North Carolina Banking Institute

Volume 24 | Issue 1 Article 14

3-1-2020

Biometrics and Banking: Assessing the Adequacy of the Gramm-Leach-Bliley Act

Meredith E. Bock

Biometrics and Banking: Assessing the Adequacy of the Gramm-Leach-Bliley Act

I. INTRODUCTION

Massive data breaches in the banking industry are commonplace, exposing the personal information of millions of consumers.[1] In response to these breaches, banks are incorporating biometrics into their security systems in order to better protect consumer information.[2] Biometric technology involves using individuals' physical characteristics as a form of identity verification[3] and has been widely implemented through features such as fingerprint scanning in mobile banking.[4] Significant development is expected over the next few years as the traditional PIN and password become less secure and banks make efforts to update their security measures.[5]

Although biometric technology offers increased security, there is significantly more risk involved in collecting and storing this information because banks are gathering data on immutable characteristics of

---

1. *See, e.g.*, *Information on the Capital One Cyber Incident*, CAPITAL ONE, https://www.capitalone.com/facts2019/ [https://perma.cc/Y2EG-GMTF] (last updated Sept. 23, 2019, 4:15 PM) ("[The Capital One's Cyber Breach] affected approximately 100 million individuals in the United States and approximately 6 million in Canada."); *Equifax Data Breach*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/data-breach/equifax/ [https://perma.cc/VY98-FEKT] (last visited Nov. 13, 2019) ("[T]he sensitivity of the personal information held by Equifax and the scale of the problem makes this breach unprecedented.").

2. *See* Allison Arthur & Bethany Frank, *Five Examples of Biometrics in Banking*, ALACRITI (May 8, 2019), https://www.alacriti.com/biometrics-in-banking [https://perma.cc/YH4D-W7D7] (providing multiple examples of the implementation of biometric technologies in banking today, including fingerprint scanning, voice authentication, and a biometric payment card).

3. *Behavioral Biometrics and Biometrics in Payment Cards: Beyond the PIN and Password*, GEMALTO, https://www.gemalto.com/financial/inspired/behavioral-biometrics [https://perma.cc/326G-2JLT] (last updated Sept. 30, 2019) [hereinafter *Behavioral Biometrics and Biometrics in Payment Cards*].

4. *See* Arthur & Frank, *supra* note 2 (identifying fingerprint verification as one of the many ways banks incorporate biometrics into their security systems).

5. *See* Jim Marous, *The Biometric Future of Banking*, THE FIN. BRAND (Oct. 3, 2016), https://thefinancialbrand.com/61449/biometric-banking-password-trends/ [https://perma.cc/V487-UZ43] (discussing the weaknesses of passwords and potential alternatives, including the use of biometric data).

consumers.[6] In the event of a breach, consumers' most intimate information, including data like fingerprints and retinal scans, would be exposed.[7] Despite this increased risk, the Gramm-Leach-Bliley Act's ("GLBA") privacy provisions, setting out requirements for the protection of consumer information by financial institutions, do not contain specific parameters for the collection of biometric data.[8] Conversely, other legislatures recognized the sensitivity of biometric information and enacted statutes to protect it, including several U.S. states and the European Union.[9] As more entities begin to recognize the need for increased security measures for biometric data, the GLBA should be updated to incorporate similar provisions.[10]

This Note assesses the adequacy of the GLBA in protecting biometric data by comparing it to statutes that contain varying levels of biometric-specific language. This Note proceeds in six parts. Part II explains current biometric technologies and their actual and potential uses in the banking industry.[11] Part III analyzes the provisions of the GLBA and additional regulations pursuant to the GLBA set forth by the Consumer Financial Protection Bureau ("CFPB").[12] Part IV provides an overview of current legislation, including statutes containing special parameters for the collection and use of biometric information, and compares those statutes with others that do not contain such parameters.[13] Part V examines the need for implementation of biometric specific language into the GLBA in order to adequately protect consumer data.[14]

---

6. Stacy Cowley, *Banks and Retailers Are Tracking How You Type, Swipe, and Tap*, N.Y. TIMES (Aug. 13, 2018), https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html [https://perma.cc/DG5H-R6MB].

7. *Behavioral Biometrics and Biometrics in Payment Cards*, *supra* note 3.

8. *See* Gramm-Leach Bliley Act ("GLBA") § 509, 15 U.S.C. § 6809(4) (2018) (containing no specific references to the inclusion of biometric information under the definition of Nonpublic Personal Information).

9. Shinabarger & Swanson, *Several States Considering Laws Regulating the Collection of Biometric Data*, WINSTON AND STRAWN, LLP (Feb. 6, 2019), https://www.winston.com/en/privacy-law-corner/several-states-considering-laws-regulating-the-collection-of-biometric-data.html [https://perma.cc/6QLM-WK9E]; EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1 [hereinafter *GDPR*].

10. *See* Shinabarger & Swanson, *supra* note 9 (identifying a number of states with pending, proposed, or enacted legislation regarding the regulation of biometric information).

11. *See infra* Part II.

12. *See infra* Part III.

13. *See infra* Part IV.

14. *See infra* Part V.

Part VI recommends changes to the GLBA that would reflect the need for increased protection of this sensitive data.[15]

II. CAPABILITIES OF BIOMETRIC TECHNOLOGIES

Biometric technology is a rapidly evolving field involving the identification of an individual through physical or behavioral characteristics.[16] Most consumers are familiar with the use of physical biometrics, such as fingerprint scanning capabilities often used by cell phone manufacturers.[17] Another emerging area of biometrics is the collection of behavioral data, including tracking keystrokes and handwriting.[18] Banks are implementing both physical and behavioral biometrics in an attempt to upgrade their security.[19]

Physical biometric data uses tangible characteristics to verify a user's identity.[20] Although many different physical features can be used to authenticate an individual, the most common technologies today are fingerprint scans, facial recognition, retinal scans, and DNA collection.[21] Regardless of the form of physical biometric information being collected, the collection process is the same: enrollment, where an image or recording of a specific trait is captured; storage, where this image is translated into code; and comparison, where the system compares a provided trait with stored information to determine if there is a match.[22] For example, facial recognition technology scans an image of a face and

15. *See infra* Part VI.

