However, when the context for the application of the same identifier changed from security to other realistic uses of the data, like targeted advertisements, the comfort level of the respondents dropped considerably.[292]

Behavioral biometric identifiers and the information that can be gathered from them pose additional concerns.[293] As different methods of quantifying and collecting behavioral biometric identifiers become more advanced, like eye-tracking technology in VR and heart rate monitoring via laptop computers, the security of these identifiers and the private information that can be extracted from them warrant increased protections.[294]

Behavioral biometric identifiers are different from physical biometric identifiers in that they reveal information most people want to keep private, whether it is sexual attraction deduced from pupil dilation or gender assigned at birth deduced from facial geometry and voice patterns.[295] Laws like BIPA

---

284. *Id.*
285. *Id.*
286. *Id.*
287. *Id.*
288. Chris Teale, *Voters Overwhelmingly Back Major Provisions of Proposed Federal Data Privacy Law*, MORNING CONSULT (June 15, 2022), https://morningconsult.com/2022/06/15/support-for-federal-data-privacy-law/ [https://perma.cc/PT44-DCCW].
289. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
290. Kugler, *supra* note 67.
291. *See id.*
292. *See id.* at 140.
293. Stein, *supra* note 73.
294. *Id.*
295. Kugler, *supra* note 67.

do not specifically account for behavioral biometrics.[296] BIPA protections are limited to "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[297]

Consumers may be fine with allowing companies that design VR headsets to record their eye heat maps to help improve the VR software.[298] However, consumers would probably take issue with the companies using eye-tracking software to record a person's behavioral biometrics and then selling that data to advertisers.[299] While the utilization of behavioral biometric identifiers may seem beyond legislation, BIPA suits have been litigated over some of the instances where a change in the application of physical biometric identifiers make people meaningfully uncomfortable.[300]

As technology continues to develop, making the collection and use of behavioral and physical biometric identifiers more practical, the resulting purpose drift will result in applications of these identifiers that make people meaningfully uncomfortable.[301] In response, states will pass, and have already passed, legislation to protect these identifiers.[302] Estate planners should be able to assert these rights because the current gap in the law allows corporations to use the identifiers of the deceased in a way that makes society meaningfully uncomfortable.[303]

3. The Contribution of Biometric Identifiers to Invasive Advertising Practices

Beyond unforeseen potential consequences of unregulated biometric identifier collection and use, behavioral biometric identifiers can be used to increase the accuracy of invasive targeted advertising.[304] Internet users have long accepted that the more they interact with websites like Google and Instagram, the more personalized their recommended advertisements become.[305] Normally these advertisements are benign, such as a pop-up advertisement for blue jeans after shopping online for pants the previous day.[306] However, corporations have not limited themselves to just monitoring

296. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
297. *Id.*
298. Stein, *supra* note 73.
299. Kugler, *supra* note 67.
300. *See* discussion *supra* Section II.C.
301. Kugler, *supra* note 67.
302. PERKINS COIE, *supra* note 47.
303. Author's original thought; Kugler, *supra* note 67.
304. Umar Iqbal et al., *Your Echos are Heard: Tracking Profiling and Ad Targeting in the Amazon Smart Speaker Ecosystem*, CORNELL UNIV. 1, 16–17 (May 11, 2022), https://arxiv.org/pdf/2204.10920.pdf [https://perma.cc/P6CN-LWKK].
305. Brian X. Chen, *Are targeted ads stalking you? Here's how to make them stop*., SEATTLE TIMES (Aug. 31, 2018), https://www.seattletimes.com/business/are-targeted-ads-stalking-you-heres-how-to-make-them-stop/ [https://perma.cc/8MX5-RV95].
306. *Id.*

browsing history.[307]

Smart speakers have been shown to record audio from their environments and share that information online with third parties that can use this audio to produce targeted advertisements.[308] Again, these advertisements can be innocuous, such as seeing an advertisement for shoes after a conversation with a friend about wanting to buy new shoes.[309] However, the next step is more invasive: "Amazon has a patent for advertising products to users based on inferences from physical and emotional characteristics of users' voices, e.g., targeting cough-drop ads at users with colds."[310] Some users may find this helpful, but others could be concerned about the level of intimate information these smart speakers are privy to.[311]

