AUTOMATIC DELETION OF BIOMETRIC DATA IN FINANCIAL INSTITUTIONS

Alina Big

I. INTRODUCTION

With the emergence of a global economy and an expanding digitalized world, our reality is slowly moving towards an entirely virtual world. From smart washing machines, to smart key chains, the information we share today could be information that we cannot take back tomorrow. While data used to be forgotten, now the shift is towards remembering and storing it for eventual future use. Financial institutions cannot afford to fall behind in recognizing this trend. These institutions must implement new strategies and ways to protect their market shares. With the emergence of new technology, people do not need banks anymore; instead, they need banking. Ranging from fingerprint technology, to eye scans, biometric data is found across many mobile banking applications in a multitude of ways. Banks offer more and more innovative products, slowly moving into the virtual world.

The beneficial growth of a digitalized world also brings negative effects. The multitude of data breaches forces companies to migrate away from traditional passwords towards the widespread use of biometrics, which offers unique safety measures for consumers but, they cannot obtain these safety measures without regulations expressly tailored to protect biometric data. Unfortunately, at the federal level, the United States does not offer this much needed protection.[1]

When it comes to financial institutions, the government relies on outdated laws that protect traditional data but fail to offer any sort of protection for biometric data. Furthermore, financial institutions not only retain customers' data, but the law requires them to comply with data retention principles. This spread of biometric data collection and retention by financial institutions coupled with the lack of specific regulation in the United States precipitate security issues.

[1] *Biometric Data and Data Protection Regulations (GDPR and CCPA)*, THALES (Jun. 27, 2020), https://www.gemalto.com/govt/biometrics/biometric-data.

This Comment takes the position that the present regulations applied to financial institutions do not adequately protect individuals' biometric data and, considering the high level of privacy at stake, the government must implement new regulations that provide for automatic deletion of such data when a customer closes the account.

Part II of this Comment presents the principle of recordkeeping within financial institutions, its initial purpose, as well as its evolution. Part III defines biometric data, the way financial institutions collect such data, and the reasons behind their intensive use. This Part also presents how several companies' approaches render biometric data a target for hackers. Part IV presents the regulations of personal data in the United States at the federal and state level, as well as the European Union's innovative regulation, and argues why none have sufficiently tailored these regulations to protect biometric data after the relationship between a financial institution and a customer ends. Part V of this article presents the security issues created by third party transactions of personal information. Part VI proposes a solution for biometric data deletion that mirrors the customers' expectations and gives users control over the information once they terminate the relationship with a financial institution.

II. RECORDKEEPING REQUIREMENTS FOR FINANCIAL INSTITUTIONS

Laws scattered throughout many statutes require financial institutions, one of the most regulated industries in the United States, to comply with different document retention requirements.[2] One of these statutes is the federal Bank Secrecy Act ("BSA").[3] The BSA was adopted in 1970 as an anti-money laundering system and helped identify the movement of currency into or out of the United States; the statute also imposed criminal liability for any assistance in the laundering of money.[4] In 2001, following the September 11th terrorist attacks, federal regulations began focusing even more on preventing transactions with persons who could threaten national security.[5] In order to prevent and

[2] Elizabeth Fast, *Document Retention Policy for Banks*, SPENCER FANE (Jul. 15, 2016), https://www.spencerfane.com/publication/document-retention-policy-for-banks/.

[3] Currency and Foreign Transactions Act, 31 U.S.C.S. § 5311 (1970) [hereinafter "Bank Secrecy Act"] (codified as amended in scattered sections of 31 U.S.C.).

[4] *The Bank Secrecy Act and the USA Patriot Act: Before the Comm. On Int'l Relations, U.S. House of Representatives*, 108th Cong. (2004) (Testimony of Herbert A. Biern, Senior Associate Director, Division of Banking Supervision and Regulation) [hereinafter "Biern Testimony"].