16. *Biometrics: Authentication and Identification (Definition, Trends, Use Cases, Laws and Latest News) – 2020 Review*, GEMALTO, https://www.gemalto.com/govt/inspired/biometrics [https://perma.cc/EFB4-DENG] (last updated Jan. 17, 2020) [hereinafter *Biometrics: Authentication and Identification*] ("This is the basic principle of biometrics: to identify a person based on certain unique characteristics.").

17. *See* Calvin Hsieh, *Fingerprint-on-Display Module Market to Grow Nearly 600 Percent in 2019*, IHS MARKIT (May 14, 2019), https://technology.ihs.com/614074/fingerprint-on-display-module-market-to-grow-nearly-600-percent-in-2019 [https://perma.cc/G9NG-CTXM] ("[D]isplay fingerprint sensing technology . . . has been optimized by suppliers and widely adopted by smartphone brands . . . .").

18. *Biometrics: Authentication and Identification*, *supra* note 16.

19. *See* Arthur & Frank, *supra* note 2 (identifying the collection of behavioral biometric data by RBS as well as several examples of physical biometric information).

20. *Biometrics: Authentication and Identification*, *supra* note 16.

21. *Id.*

22. Tracy V. Wilson, *How Biometrics Works*, HOWSTUFFWORKS, https://science.howstuffworks.com/biometrics.htm [https://perma.cc/9JF4-E4CC] (last visited Feb. 6, 2020).

matches specific data points, such as the distance from the nose to the lip, to create a "facial signature."[23] This signature is then converted into a unique numerical code, which is stored either within a device, as with facial recognition technology in smartphones, or in an encrypted database.[24] The next time the user scans his or her face, the system compares the generated code with those previously stored in the system and if a match is found, the user's identity is authenticated.[25]

Physical biometrics are especially prevalent in law enforcement and border control in the form of fingerprint collection and scanning.[26] For example, the Department of Homeland Security introduced an "e-passport" in October 2006, which includes a chip containing the personal information traditionally found on a passport, as well as a biometric identifier, like a fingerprint, and a virtual photograph of the individual.[27] Cell phone companies also implemented fingerprint scanning and facial recognition technologies as part of their security features.[28] Many other companies, including financial institutions, use this technological infrastructure to provide customers with biometric login options as well.[29]

Although physical biometric data is currently the most widely used, behavioral biometric technologies are also rapidly evolving.[30] Unlike physical biometrics, behavioral biometrics analyze behaviors

---

23. Hussain Kanchwala, *How Does Facial Recognition Work?*, SCIENCE ABC (Feb. 9, 2019), https://www.scienceabc.com/innovation/facial-recognition-works.html [https://perma.cc/AVS3-L25U].

24. *Id.*

25. *Id.*

26. *Biometrics: Authentication and Identification*, *supra* note 16.

27. *e-Passports*, DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/e-passports [https://perma.cc/U4W9-VPKH] (last updated Sept. 20, 2019).

28. *See* AppleInsider Staff, *Apple Announces 'Touch ID' Fingerprint Scanner for iPhone 5S*, APPLE INSIDER (Sept. 10, 2013, 11:05 AM), https://appleinsider.com/articles/13/09/10/apple-announces-touch-id-fingerprint-scanner-for-iphone-5s [https://perma.cc/BG52-G2GQ] (introducing the fingerprint scanning feature found on the iPhone 5S, the first generation to contain such a scanner).

29. *See* Annie Dossey, *Biometric Authentication For Convenience in Mobile Banking: What Banks Need to Know*, CLEARBRIDGE MOBILE (Jan. 8, 2019), https://clearbridgemobile.com/biometric-authentication-for-mobile-banking/ [https://perma.cc/TCZ7-G5U9] ("Apple got the ball rolling for biometric authentication with Touch ID, and as a result, financial institutions are embracing the fingerprint login for mobile banking apps.").

30. *See* INT'L BIOMETRICS AND IDENTITY ASS'N, BEHAVIORAL BIOMETRICS 2 (2017), https://www.ibia.org/download/datasets/3839/Behavioral%20Biometrics%20white%20 [https://perma.cc/QT84-JSXQ] (describing the utility of behavioral biometric technologies and the growing trend toward using said technologies).

such as keystrokes, handwriting, and navigation of a webpage to verify a user's identity.[31] The technology tracks the subconscious behaviors of a user during the course of an activity to create a unique profile that is virtually impossible to replicate.[32] This data is collected primarily through the use of specialized software or, in the case of data collected from smartphones, through sensors that already exist on the device.[33] It is then analyzed by artificial intelligence technology, which identifies minute patterns and creates a profile of micro-habits that are completely unique to the individual.[34] Behavioral biometric data is often used in fraud detection within companies and can evaluate security risks within the company by analyzing the behavior patterns of employees who access sensitive information.[35]

In recent years, many large banks have implemented both physical and behavioral biometric technologies into their security mechanisms, including fingerprint scanning in mobile banking interfaces, as previously mentioned.[36] Increased security concerns, coupled with consumer demands for increased speed and convenience, drove banks to first develop more innovative solutions involving physical biometrics.[37] For example, Wells Fargo offers commercial clients the option of using retinal scans taken from the camera of a user's phone, in addition to allowing fingerprint scanning for both commercial and personal accounts.[38] Similarly, Barclays implemented the use of finger vein analysis, which is comparable to fingerprint scanning but involves scanning the vein patterns in an individual's finger.[39] Also, Royal Bank of Scotland ("RBS") has incorporated biometrics into its security infrastructure in a number of ways, including in the creation of a biometric payments card by its affiliate, NatWest.[40] This payment card