Physical characteristics of the user's voice aside, advertisements directed to users based on their emotional state imply the collection and use of behavioral biometric identifiers.[312] This raises concerns under state laws like BIPA: did the smart speaker user give informed consent for their voiceprint to be transferred to a third party?[313] Additionally, now that the third party has this recording, will they be able to keep it safe from data breaches?[314] Voiceprints can also lead to inferences about the user's sensitive physical information, like their age and health, and psychological information like mood.[315]

Voiceprint biometric identifiers are one example of behavioral biometrics used in advertising.[316] The collection of a consumer's response when exposed to certain advertisements helps companies further tailor ads like the smart screen coolers in *Roberts v. Cooler Screens Inc.*[317] The cooler screens detect emotional responses to the advertisements shown.[318] While the screen and the program powering it may not get a response the first few times a consumer interacts with the cooler, it continues to learn until eventually, the screen is unconsciously influencing the consumer's purchase.[319] The utilization of behavioral biometrics in advertising gives an advertiser an unfair advantage over the unassuming consumer, especially when the consumer is unaware that the corporation is collecting their response to the

307. Umar Iqbal et al., *supra* note 304, at 1.
308. *Id.* at 2.
309. *Id.* at 3.
310. *Id.* at 1.
311. *Id.*
312. *Id.* at 1, 17.
313. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); Umar Iqbal et al., *supra* note 304.
314. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); Umar Iqbal et al., *supra* note 304 at 1.
315. Umar Iqbal et al., *supra* note 304 at 1.
316. *Id.*
317. Kristin Bryan, *supra* note 202; Roberts v. Cooler Screens Inc., No. 2022-CH-01824 (Ill. Cir. Ct. July 1, 2022).
318. *Id.*
319. *Id.*

advertisement.[320]

B. The Property Rights Afforded to Biometric Identifiers in Biometric Privacy Legislation Make Estate Planning the Best Method to Manage Biometric Identifiers Post-Mortem

Classifying biometric identifiers as property rights brings these characteristics within the realm of estate planning and would allow the rights granted by biometric privacy legislation to be asserted on behalf of the deceased.[321] This solution does not require additional legislation; it merely builds on and applies a different interpretation to existing biometric privacy legislation.[322] This subsection will explore other potential solutions, including the pros and cons of each.[323]

1. Copyright Law

Copyright law has been used by estate planners in the past to seal an individual's "original works of authorship fixed in any tangible medium of expression" upon request.[324] Generally, authors or important figures would use this approach to prevent private documents like letters, journals, or unfinished works from being sold or viewed after their death.[325] Though the concept itself is helpful to this Comment's argument that decedents should be able to choose who sees their private information, applying copyright law to biometric identifiers poses several practical problems.[326]

The biometric identifiers at issue are neither tangible nor works of authorship: they are electronic records of different, immutable characteristics corporations collect from their users.[327] Individuals have no autonomy in the creation of their biometric identifiers, and neither is the individual involved in the creation of the electronic record of their biometric identifier.[328] The application of copyright law is therefore difficult because it protects a creator's original works from misuse.[329] Even if copyright was compatible with biometric identifiers, the estate planner would still need a method to get the record of the identifier off of the corporation's server where it is kept to

320. Umar Iqbal et al., *supra* note 304, at 2–3.
321. *See supra* notes 234–36 and accompanying text.
322. *See* discussion *supra* Part II.
323. Elizabeth D. Barwick, *All Blogs Go to Heaven: Preserving Valuable Digital Assets Without the Uniform Fiduciary Access to Digital Assets Act's Removal of Third Party Privacy Protections*, 50 GA. L. REV. 593, 599–600 (2016).
324. 17 U.S.C. § 102(a).
325. *See* Barwick, *supra* note 324, at 595–96.
326. *Id.*
327. Wong, *supra* note 68.
328. *Id.*
329. Barwick, *supra* note 324.

retroactively seal the deceased's information.[330]