[5] Amanda Bloch Kernan, *Sustaining the Growth of Mobile Money Services in Developing Nations: Lessons From Overregulation in the United States*, 51 VAND. J. TRANSNAT'L L. 1109, 1128-30 (2018).

track suspicious transactions before they reached terrorists, Congress enacted the USA PATRIOT Act,[6] which criminalizes the financing of terrorism and "augmented the existing BSA framework by strengthening customer identification requirements for banks and other financial institutions."[7] In 2018, Congress took a step further and tightened up its requirements for financial institutions by demanding the identification and verification of all account owners, as well as stricter record maintenance.[8]

According to the BSA, financial institutions, as money service businesses, must have effective anti-money laundering programs.[9] They also must keep records of the customer's identity information for five years.[10] While this standard procedure did not pose problems in the past, in this new digitalized era, the amount of data retained by any institution can have a great impact on someone's life. More and more customers use biometric identifiers[11] for access authentication when they interact on digital platforms, including their banks. Unfortunately, the record retention requirement does not refer to any particular data that institutions must keep; instead, the obligation requires financial institutions to keep any "transaction records created in the ordinary course of business necessary to . . . access activation, loads, reloads, purchases, withdrawals, transfers, or other prepaid-related transactions."[12] This lack of qualification allows financial institutions to qualify any data as "necessary" to "access activation" and pertaining to a "transaction record created in the ordinary course of business." Once the data meets one of these requirements it is therefore subject to the record retention regulations.

When a bank acquires an individual's personal information, the data collected loses its "private" status every time the government

---

[6] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 2001 U.S.C.C.A.N. (115 Stat.) 369 (codified at 18 U.S.C.S. § 1960 (2001) and in other amended sections of the U.S. Code).

[7] Biern Testimony, *supra* note 4.

[8] Kernan, *supra* note 5, at 1129.

[9] Bank Secrecy Act, 31 U.S.C.S. § 5311 et al.

[10] Nizan Geslevich Packin & Yafit Lev-Aretz, *Big Data And Social Netbanks: Are You Ready to Replace Your Bank?*, 53 HOUS. L. REV. 1211, 1251 (2016).

[11] "Biometric" refers to automatic techniques of identifying individuals based on a unique physical characteristic. *See* Lisa Jane McGuire, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV., 441, 444 (2000); *see infra* PART III.A. p. 7.

[12] Packin, *supra* note 10, at 1251 (quoting Bank Secrecy Act, 31 U.S.C. § 5311).

decides that it is necessary to investigate such data.[13] This unfortunate effect relies on the premise that individuals who share their data voluntarily lose their "reasonable expectation to privacy."[14] In other words, if the government deems it necessary, it can access any personal information a bank has, as long as the bank retained the data.

As its main problem, the record retention requirement only establishes a "mandatory minimum" for data retention and does not require its mandatory deletion at the end of the period.[15] As a result, financial institutions can hold onto the individual's biometric data for as long as they want, even after the mandatory retention period terminates.[16] Traditionally, retaining vast amount of personal information was not desirable.[17] Without digital advantages, financial institutions were forced to retain all the information in hardcopy, a burdensome process that took much needed time and physical space.[18] Today, however, the digitalized aspect of all transactions allows institutions to collect as much information as they find useful, and to keep for as long as they choose.[19] It is now easier to retain data because everything is electronic, i.e., everything is in "the cloud."[20] Moreover, given the nature of the personal data collected and its value in an innovative society, banks might find it convenient not to delete customers' data even after the retention period ends. All these changes in society present a novel risk that financial institutions not only may retain the individual's biometric data, but they also can find the

[13] *See* Dina Moussa, *Protecting Privacy in Our Financial Transactions: An Alternative Method to Thinking About Our Privacy in the Digital Era*, 1 GEO. L. TECH. REV. 342, 360 (2017).

[14] Moussa, *supra* note 13, at 360; United States v. Miller, 425 U.S. 435, 440-45 (1976) (holding that individuals have no reasonable expectation of privacy from the government in bank records and that banks must keep records and provide them to the government when necessary), *superseded by statute*, Right to Financial Privacy Act of 1978, Pub. L. No. 116-158, 92 Stat. 3641.

[15] *See* Peter Sloan, *The Compliance Case for Information Governance*, 20 RICH. J.L. & TECH. 4, 23 (2014). Regulations do establish how entities should dispose of information, but not when. *See* 16 C.F.R. § 682.3(a) ("Any [entity that] maintains . . . consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.").

[16] *See generally*, DELOITTE, *Is it time to go paperless? Records management: The cost of warehousing bad habits*, (2012).