31. *Id.* at 3.
32. *Id.*
33. *Id.*
34. *Id.*
35. *Id.* at 5.
36. *Biometrics: Authentication and Identification*, *supra* note 16.
37. *See Behavioral Biometrics and Biometrics in Payment Cards, supra* note 3 ("[M]easures to protect end-users from hacking and fraud have to be delivered without jeopardizing the consumer experience.").
38. Kristen Mosbrucker, *The Eyes Have It: Wells Fargo Bringing Smartphone Retinal Scanning to Tech-Savvy SA*, SAN ANTONIO BUS. J. (May 3, 2016, 2:47 PM), https://www.bizjournals.com/sanantonio/news/2016/05/03/the-eyes-have-it-wells-fargo-bringing-smartphone.html [https://perma.cc/YN4L-9X29].
39. Arthur & Frank, *supra* note 2.
40. *Id.*

has a fingerprint scanner on the card itself, which is used to verify payments in place of the traditional PIN.[41] Citibank has integrated voice authentication in its call centers, which offers a mix of physical and behavioral biometric data collection that recognizes inflection and other speech patterns as an alternative to providing identifying information over the phone.[42]

In addition to using physical biometric data, banks like RBS are also integrating behavioral biometric technology into their fraud detection systems and have already reaped the benefits.[43] In one instance, the RBS behavioral biometric system indicated that a particular consumer had the tendency to enter the consumer's numerical password using the number pad on the side of the keyboard.[44] When a hacker attempted to access this individual's account using the row of numbers across the top of the keyboard, the bank recognized this inconsistent behavior and immediately sent a fraud alert.[45]

There is an undeniable trend toward the implementation of biometric technologies in financial institutions.[46] Although there are demonstrated benefits to using this technology to increase account security, there are also significant privacy concerns associated with the collection of biometric information.[47] A number of legislative bodies, including the European Union and several states in the United States, have recognized these concerns and implemented forms of biometric-specific legislation as a result, but these concerns are not reflected in the GLBA.[48]

---

41. Press Release, Royal Bank of Scot., NatWest to Launch Biometric Payments Card Pilot (Mar. 22, 2019) https://www.rbs.com/rbs/news/2019/03/natwest-to-launch-biometric-payments-card-pilot.html [https://perma.cc/Y27Z-FE6P].

42. Arthur & Frank, *supra* note 2.

43. *See* Cowley, *supra* note 6 (describing an attempted data breach that was avoided because discrepancies in the behavioral biometric profile indicated that the account was being hacked).

44. *Id.*

45. *Id.*

46. *See* Arthur & Frank, *supra* note 2 (illustrating a number of ways banks have begun implementing biometric technologies); s*ee also* Cowley, *supra* note 6 (explaining how behavioral biometrics detected fraudulent activity on the account of an RBS account holder).

47. *See* Cowley, *supra* note 6 ("Privacy advocates view the biometric tools as potentially troubling . . . .").

48. *See* Shinabarger & Swanson, *supra* note 9 (compiling information about currently pending state legislation on biometric data use). Legislation has also been introduced at the federal level through two primary pieces of legislation. The first is the Commercial Facial Recognition Privacy Act, which would "prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user, and for other purposes." Commercial Facial Recognition Privacy Act of 2019, S.

III. THE GRAMM-LEACH-BLILEY ACT

The GLBA governs the protection of customer information collected by financial institutions, creating an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[49] "Nonpublic personal information" is defined as "personally identifiable financial information," and includes information used to obtain a product, service, or information gained from or in connection with a transaction.[50] This includes personal information such as a customer's "name, address, income, [or] Social Security number."[51] The GLBA requires that financial institutions provide notice of their privacy policies to consumers and maintain adequate standards to ensure that consumer information remains secure.[52] Further, although the GLBA permits financial institutions to provide this information to nonaffiliated third parties, it requires that financial institutions give consumers notice and the opportunity to opt out of these disclosures.[53]

Protections outlined in the GLBA were enhanced through the creation of the Consumer Financial Protection Bureau ("CFPB"), a bureau within the Federal Reserve System created as part of the Dodd-Frank Act ("Dodd-Frank") to further ensure that consumer information was being adequately protected.[54] The CFPB enacted Regulation P,

---

847, 116th Cong. (2019). The second is the Consumer Online Privacy Rights Act, or COPRA, "[prohibits] harmful data practices, . . . creates new data security protections, . . . [and] creates new enforcement and accountability measures to protect all consumers." Press Release, Sen. Maria Cantwell, Consumer Online Privacy Rights Act of 2019 (Nov. 26, 2019), https://www.cantwell.senate.gov/imo/media/doc/COPRA%20One-Pager.pdf [https://perma.cc/5VLG-FJE5]. However, this second piece of legislation does not apply to banks and financial institutions. Alysa Zeltzer Hutnik & Khouryanna DiPrima, *A National Federal Privacy Law? Check Out COPRA, The Most Comprehensive Privacy Bill Introduced Yet*, KELLEY DRYE (Dec. 2, 2019), https://www.adlawaccess.com/2019/12/articles/a-national-federal-privacy-law-check-out-copra-the-most-comprehensive-privacy-bill-introduced-yet/ [https://perma.cc/U9GD-98CC].

49. Gramm-Leach Bliley Act ("GLBA") § 501, 15 U.S.C. § 6801(a) (2018).

50. 15 U.S.C. § 6809(4); FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT 4 (2002), https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf [https://perma.cc/S5XJ-SEAL].