2. Posthumous Right to Privacy and The Right of Publicity

Asserting the privacy rights on behalf of a decedent seems to be the most obvious and workable solution to this problem.[331] There is a statutory precedent that implies the existence of a posthumous right to privacy in HIPAA and FOIA.[332] While these two statutes have the effect of protecting the privacy rights of the deceased, the stated purpose is to protect the security rights of the decedent's survivors.[333] Additionally, judicial precedent and common law have established that a cause of action asserting privacy rights on behalf of another will not work.[334] Consequently, making this solution workable requires new legislation that specifically protects the privacy rights of the dead and would allow a third party to assert these rights on behalf of a decedent.[335]

The right to publicity is often mentioned in conjunction with the issue of the biometric privacy rights of the dead.[336] Theoretically, every person has the right to publicity; however, in litigation, the pleading party must prove that their likeness was worth value before the appropriation.[337] Practically, the right to publicity litigation is mostly reserved for public figures that can quantifiably prove the value of their likeness.[338]

When the right of publicity is applied on behalf of an estate it is usually brought by an estate holder.[339] At this point the estate holder has rights in and effectively owns the decedent's likeness, the estate holder normally sues a third party for making money off the likeness of the deceased.[340] This scenario and cause of action do not fit well with the problems presented here.[341] There is no economic incentive to assert a right of publicity cause of action on behalf of the deceased to restore their biometric identifiers.[342] Additionally, because the right of publicity requires the estate holder to have full control of the deceased likeness, a main concern of this Comment is a decedent's right to protect their privacy from the world, including their

330. Ashley, *supra* note 31.
331. *Id.*
332. 45 C.F.R. § 160.103; 5 U.S.C. § 552.
333. 45 C.F.R. § 160.103.
334. Moore v. Charles B. Pierce Film Enters., Inc., 589 S.W.2d 489, 491 (Tex. App.—Texarkana 1979, writ ref'd n.r.e.).
335. Barwick, *supra* note 324.
336. Ashley, *supra* note 31.
337. *Id.*
338. *Id.*
339. *Id.*
340. Shannon F. Smith, *supra* note 21.
341. Ashley, *supra* note 31.
342. *Id.*

heirs.[343]

3. While It Is Difficult to Assign a Dollar Amount to Biometric Identifiers, That Does Not Imply That the Identifier Does Not Have Value

The ability to assign a quantifiable dollar amount to something is generally a useful way to prove that that an individual has property rights in that thing.[344] However, when it comes to biometric identifiers the assignment of a dollar amount for an individual identifier becomes esoteric.[345] If the value comes from the immutability and uniqueness of the characteristics they may be worth the same amount as a good password manager.[346] From the perspective of corporations however, biometric identifiers were not valuable until they were aggregated into databases the corporation could then mine for data.[347]

The ease and reliability of biometric authentication have made the biometric identification systems market very profitable and is expected to double in size from 2019 to 2024.[348] Despite the value of the market as a whole, there is no specific reported value of an individual biometric identifier.[349] Just like a hospital patient would have a hard time finding someone to pay for their medical chart, an individual would have a hard time finding someone to buy their biometric identifiers.[350] However, the companies that collect and use biometric data did not find them valuable until they were able to aggregate and mine the entire database.[351] Additionally, data privacy legislation violations are commonly penalized by monetary fines.[352] This all goes to show that while there may not be a market for individual biometric identifiers, there is a market for biometric identifiers in the aggregate.[353] State legislatures that have passed biometric data privacy laws agree that biometric data is being collected and marketed and acknowledge the risk of exploitation of this valuable asset in the statement of

343. *See id.*; author's original thought.
344. Ashley, *supra* note 31.
345. *Id.*
346. Author's original thought; *see id.*
347. Appenteng & Gordon, *supra* note 142.
348. *Biometric System Market by Authentication Type (Single-Factor: Fingerprint, Iris, Palm Print, Face, Voice; Multi-Factor), Offering (Hardware, Software), Functionality (Contact, Noncontact, Combined), End User, and Region—Global Forecast to 2024*, MKTS. AND MKTS. (Oct. 2019), https://www.marketsandmarkets.com/Market-Reports/next-generationbiometric-technologies-market-697.html [https://perma.cc/VU8S-JKAK].
349. Ashley, *supra* note 31.
350. *See id.*
351. Appenteng & Gordon, *supra* note 142.
352. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018); TEX. BUS. & COM. CODE ANN. § 503.001.
353. Ashley, *supra* note 31.