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] The term refers to high-capacity data centers available to many users over the Internet.

mandatory retention beneficial at the expense of customers' reasonable expectation of privacy.

The widespread use of personal data transactions and the public concern behind it pressed legislators around the world to recognize its sensitive nature and enact comprehensive data protection regulations.[21] Unfortunately, at the federal level, the United States lacks regulations regarding the use of biometric data.[22] The sensitive nature of this data requires stricter regulations than those we already have for traditional personal data. This is especially true for financial institutions because the nature of their business—money—creates a high risk of hacking.[23] Also, banks must enter into third-party contracts to store the vast amount of information they use,[24] adding another layer of concern for all the users that share their data. When enacting record keeping policies for financial institutions, Congress sought to prevent and solve financial crimes. Congress did not seek to intrude into innocent, private citizens' most valuable personal data, however the laws have had that effect.

III. THE WIDESPREAD USE OF BIOMETRIC DATA

The government, especially law enforcement agencies, started using biometric identification as early as 1960 and, by the end of the 1980s, biometric recognition became fully automated and widely accessible.[25] The government still uses biometric recognition and authentication as important tools in the war on crime.[26] This technology extends beyond governmental use; private companies have also started using biometric identifiers in their commercial products.[27] The digital

[21] Olivier Sylvain, *Foreword: The Market for User Data*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1087, 1092 (2019).

[22] Lauren Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, 60 B.C. L. REV. 347, 364 (2019).

[23] *See* G. Dautovic, *Top 25 Financial Data Breach Statistics for 2020*, FORTUNLY, (Sept. 30, 2020), https://fortunly.com/statistics/data-breach-statistics/#gref (noting that 71% of all data breaches are financially motivated and that cyber-attacks are 300 times more likely to hit the financial industry than other industries).

[24] *See* Mary Thorson-Wright, *Is your bank protected from third-party risks?*, INDEPENDENT BANKER, (Sept. 1, 2020), https://independentbanker.org/2020/09/is-your-bank-protected-from-third-party-risks/.

[25] Carmen Aguado, *Facebook or Face Bank?*, 32 LOY. L.A. ENT. L. REV. 187, 191-92 (2011/2012).

[26] Jake Stroup, *Biometric Identification and Identity Theft*, BALANCE (Apr. 30, 2020), https://www.thebalance.com/biometric-identification-and-identity-theft-1947595.

[27] *See* Leonardo Sam Waterson, *10 Ways Biometric Technology is Implemented in Today's Business World*, M2SYS (Nov. 29, 2018),

world brings about innovation, but also brings about many risks. The extraordinary advances in technology and the need to enhance security due to data breaches can explain the widespread use of biometric data in all industries. Millions of people utilize mobile banking applications today, and this number grows each day.[28] But there is also a growing trend in financial markets where consumers are using non-bank financial institutions[29] for their financial transactions, which causes banks' market shares to shrink. Most of the time, these institutions attract their consumers by offering innovation and flexibility.[30] Modern banks understand these new customer expectations and try to improve their products by offering innovative services.[31] New approaches and ideas arise daily, and people seem ready to embrace them. Yet, all these advantages bring security problems that could be quashed by proper regulations.

A. What is Biometric Data?

The idea of using biometric identification technology is certainly not new, but the widespread use of such technology poses concerns.[32] Biometrics, as automatic techniques of identifying individuals based on unique physical characteristics, have a high degree of reliability because they uniquely identify each individual and likely will not change over time.[33] Biometric data is vast and can range from traditional fingerprinting to innovative palm-vein reading.[34]

https://www.m2sys.com/blog/biometric-technology/10-ways-biometric-technology-implemented-business/.

[28] Matthew Y. Chang, *Mobile Banking: The Best Hope for Cyber Security Development*, 2016 U. ILL. L. REV. 1191, 1219 (2016).

[29] "Nonbank financial companies (NBFCs), also known as nonbank financial institutions (NBFIs) are financial institutions that offer various banking services but do not have a banking license." James Chen, *Nonbank Financial Companies (NBFCs)*, INVESTOPEDIA (Jun. 14, 2020), https://www.investopedia.com/terms/n/nbfcs.asp.