51. FED. TRADE COMM'N, *supra* note 50, at 4.

52. 15 U.S.C. § 6803(a).

53. *Id.* § 6802(a)–(b).

54. Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") § 1011, 12 U.S.C. § 5491 (2018).

which implements the privacy provisions in the GLBA and governs the use of personal information collected by banks and other financial institutions.[55] Specifically, Regulation P "requires a financial institution to provide notice to customers about privacy policies and practices," identifies when disclosure to non-affiliated third parties is permissible, and allows consumers to "opt-out" of said disclosure.[56] Although GLBA and Regulation P were not enacted to protect biometric data specifically, they set forth guidelines for the use of consumer information in general.[57]

Through Dodd-Frank, the CFPB was created as the agency to "regulate the offering and provision of consumer financial products and services under the federal consumer financial laws," which include the privacy provisions of the GLBA.[58] The CFPB promulgated Regulation P pursuant to the GLBA privacy provisions to ensure the adequacy of the security measures implemented by financial institutions.[59] Regulation P describes the annual consumer notices that must be provided by financial institutions and includes a description of the information that may be provided to nonaffiliated third parties.[60] These guidelines also set out a process that must occur before a bank may provide nonpublic personal information to a nonaffiliated third party.[61] Notice must be given to consumers informing them that their information may be disclosed to a third party and such notice must contain an adequate opportunity to "opt-out."[62] Barring any exception under Regulation P, a financial institution may only release nonpublic personal information to nonaffiliated third parties after a consumer has failed to "opt-out."[63]

---

55. Privacy of Consumer Financial Information (Regulation P); 12 C.F.R. § 1016.1 (2018).

56. *Id.* §§ 1016.1(a)(1)–(3).

57. *See* Dodd Frank § 1093(1), 15 U.S.C. § 6801 (2018) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."); *see also* 12 C.F.R. § 1016.10 (outlining additional specific provisions regarding the collection and use of consumer personal information).

58. Dodd Frank § 1002; 15 U.S.C. § 5491(a).

59. 12 C.F.R. § 1016.1(b)(1).

60. *Id.* § 1016.10. "Nonaffiliated third parties" is defined as "any person except your affiliate or a person employed jointly by you and any company that is not your affiliate (but nonaffiliated third party includes the other company that jointly employs the person)." 12 C.F.R. §1016.3(o)(1).

61. 12 C.F.R. § 1016.7.

62. *Id.*

63. *Id.*

The GLBA and CFPB's Regulation P created safeguards for the protection of consumer data.[64] Given the highly sensitive nature of the biometric information collected, there is a question of whether these pieces of legislation do enough to ensure protection of biometric data.[65] Conversely, other entities have faced this issue by enacting biometric-specific legislation, each of which outlines specific precautions when collecting biometric information from a consumer.[66]

IV. THE CURRENT STATE OF BIOMETRIC LEGISLATION

Biometric information is undoubtedly the most personal information that can be collected, and many are skeptical about the adequacy of current legislation to ensure its protection.[67] In response, there has been a recent rise in biometric-specific legislation throughout the United States and the European Union.[68] In the United States, several states have adopted statutes governing the collection and sale of biometric information.[69] In the European Union, similar protections are found in the General Data Protection Regulation (GDPR), including provisions applicable to processing biometric data.[70]

64. *Id.* § 1016.1(a); Gramm Leach Bliley Act ("GLBA") § 501; 15 U.S.C. § 6801(a) (2018).

65. *See Behavioral Biometrics and Biometrics in Payment Cards*, *supra* note 3 ("Consumers will enjoy an even more seamless experience, but the industry must exercise extreme caution when working in this area. Biometric data is arguably the most personal and private data that anyone has. And unlike a password or PIN number, you aren't able to change it. If personal biometric data is compromised or lost, the impact on consumer confidence in the technology could be catastrophic.").

66. *See, e.g.*, Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 25(c) (2019) (governing the collection and use of biometric information in Illinois).

67. *See Behavioral Biometrics and Biometrics in Payment Cards, supra* note 3 (discussing the extremely sensitive nature of biometric information).

68. *See* Shinabarger & Swanson, *supra* note 9 (identifying states with currently enacted or pending legislation regarding the collection, storage, and use of biometric data); *GDPR*, *supra* note 9 (governing the use of consumer information being processed in the European Union).

69. *See, e.g.*, TEX. BUS. AND COM. CODE ANN. § 503.001 (West 2019) (governing the collection, storage, and use of biometric information).

70. *GDPR*, *supra* note 9, at 9.

A. Biometric-Specific Legislation

As biometric data collection becomes more prevalent, many legislative bodies are taking steps to ensure consumer protection.[71] However, most legislation addressing biometric data is not applicable to financial institutions because they are governed by the GLBA.[72] This section discusses current biometric-specific legislation as a potential model for statutory language that could be incorporated into the GLBA.

1. State Biometric Legislation: The Illinois Biometric Information Privacy Act

As a preliminary point, it is important to note that the state statutes discussed in this section are not applicable to financial institutions because these institutions are governed by federal legislation through the GLBA.[73] The biometric-specific statutes apply to private entities exclusively, and although certain CCPA provisions apply to financial institutions, biometric data falls under the purview of the GLBA and is therefore excluded from the CCPA.[74] Instead, the state statutes serve as a potential model for provisions that could be incorporated into the GLBA.[75]

Enacted in 2008, the Illinois Biometric Information Privacy Act ("BIPA") was the first biometric legislation enacted in the United States.[76] BIPA requires any private institution to establish and publish guidelines for the retention of biometric information, as well as the destruction of this information "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever

71. *See* Shinabarger & Swanson, *supra* note 9 (identifying a number of states that have implemented biometric-specific legislation); *see generally GDPR*, *supra* note 9 (protecting the personal data of EU consumers).