intent portions of their legislation.[354]

To function comfortably in today's society, it is almost a prerequisite for individuals to engage with the internet or some form of social media.[355] In exchange for their interaction with these "free" and necessary services, individuals forfeit their unique and valuable biometric data for an indeterminate period.[356] Additionally, even in states that do provide their constituents with some form of protection, the deceased are left out, leaving their biometric identifiers vulnerable to misuse.[357]

C. Biometric Identifiers are More Similar to Digital Assets Governed by the RUFADAA, Than the General Right to Privacy that Lapses on Death

The issue with extending this data security right to the dead is that some jurisdictions with established biometric privacy protections have already declined to extend the protections to the dead.[358] The Attorney General of Texas, Ken Paxton, has claimed that because laws of this kind are intended to protect an individual's privacy, and the right of privacy is purely personal and lapses on death, CUBI protections do not extend to a deceased individual's biometric data.[359] Attorney General Paxton's assertion finds authority in Texas case law denying a relational right to privacy in defamation or libel suits.[360]

While that precedent is still good, the comparison of a relational right to privacy to biometric identifier privacy is flawed in the harm analysis.[361] A defamation suit is brought to redress the injury that manifests itself as a result of untrue statements made by another.[362] The defamed individual must experience some harm for an injury to have occurred.[363] This tort cannot apply to the deceased because they are incapable of feeling the harm.[364] However, biometric privacy laws protect from the unforeseen downstream consequences of the collection and use of an individual's biometric identifiers, and these consequences are the same regardless of whether the individual is alive or dead.[365] Additionally, as the application of behavioral biometrics become more commonplace, the deceased are more at risk of

354. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018); TEX. BUS. & COM. CODE ANN. § 503.001.

355. Barwick, *supra* note 324.

356. *Id.*

357. Ashley, *supra* note 31.

358. Tex. Att'y Gen. Op. No. OR-06114 (2021).

359. *Id.*

360. Moore v. Charles B. Pierce Film Enters., Inc., 589 S.W.2d 489, 491 (Tex. App.—Texarkana 1979, writ ref'd n.r.e.).

361. *Id.*

362. TEX. CIV. PRAC. & REM. CODE ANN. § 73.001.

363. *Id.*

364. Tex. Att'y Gen. Op. No. OR-06114 (2021).

365. *See* discussion *supra* Section III.A.

forfeiting private information that can be collected from these identifiers.[366] Therefore, a better comparison is that of biometric identifiers and digital assets governed by the RUFADAA.[367]

The RUFADAA considers the decedent's right to privacy, letting them decide who among their heirs can access their digital assets and electronic communications.[368] Effectively, the RUFADAA recognizes that digital assets and stored electronic communications are private and provides a posthumous right to privacy for the deceased who utilize the protections of this act.[369] Similarly, this Comment argues that the rights provided by biometric data privacy laws give the owner of biometric identifiers property rights, and therefore, a similar ability to dictate what happens to their unique identifiers after death.[370]

The drafters of the RUFADAA not only acknowledged that digital assets like email accounts had value and could be considered property, but that the communications within contained private information the deceased could choose whether to share with their descendants.[371] This concept is similar to the practice of decedents, often famous authors, sealing their private documents in their will.[372] By sealing their private documents, the decedent prohibits even their heirs from accessing and distributing the information contained within.[373]

Although sealing private documents is rooted in copyright law, there is still the effect of creating posthumous privacy.[374] In a similar manner, dictating what happens to biometric identifiers after a person's death gives the decedent control over private information that can be collected from the identifier as well as the identifier itself.[375] A decedent would be able to choose to give permission to use their biometric identifiers.[376] This is similar to a grandmother giving her family permission to use her voiceprint so that an Amazon Alexa could read to her grandchild with her voice.[377] In this case, the grandchild is able to hold onto the memories of their grandmother but in a way the grandmother consented to.[378]

The process of drafting the RUFADAA was a long one and included the preliminary Uniform Fiduciary Access to Digital Assets Act (UFADAA).[379]

366. Stein, *supra* note 73.
367. Revised Unif. Fiduciary Access to Digit. Assets Act § 3.
368. *Id.* § 4.
369. *Id.* § 3.
370. Author's original thought.
371. Revised Unif. Fiduciary Access to Digit. Assets Act § 6.
372. Barwick, *supra* note 324, at 622–23.
373. *Id.*
374. *Id.*
375. *Id.*
376. *Id.*; Author's original thought.
377. Allyn, *supra* note 21.
378. *Id.*; Author's original thought.
379. Barwick, *supra* note 324, at 600.

The UFADAA struggled in finding a balance between allowing the beneficiaries of the decedent's estate access to online communication and digital assets to which they are due, and protecting the privacy of the deceased and the living people they communicated with.[380] On one side, the decedent's family cited the ease of estate administration to justify unlimited access to a decedent's digital assets.[381] To preserve the decedent's privacy, however, the RUFADAA implemented a third party to sift through these assets and communications allowing the family access only to those assets that relate to estate administration while withholding private communications.[382]

This same process should be implemented for a decedent's biometric identifiers.[383] Some biometric identifiers like fingerprints are physical characteristics that may not warrant privacy concerns.[384] Behavioral biometric identifiers, however, have the potential to reveal personal information like sexual preference.[385] Bringing biometric identifiers into estate planning would allow a decedent to keep private information private while still allowing their survivors to make sure the identifiers themselves are properly maintained by the corporations that collect them.[386]

The administration of a decedent's estate should not justify a deep dive into their biometric identifiers and all the information that can be collected from the identifiers.[387] Classifying biometric identifiers as property due to the rights afforded to the individual in biometric privacy legislation would narrow the scope of access and control of biometric identifiers.[388] The access could be restricted to a decedent's specifications in their will, or if intestate, only to the control necessary to ensure cyber criminals are not abusing the identifiers.[389]

1. Reliance on the Classification of Biometric Identifiers as Digital Assets to Bring Them Within the Scope of the RUFADAA May be Insufficient

The RUFADAA extends the power of a fiduciary to include the management of an individual's digital assets when the individual loses the ability to manage those assets.[390] The RUFADAA balances the privacy rights

380. *Id.* at 597.
381. *Id.*
382. Revised Unif. Fiduciary Access to Digit. Assets Act § 6.
383. Author's original thought; *see* Kugler, *supra* note 67, at 117.
384. Kugler, *supra* note 67, at 117.
385. Stein, *supra* note 73.
386. Author's original thought.
387. Barwick, *supra* note 324, at 623.
388. Author's original thought; *see* Barwick, *supra* note 324, at 623; Revised Unif. Fiduciary Access to Digit. Assets Act § 6.
389. *See* Revised Unif. Fiduciary Access to Digit. Assets Act § 6.
390. *Id.* § 3.

of the decedent by requiring the original user to consent to fiduciary access via a will or some other record.[391] The RUFADAA has been passed in forty-seven states and indicates that most states recognize a gap in estate planning law that had left digital assets unaccounted for.[392]

Digital assets are defined in the RUFADAA as "an electronic record in which an individual has a right or interest."[393] As defined, biometric identifiers would classify as digital assets in states like Illinois, California, and Texas which already have laws in place that recognize an individual's right to control their biometric identifiers.[394] With the inevitable passage of either a comprehensive federal data privacy framework or legislation adopted by the individual states creating property rights in biometric identifiers, combined with the RUFADAA, the solution proposed by this Comment seems obsolete.[395]

The difficulty with relying on the combination of the RUFADAA and federal data privacy legislation is the difficulty of classifying biometric identifiers as digital assets.[396] This difficulty stems from whether the value of a biometric identifier comes from its intrinsic uniqueness and immutability, or whether the value comes from how companies have developed the software to collect, aggregate, and mine the biometric data of all their users (i.e., the electronic record itself).[397] If the underlying asset is the biometric identifier itself then it would be difficult to define as a digital asset, as per the RUFADAA, "[t]he term [digital asset] does not include [the] underlying asset or liability unless the asset or liability is itself an electronic record."[398] Different interpretations of digital assets by different jurisdictions and courts could lead to different outcomes that would nullify the goal of a comprehensive federal framework.[399]

2. While the RUFADAA Itself May Not be the Correct Solution, a Uniform Act Left to Individual State Adoption Might

Illinois set the scene for biometric privacy legislation in 2008.[400] While

391. *Id.* § 6.