72. Gramm Leach Bliley Act ("GLBA") § 501, 15 U.S.C. § 6801 (2018).

73. *See, e.g.*, Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 25(c) (2019) ("Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.").

74. *See, e.g.*, *id.* (specifically excluding financial institutions that are subject to the GLBA).

75. *See generally id.* (implementing additional restrictions for biometric data that are significantly stricter than those found in the GLBA).

76. Niya T. McCray, *The Evolution of U.S. Biometric Privacy Law*, FOR THE DEFENSE (May 2018) at 77–78.

occurs first."[77] Further, private companies must obtain informed consent from consumers prior to collecting said information.[78] This provision is particularly noteworthy because it functions as an "opt-in" policy where consumers must affirmatively consent to the use of their personal information.[79] The "opt-in" policy is in contrast to the GLBA's policy for financial institutions, operating as an "opt-out" policy where consumers must take affirmative steps to prohibit the use or transfer of their personal information.[80] BIPA also offers a private right of action for consumers who are "aggrieved by a violation of this Act . . ." allowing individuals to collect up to $1000 for each negligent violation and up to $5000 for violations that are considered intentional or reckless.[81] The private right of action is the main difference between biometric legislation in Illinois and legislation in other states that is otherwise similar to BIPA.[82] BIPA is the most comprehensive legislation applicable to biometrics, and most states with similar statutes have modeled them after BIPA.[83] As of September 5, 2019, similar legislation restricting the collection and use of biometric information has been enacted in six states and proposed in ten others.[84]

2. International Biometric Legislation: The General Data Protection Regulation's Biometric Provisions

Although the GDPR does not directly apply to financial institutions in the United States, it does apply to entities processing data related to the "offering of goods or services . . . to such data subjects in the Union," meaning that banks serving individuals in the European

77. Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 15 (2019).

78. *Id.*

79. *Id.*

80. Gramm Leach Bliley Act ("GLBA") § 502, 15 U.S.C. § 6802(b) (2018).

81. Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 20(1)–(3) (2019).

82. *See, e.g.*, TEX. BUS. AND COM. CODE ANN. § 503.001 (West 2019) (eliminating the private right of action for consumers that have been harmed through violations of the Act).

83. McCray, *supra* note 76 at 77.

84. Illinois, Texas, Washington, Arkansas, California, and New York have enacted legislation or regulations regarding the use of biometric information. *State Biometric Privacy Legislation: What You Need to Know*, THOMPSON HINE (Sept. 5, 2019), https://www.thompsonhine.com/publications/state-biometric-privacy-legislation-what-you-need-to-know [https://perma.cc/9BDB-Z67F]. Delaware, Alaska, Florida, Arizona, Hawaii, Oregon, Massachusetts, New Hampshire, New Jersey and Rhode Island have introduced legislation, but it has not been enacted. *Id.*

Union must comply with this statutory scheme.[85] The GDPR takes a very strict approach to the collection and use of biometric data.[86] One of the primary purposes of the GDPR is to ensure that there is no processing of personally identifiable information; thus, most of the provisions require the data be anonymized before processing.[87] This is directly contrary to the nature of biometric data—it is an individual's most personal and identifiable information.[88] Unsurprisingly, these seemingly inconsistent principles led to very strict guidelines for any company collecting biometric data in the European Union.[89]

Under the GDPR, biometric data collection requires express consent from the consumer to be used only for a specific purpose, with very few exceptions.[90] Once an institution has obtained explicit consent from the consumer regarding the collection and use of their biometric data, restrictions applicable to all other data under GDPR are still enforced.[91] This includes appointing a Data Protection Officer if the company collects personal information and strict guidelines for the storage and protection of consumer information.[92] Under the GDPR, personal information obtained by a company, or in this case, a financial institution, must be encrypted or pseudonymized in some way.[93] Policies must also be in place to allow the organization to restore or recover the personal information if it is lost, and the GDPR further requires regular testing of security measures to ensure their adequacy.[94] These measures are intended to recognize the importance of an individual's ability to

85. *GDPR*, *supra* note 9, at 3.

86. *See id.* at 5(1)(b) (stating that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes . . . .").

87. *Id.* at 25(1).

88. *See Behavioral Biometrics and Biometrics in Payment Cards*, *supra* note 3 ("If personal biometric data is compromised or lost, the impact on consumer confidence in the technology could be catastrophic.").

89. *See GDPR*, *supra* note 9, at 9(1) (prohibiting the collection of biometric data unless an exception applies, such as obtaining explicit consent from the individual).

90. *Id.* at 9(2)(a).

91. *Id.*

92. *Id.* at 37.

93. *Id.* at Recital (28)–(29). "'[P]seudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." *Id.* at 4(5).

94. *See id.* at 30 (requiring controllers to maintain detailed records of its processing activities).

protect personal data and to ensure that individuals retain the right to protection of their personal information, a right that is recognized in some state legislatures as well.[95]

B. Non-Specific Privacy Legislation: The California Consumer Privacy Act

The California Consumer Privacy Act ("CCPA"), effective as of January 2020, is considered one of the most comprehensive pieces of privacy legislation in the United States and is often compared to the GDPR.[96] The CCPA defines biometric information but does not contain any provisions specifically regarding the collection of biometric data.[97] Instead, it categorizes this data as part of "personal information" in general.[98] "Personal information" is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" and includes data such as biometrics, employment and education information, and other unique personal identifiers.[99] The CCPA mirrors the GDPR in its recognition of an individual's right to protection of personal information.[100] It offers a right to know what information companies obtain, a right to access a copy of the personal information a company collects about an individual, and a right to have this information removed or deleted.[101] The CCPA also allows consumers to "opt-out" and prevent companies from selling or

95. *See id.* at Recital 7 ("[Technological] developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data."); *State Biometric Privacy Legislation: What You Need to Know*, *supra* note 84.