392. *Fiduciary Access to Digital Assets Act, Revised*, UNIF. L. COMM'N, https://www.uniformlaws.org/committees/community-home?attachments=&communitykey=f7237fc4-74c2-4728-81c6-39a91ecdf22&libraryentry=e9f85d7c-13f3-4918-a000-0abe7fab7f62&pageindex=0&pagesize=12&search=&sort=most_recent&viewtype=card (last visited Oct. 18, 2022) [https://perma.cc/F858-64P3].

393. Revised Unif. Fiduciary Access to Digit. Assets Act § 2007.002.

394. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018); TEX. BUS. & COM. CODE ANN. § 503.001.

395. Bellamy, *supra* note 104.

396. Revised Unif. Fiduciary Access to Digit. Assets Act § 2(10).

397. Ashley, *supra* note 31.

398. Revised Unif. Fiduciary Access to Digit. Assets Act § 2(10).

399. *See* 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); *see* CAL. CIV. CODE § 1798.100 (West 2018); *see* TEX. BUS. & COM. CODE ANN. § 503.001.

400. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).

technology is beginning to move past the protections established in the original act, BIPA itself is an important piece of legislation that could easily be updated to include behavioral biometrics.[401] As more states have begun to implement their respective biometric privacy laws—all with different levels of protection and nuance—a uniform act for biometric data is worth considering.[402]

A uniform act would be beneficial to individuals and corporations alike.[403] Individuals in states that are focused on other issues would be able to protect their biometric identifiers without the state legislature having to take the time to draft biometric privacy legislation from scratch.[404] Local companies would be able to tailor their operations to meet the requirements of that state.[405] National corporations would also have an expectation of the limit to their ability to utilize their consumer's biometric identifiers.[406] Both types of corporations would be able to lobby the state legislature to customize the law for that state, while individuals would go into the drafting process with an expectation of a minimum for protections and be able to negotiate for more if needed.[407]

The drafting of a uniform act would also allow the deceased to get the representation regarding their biometric identifiers to fill the gaps in the current laws.[408] Either way, the drafting of a uniform code affords the affected parties the opportunity to advance their interests.[409] Currently, the country is on track for the adoption of fifty different laws that accomplish the same purpose; a uniform act may avoid this potential headache.[410]

D. Additional Counter-Arguments

The extension of the property rights created by biometric data legislation to the realm of estate planning would prevent a wave of legislation rather than create it.[411] As mentioned above, data privacy legislation maintains its efficacy by acting as an incentive for companies to comply with the legislation's standards like all laws.[412] Postmortem identity theft and

401. *See* Bryan et al., *supra* note 318.
402. DiRago, *supra* note 13.
403. Timothy Gatton, *Restatements of the Law and Uniform Laws: Uniform Laws & Model Acts; Introduction and Explanation,* OKLA. CITY UNIV. SCH. OF L. 1, 1 (last updated Sept. 12, 2022), https://libguides.okcu.edu/c.php?g=225285&p=1492987 [https://perma.cc/NC3T-JRPW].
404. *See id.*
405. *See id.*
406. *See id.*
407. *See id.*
408. *See id.*
409. *See* Gatton, *supra* note 403.
410. DiRago, *supra* note 13.
411. Prescott, *supra* note 104.
412. *See* discussion *supra* Part III.

misuse of biometric identifiers will spawn litigation either way.[413] From the perspective of a judge or another member of the court, it would be easier to adjudicate a matter addressed by the legislature than an esoteric matter of first impression with differing legislation and holdings that vary state to state.[414]

The manner in which corporations usually breach their duty to obtain informed consent from their consumers before transferring their biometric data to third parties lends itself to class action lawsuits rather than individual suits.[415] States could choose to limit this cause of action to class action suits.[416] This would prevent the backlog of the judicial system while giving individuals all the advantages of class action suits.[417]

Moore v. Regents of the University of California establishes that once a person parts with their genetic information, the information is considered abandoned property and the person loses all rights to it.[418] This may lead to a claim that the holding in *Moore* nullifies this Comment's argument that biometric information should be considered personal property, however, the context for *Moore* and the collection and use of biometric data is different.[419]

In *Moore*, the Supreme Court of California held that Moore lost his rights to his genetic information for two reasons.[420] First, socially important medical research would be hindered if researchers had to confirm that every cell line they used came from a willing donor, discouraging research.[421] Second, the court found that Moore's cells were similar to a donated organ.[422] California statutes do not consider personal property interests for donated organs because researchers only discover the potential value after experimentation or research which can take months or years.[423]

Biometric identifiers are different from cells because ensuring an individual's privacy or preventing the misuse of the identifier hinders no socially important research.[424] Additionally, the individual biometric identifier is not worth anything; to compare it to potentially groundbreaking medical research is to take the importance of one biometric identifier to a company out of perspective.[425]

---

413. *Are You Ready for the BIPA Tsunami? The New Wave of Biometric Statutes*, LOCKE LORD (July 2020), https://www.lockelord.com/newsandevents/publications/2022/07/are-you-ready-for-the-bipa-tsunami [https://perma.cc/QDN6-2KKK].

414. *See id.*

415. *See* discussion *supra* Section II.C.

416. FED. R. CIV. P. 23.

417. *See id.*

418. Moore v. Regents of Univ. of Cal., 249 Cal. Rptr. 494, 498 (Cal. Dist. Ct. App. 1988).

419. *See id.* at 499.

420. *Id.* at 505, 508.

421. *Id.* at 508.

422. *Id.* at 505.

423. *Id.* at 508.

424. *Id.*

425. *Id.*

The efficacy of survivability statutes to redress violations of the deceased's biometric identifiers is not sufficient to adequately protect their interests.[426] Survivability statutes require the injured party to be harmed while still alive.[427] The cause of action asserted on behalf of the deceased is merely a continuation of the cause of action the injured party could have asserted while living.[428] This factor limits the application of state survivability statutes to violations of biometric privacy legislation that occurred while the injured party was still alive.[429]

E. Practical Considerations for Change

The potential benefits of biometric authentication technology merit corporate investment in the market and legislation protecting consumers.[430] As complex password managers and two-factor authentication become more commonplace, consumers and corporations alike are looking for easy secure ways to sign into various services.[431] The state and federal legislatures alike recognize the tone of this undercurrent and the potential dangers of biometric identifiers.[432] In response, they have either passed or proposed data privacy laws addressing biometric data.[433]

Corporations themselves also recognize the need for their customers to feel secure that their biometric identifiers will not be misused.[434] In attempting to address consumer concerns, however, corporations that operate in the United States have to deal with at least four different state statutes—all of which define biometric identifiers in different ways, have different infraction penalties, and have different methods of enforcement.[435] Introducing the biometric rights of the dead into this environment will certainly create more problems in the short term.[436] In the long term, however, corporations avoid the headache of having to comply with multiple standards if there is a national standard.[437] Additionally, corporations will be less susceptible to a data breach via postmortem identity theft.[438]

Moving forward it will be important for state legislatures to balance the need to protect the privacy of their constituents with the need of the

426. TEX. CIV. PRAC. & REM. CODE ANN. § 71.021.
427. *Id.*
428. *Id.*
429. *Id.*
430. Korolov, *supra* note 7.
431. *Id.*
432. *See* discussion *supra* Part I.
433. Korolov, *supra* note 7.
434. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
435. PERKINS COIE, *supra* note 47.
436. Prescott, *supra* note 104.
437. PERKINS COIE, *supra* note 47.
438. Korolov, *supra* note 7.