96. *See* Lydia de la Torre, *GDPR Matchup: The California Consumer Privacy Act 2018*, INT'L ASS'N OF PRIVACY PROF. (July 31, 2018), https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/ [https://perma.cc/2QAP-FSP4] ("Most data protection professionals would agree that the GDPR sets the global 'gold-standard' for data protection and has forced companies across the globe to significantly update their data practices and ramp up their compliance programs . . . the CCPA has the potential to become as consequential as the GDPR.").

97. California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.140(b) (West 2018).

98. *Id.* § 1798.140(o)(1).

99. *Id.* § 1798.140(o).

100. *See id.* § 1798.100 (affording consumers the right to obtain information regarding the personal information companies collect).

101. *Id.*

collecting their personal information.[102] The CCPA is considered the hallmark of data privacy legislation in the United States and could offer a valuable model for increased data protection language in the GLBA.[103]

V. THE GLBA IS INADEQUATE IN PROTECTING CONSUMER BIOMETRIC INFORMATION

As it stands today, the system for protecting consumer information within the financial services industry is weak at best.[104] For example, Capital One experienced a data breach in the summer of 2019 wherein approximately 106 million individuals had their personal information exposed.[105] The personal information released in this breach included customer status data such as credit limits and payment information, as well as 140,000 social security numbers and 80,000 bank account numbers.[106] Similarly, Equifax experienced a data breach in September 2017 that affected approximately 147 million people and led to the release of personal information including addresses, social security numbers, and driver's license numbers.[107] Equifax was forced to pay up to $700 million in settlements.[108] The regular occurrence of data breaches indicates inadequacies in consumer protection regulations and a need to implement stricter measures of ensuring consumer protection, especially because risks are compounded as banks begin to explore the use of biometric technology.[109] One of the primary concerns regarding the use of biometric information is the lack of recourse should individuals be affected by a security breach involving biometric information.[110] A

102. *Id.* § 1798.120.

103. *See* de la Torre, *supra* note 96 (identifying the GDPR as the "'gold-standard' for data protection").

104. *See, e.g.*, *Information on the Capital One Cyber Incident*, *supra* note 1 (describing the impact of the Capital One cyber breach on customers, including the number of individuals affected and the type of data that was compromised); *see also Equifax Data Breach*, *supra* note 1 (explaining the scope and type of data exposed in the Equifax data breach that occurred in September 2017).

105. *Information on the Capital One Cyber Incident*, *supra* note 1.

106. *Id.*

107. *Equifax Data Breach*, *supra* note 1.

108. *Id.*

109. *See* Cowley, *supra* note 6 (addressing the privacy concerns associated with collection of biometric data).

110. *See Behavioral Biometrics and Biometrics in Payment Cards*, *supra* note 3 ("[T]he industry must exercise extreme caution when working in this area . . . If personal biometric data is compromised or lost, the impact on consumer confidence in the technology could be catastrophic.").

PIN or card number can be changed; however, there is no way to change biometric information, such as a fingerprint, if banks are subject to a breach.[111]

Currently, there is myriad legislation offering some form of protection for consumer biometric data at the state, federal, and international levels.[112] These provisions create a confusing legal landscape because different standards apply to financial institutions and other business entities in states that have enacted biometric-specific legislation.[113] State-enacted biometric legislation creates an exception for any financial institution that is "subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder," meaning that although other businesses are held to the standards set forth in statutes such as BIPA, financial institutions are exempted.[114] The ultimate result of this exception is that in order to require financial institutions to comply with provisions found in biometric legislation, these standards must be reflected in the GLBA or in a separate federal biometric statute that is applicable to financial institutions as well.[115]

Based on the current status of biometric technology in the financial industry, there are three primary options in handling biometric data collection and use.[116] First, Congress could make the determination that the GLBA is adequate in its current form.[117] Second, Congress could follow in the footsteps of California by raising data privacy standards for

111. *Id.*

112. *See* Gramm Leach Bliley Act ("GLBA") § 501, 15 U.S.C. § 6801 (2018) (offering protections for consumer personal information in general); *see also* Shinabarger & Swanson, *supra* note 9 (identifying states with biometric-specific legislation); *see generally GDPR*, *supra* note 9 (affording protections for all personal data with specific carve-outs for the collection of biometric data).

113. *See* Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 25(c) (2019) ("Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.").

114. Gramm Leach Bliley Act ("GLBA") § 507, 15 U.S.C. § 6807; Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 25(c) (2019).

115. *See* Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 25(c) (2019) (exempting financial institutions governed by the GLBA from the provisions of BIPA).

116. *See generally* Cowley, *supra* note 6 (summarizing the biometric methods used by banks).

117. *See* 15 U.S.C. § 6801 ("[E]ach financial institution has an affirmative and continuing obligation . . . to protect the security and confidentiality of those customers' nonpublic personal information.").

all types of information instead of naming biometric data specifically.[118] Third, Congress could adopt provisions like those found in BIPA and the GDPR, specifically naming biometric technology as a sensitive type of data and carving out additional requirements for financial institutions that wish to collect biometric data.[119]

It can be argued that adequate protections are already in place to protect consumer data and additional provisions should not be added into the GLBA.[120] Biometric data technologies are expensive and banks must rely on third parties to implement these systems.[121] Using biometrics may be cost-prohibitive for many smaller banks governed by the GLBA, and the larger banks using the technologies are likely subject to the GDPR.[122] If there is adequate legislation governing financial institutions' use of biometric technology, some may argue that amending the GLBA and Regulation P is unnecessary.[123] Similarly, it could be dangerous to implement increased privacy measures for a technology that is not well-established and is rapidly evolving.[124] Taking steps to add biometric specific legislation while the technology is in its infancy risks implementing provisions that are outdated as soon as they are enacted, wasting resources and frustrating the statute's purpose.[125] These concerns indicate an amendment to the GLBA would be premature and would not ensure the protection of all forms of biometric data long term.[126]

---

118. *See* California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.100 (West 2018) (offering rights to consumers regarding their ability to control the personal data collected by businesses).

119. Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 15 (2019); *GDPR*, *supra* note 9, at 9.

120. *See* 15 U.S.C. § 6801(a) (creating affirmative obligations for financial institutions regarding protecting consumer data).

121. *See* Cowley, *supra* note 6 (identifying BioCatch as a leading provider of biometric technologies, along with many other third parties offering biometric analytical services).

122. *See* Jane Irene Kelly, *Do Banks Need Biometric Security Standards?*, SECURITY.COM (Sept. 26, 2018), https://blog.security.com/do-banks-need-biometric-security-standards/ [https://perma.cc/F3CX-JW89] ("Overly prescriptive regulations for biometrics in a rapidly changing technology environment would likely create challenges for banks . . . .").

123. *See* 15 U.S.C. § 6801 (providing general consumer protection without specific mentioning biometric data); Privacy of Consumer Financial Information (Regulation P); 12 C.F.R. § 1016.10 (2018) (limiting disclosures of personal information to nonaffiliated third parties).

124. Kelly, *supra* note 122.

125. *Id.*

126. *See id.* (identifying concerns about updating regulations of rapidly evolving technologies like biometrics).

An alternative method for the incorporating biometric protection in the GLBA is to follow in the footsteps of California by implementing legislation similar to the CCPA.[127] The CCPA, considered to be akin to the GDPR in scope, does not contain provisions specific to the collection and use of biometric data.[128] Instead, it offers increased protections for all types of personal data, biometric and otherwise.[129] The CCPA also creates a private right of action in the case of a data breach, creating a valuable recourse for consumers whose data is exposed.[130] The CCPA is a middle ground in the incorporation of biometric technologies into legislation by recognizing the biometric data as a sensitive class of information without providing protection specific to biometrics.[131] Identifying biometrics as a sensitive class of data without outlining specific protections eliminates the concern of implementing these provisions prematurely.[132] Modeling an amendment to the GLBA after the CCPA would offer increased protection to all forms of consumer information, not just biometrics.[133]

Despite the concerns relating to incorporating biometric-specific language in the GLBA, the comprehensive provisions found in BIPA and the GDPR serve as the most helpful models.[134] For example, making the transition from an "opt-out" policy to BIPA's "opt-in" policy for the collection and use of all "nonpublic personal information" would ensure consumers are properly informed and have explicitly consented to the use of such sensitive information.[135] Further, BIPA and other similar legislation sets forth specific guidelines for the destruction and retention

127. California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798 (West 2018).

128. *See id.* § 1798.140 (protecting consumer data in general and including biometric data without offering specific protections for the collection and storage of biometric information).

129. *Id.* § 1798.140(o).

130. *Id.* § 1798.150.

131. *See id.* § 1798.140(o) (including biometric data in the definition of "Personal Information" that is protected).

132. *See* Kelly, *supra* note 122 (identifying disadvantages to implementing legislation prematurely).

133. *See* CAL. CIV. CODE § 1798.140 (West 2018) (enacting increased consumer protections for the collection and use of data).

134. Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 15 (2019); *GDPR, supra* note 9.

135. *See* Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 15 (2019) (creating an "opt-in" provision that requires affirmative consent to the collection of personal information).

of biometric information, including time limits for retention.[136] Implementing similar regulations in the financial industry would require financial institutions to store only biometric information that is being used for ongoing business purposes.[137] Updates to the GLBA could also take cues from the GDPR by including specific language stating that biometric information must be stored with the same or more protective methods that are used for other confidential information and acknowledging the increased value and sensitivity of biometric information.[138] Finally, the private right of action for violations of this statute may offer a remedy to consumers whose data has been compromised.[139] This private right of action would guarantee that, in cases of breach, individuals are entitled to compensation for loss of their information.[140]

Although there are multiple ways to handle the increased sensitivity of biometric data, the ideal path forward involves amending the GLBA in a way that models it after the GDPR and incorporates features from other biometric specific legislation and the CCPA.[141] The abundance of security breaches in the financial industry indicates a need for increased protection of consumer information, and this need is compounded by the collection and use of more sensitive information.[142] Currently, biometric technology in the financial industry is dominated by larger banks, but this technology will continue to develop, and it is likely that smaller banks may begin to implement biometrics as well.[143] Banks conducting business in the European Union are complying with the

136. *See, e.g.*, *id.* (creating specific restrictions on the retention of biometric information, many of which have been implemented by other states).

137. *See id.* (requiring that biometric information be destroyed "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.").

138. *GDPR*, *supra* note 9, at 5(e)(1).

139. *See* Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 20 (2019) (carving out a private remedy for consumers aggrieved by a violation of the statute).

140. *See id.* (outlining the minimum damages an individual is entitled to in the event of a breach).

141. *GDPR*, *supra* note 9; California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798 (West 2018).

142. *See, e.g.*, *Information on the Capital One Cyber Incident*, *supra* note 1 ("[T]his event affected approximately 100 million individuals in the United States and approximately 6 million in Canada"); *see also Equifax Data Breach*, *supra* note 1 ("[T]he sensitivity of the personal information held by Equifax and the scale of the problem makes this breach unprecedented.").

143. *See Biometrics: Authentication and Identification*, *supra* note 16 ("The global biometric market is expected to top USD 50 billion by 2024 . . . .").