corporation and consumers alike to secure data with biometric identifiers.[439] The fact of the matter is that biometric identifiers and authentication provide a secure and quick method to keep devices and documents safe.[440] The speed and efficiency of biometric authentication gives corporations utilizing this form of authentication an advantage over those corporations that use other secure methods like two-factor authentication.[441]

Corporations may need to be happy with utilizing only this advantage of biometric data and stay away from the more invasive uses for the data.[442] Undoubtedly, progress in the collection of behavioral biometrics will continue because it is an interesting intersection of human characteristics and technology.[443] Hopefully, keeping a safe distance from some of the more nefarious applications of this data will be a priority.[444] One of the main dangers of this technology is that the majority of Americans do not know the collection of their biometric identifiers is taking place.[445] As the technology continues to develop, people will become more aware of the consequences of their actions when they allow their Instagram or Amazon Alexa to share their facial geometry or voice-print data with a third party.[446]

Many corporations already employ protections for the biometric data they collect.[447] There are multiple methods by which corporations can alter the biometrics they use to authenticate users to protect that user's biometric identifiers.[448] "Cancelable biometrics" is a practice by which a company uses a noninvertible transformation to make a new biometric template they would then use to authenticate users.[449]

For example, say an employer wants to utilize facial geometry for their employees to clock in.[450] As the company created the biometric template, they would transform the facial geometry of the employee to create a cancelable biometric that does not belong to the person.[451] Essentially, they take a picture of the employee's face, scan it like a Snapchat filter, and use that biometric template as verification.[452] This method does not seem very secure.[453] The initial record of the employee's face still exists, and every time

439. *See id.*
440. *See id.*
441. *See id.*
442. *See* Teale, *supra* note 288.
443. Tsai, *supra* note 114.
444. Stein, *supra* note 73.
445. Teale, *supra* note 288.
446. *Id.*
447. Vishal M. Patel et al., *Cancelable Biometrics: A Review,* 32 IEEE SIGNAL PROCESSING MAG. 54, 54–56 (2015).
448. *See id.*
449. *See id.* at 55–61.
450. *See id.*
451. *See id.*
452. *See id.*
453. *See id.*

the employee goes to authenticate their identity, a record of their face is created.[454]

Another method companies use to secure their consumer's biometric identifiers is a watermark system.[455] A watermark system means that the biometric identifiers stored in a database have some sort of watermark that makes them only work with a version of the authentication software associated with that database.[456] Even if the biometric identifiers are transferred to a third party, the watermark renders them useless.[457]

IV. CONCLUSION

Advances in technology used for the collection and application of biometric identifiers, in conjunction with the introduction of legislation protecting these characteristics, put the biometric data of the deceased in a unique position.[458] On one side, state legislatures have recognized that the immutability and potential for unforeseen consequences warrant protections for their constituency's biometric identifiers.[459] On the other side, the companies collecting and aggregating biometric identifiers have recognized the value of biometric identifiers in various contexts ranging from authentication to practical application in the Metaverse.[460] Cybercriminals also value biometric identifiers as a means to facilitate data breaches.[461] This leaves the biometric identifiers of the deceased vulnerable to misuse by corporations and fraudsters alike.[462] Some state legislatures included the right to control and the right to private action in their respective state laws for a reason.[463] Because the deceased can potentially suffer the same harms of repeated fraud as well as unforeseen downstream consequences, estate planners should step in to fill the gap and protect the biometric data of the dead.[464] The right of control and right to private action are both rights assigned to property; it is within an estate planner's jurisdiction to include biometric identifiers in a will.[465]

---

454. *Id.*
455. *Id.*
456. *Id.*
457. *Id.*
458. *See* discussion *supra* Section I.B.
459. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018); TEX. BUS. & COM. CODE ANN. § 503.001.
460. *See* discussion *supra* Section I.B.
461. *See* discussion *supra* Section I.B.
462. *See* discussion *supra* Section I.B.
463. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008); CAL. CIV. CODE § 1798.100 (West 2018); TEX. BUS. & COM. CODE ANN. § 503.001.
464. *See* discussion *supra* Part II.
465. *See* discussion *supra* Part II.