GDPR,[144] but there is no current federal legislation ensuring adequate protection for biometric data within the United States, which is critical as the technology grows and becomes accessible to banks that are not GDPR-compliant.[145]

Since the potential uses of biometric legislation have not been fully explored, biometric legislation should be defined as broadly as possible to allow for advances in the technology over time.[146] An ideal amendment would mirror the GDPR, which is widely regarded as the most comprehensive privacy legislation available and provided the basis for the CCPA.[147] The GDPR offers the ideal mix of the merits of biometric specific legislation and the CCPA by demanding higher standards for protection of all types of consumer information while also recognizing the unique nature of biometric data.[148] One of the most crucial provisions common to each of these pieces of legislation is the private right of action, which should be incorporated into any amendments to the GLBA.[149] A private right of action ensures that consumers can be compensated for violations of their rights under the statute and greatly increases the effectiveness of the statute.[150] It also provides a compliance incentive for financial institutions and offers a remedy to consumers, which would be invaluable due to the uniquely sensitive nature of biometric information.[151] Modeling changes to the

144. *See GDPR*, *supra* note 9, at 3 (requiring that all entities conducting business with individuals in the European Union comply with GDPR).

145. *See Biometrics: Authentication and Identification*, *supra* note 16 ("The global biometric market is expected to top USD 50 billion by 2024 . . . .").

146. *See* Kelly, supra note 122 ("Overly prescriptive standards for biometrics could create friction in transactions and potentially stifle innovation, experts warn."); *see also Biometrics: Authentication and Identification*, *supra* note 16 ("[B]iometrics has quickly established itself as the most pertinent means of identifying and authenticating individuals in a reliable and fast way, through the use of unique biological characteristics.").

147. *See* de la Torre, *supra* note 96 ("[T]he GDPR sets the global 'gold-standard' for data protection . . . .").

148. *See GDPR*, *supra* note 9, at 9 (prohibiting the collection of biometric data unless an exception applies, such as obtaining explicit consent from the individual).

149. *See, e.g.*, *id.* at 82 (offering a private right of action for aggrieved consumers).

150. *See* Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 / 20 (2019) (describing the restrictions on retention, collection, and disclosure of biometric information); *see also* John Patzakis & Craig Carpenter, *GDPR Provides a Private Right of Action. Here's Why That's Important*, X1 DISCOVERY (Feb. 28, 2018, 8:51 AM), https://blog.x1discovery.com/2018/02/28/gdpr-provides-a-private-right-of-action-heres-why-thats-important/ [https://perma.cc/9L4A-KZU2] ("Regulations which provide a private right of action, including the ability to bring a class action lawsuit, are exponentially more impactful than the vast majority of regulations which do not.").

151. *See Behavioral Biometrics and Biometrics in Payment Cards*, *supra* note 3 ("Biometric data is arguably the most personal and private data that anyone has.").

GLBA after the GDPR will require financial institutions to meet the highest standard in protecting consumer information.[152] Furthermore, incorporating the private right of action and specific protections for biometric information will provide the level of compliance and comprehensiveness demanded by the sensitivity of the data.[153]

VI. CONCLUSION

Biometric technology is the new frontier of security in banking.[154] The use of biometric data offers many benefits, namely increased protection of customer data in an era where data breaches are common.[155] In order to ensure that this data is protected, there is a need to incorporate elements of existing biometric-specific legislation into the GLBA.[156] Some states have already recognized the need for this legislation and there is a definitive trend towards implementing biometric-specific legislation nationwide.[157] From a practical standpoint, the most comprehensive update to the GLBA can be accomplished by modeling the new provisions after the GDPR.[158]

Biometric technologies are rapidly developing and legislators must stay up to date in order to maintain an adequate level of protection for consumer personal information.[159] Risks associated with the collection of biometrics can be mitigated by ensuring that statutory language is broad enough to encompass technological developments.[160] As new ways of collecting personal information emerge, legislation and

152. *See* de la Torre, *supra* note 96 ("Most data protection professionals would agree that the GDPR sets the global 'gold-standard' for data protection . . . .").

153. *See Behavioral Biometrics and Biometrics in Payment Cards, supra* note 3 (arguing that biometric data is uniquely personal information).

154. *See Biometrics: Authentication and Identification*, *supra* note 16 ("The global biometric market is expected to top USD 50 billion by 2024 . . . .").

155. *See, e.g.*, *Information on the Capital One Cyber Incident*, *supra* note 1 (describing the Capital One breach, one of the largest data breaches in history where millions of consumers' personal information was compromised).

156. Gramm-Leach Bliley Act ("GLBA") § 501, 15 U.S.C. § 6801(a) (2018) (protecting consumer data generally without specific reference to biometric data).

157. *See* Shinabarger & Swanson, *supra* note 9 (compiling information about currently pending state legislation on biometric data use).

158. *GDPR*, *supra* note 9.

159. *See* Shinabarger & Swanson, *supra* note 9 (identifying a number of states who recognized the significance of biometric data and introduced legislation to protect it).

160. *See* Kelly, *supra* note 122 ("Standards shouldn't be too detailed or technology-specific because they will restrict innovation and limit banks' choices in terms of what they can deploy.").

regulations must continue to reflect privacy risks associated with this collection and storage.[161]

MEREDITH E. BOCK*

161. *See id.* (emphasizing the importance of crafting legislation that is flexible as technology evolves).

* I would like to thank my family and friends for their support throughout my writing process. I would also like to thank my editors, Marion Brown and Erin Catlett, as well as the rest of the North Carolina Banking Institute Journal staff members for their guidance and thoughtful edits. Finally, I am extremely grateful to Professor Lissa L. Broome for her feedback, as well as her support for the North Carolina Banking Institute Journal and University of North Carolina School of Law as a whole.