[30] *Id.*

[31] Packin, *supra* note 10, at 1269.

[32] *See* McGuire, *supra* note 11, at 445-49. Until recently, biometric technology was expensive and not easily accessible, but today, the systems are financially viable and widely used. McGuire, *supra* note 11, at 446 n.31.

[33] McGuire, *supra* note 11, at 445-48; *see also* Stacy-Ann Elvy, *Commodifying Consumer Data in The Era of the Internet of Things*, 59 B.C. L. REV. 423, 437 (2018).

[34] Fingerprinting is the process by which the person's unique fingerprints patterns are compared. "[N]o two persons have the exact same arrangement of ridge patterns on their fingertips." They remain unchanged throughout life. Rudy Ng, Note*, Catching Up to Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology*, 28 HASTINGS COMM. & ENT. L.J. 425, 429 (2006). Facial recognition is a popular system that locates and measures features on the face that are distinctive. Facial recognition software then creates an algorithm or a biometric template of the face, which is stored and compared to other images. Aguado, *supra* note 25, at 193. Voice

Although there are different systems for gathering biometric data, which might not follow the same procedures, the systems generally have the same core steps. A program first scans a person's physical characteristic, then converts that data into a stored digital code, and finally compares this code with a new physical scan when the user seeks access.[35] The central element that determines the risk level faced by consumers is how the institution stores the information. Biometrics' intimate character raises concerns about whether an institution properly stores this information and, even if it does, whether the customers' privacy could still be affected by other factors, like third party transactions.[36]

In the financial industry, the novel technology uses the consumer's biometric data to identify and authenticate the user and, as a result, grant access to the bank account.[37] Banks in the United States already use a variety of biometric identifiers for user authentication and the speed of implementing new technologies is growing with each day.[38] For example, banks use voice recognition technology that grants immediate secure access to a user's account after recognizing the unique vocal patterns of the customer.[39] The Royal Bank of Scotland launched a payment card with biometric fingerprint technology, where the Personal Identification Number ("PIN") is replaced with the user's fingerprint.[40] Likewise, Barclays offers customers finger vein reader technology, which allows users to access their account by placing a finger in a small desktop scanner for authentication, allowing the user

recognition system grants user secure access after recognizing its unique vocal patterns. Dan Hansen, *Voiceprint: A Security Game-Changer for Banks and Credit Unions of All Sizes*, BIZTECH (Nov. 5, 2018), https://biztechmagazine.com/article/2018/11/voiceprint-security-game-changer-banks-and-credit-unions-all-sizes. Palm-vein reader is a biometric authentication method based on individual vein patterns in the users' palm. Margaret Rouse, *Palm Vein Recognition*, WHATIS.COM (May 2016), https://whatis.techtarget.com/definition/palm-vein-recognition.

35 McGuire, *supra* note 11, at 445.

36 Efren Lemus, *When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones*, 70 SMU L. REV. 533, 541 (2017); *see infra*, PART V., at 27.

37 Elvy, *supra* note 33, at 436.

38 *See* Hansen, *supra* note 34.

39 *See* Hansen, *supra* note 34. After the financial institution scans and saves the user's voiceprint, the system matches that data with any future calls that require authentication. The technology analyzes the individual components of someone's voice and does not require the physical presence of the individual, like other biometric modalities.

40 Alison Arthur & Bethany Frank, *Five Examples of Biometrics in Banking*, ALACRITI (May 8, 2019), https://www.alacriti.com/biometrics-in-banking.

to skip inputting traditional passwords.[41] Wells Fargo no longer uses passwords or tokens at all, allowing its clients to access their bank accounts with a simple eye scan on their mobile devices.[42]

Thus, there is a growing number of financial institutions with access to innovative technology that implements biometric authentication into their systems, which eliminates the use of traditional passwords or manual identification methods.[43] This shift in banking trends proves that not only are users prepared for such a change, but they are actually willing to adapt to a more secure—and convenient—process.[44]

B. How Biometric Data is Stored

While the legal system is still behind and does not ensure an appropriate framework for biometric data, on a technical level, companies have started implementing different measures to safeguard customer information.[45] One of these measures is encryption, a process by which understandable information is transformed into an unintelligible format by using a key; the same key then brings back the information to its original format.[46] "The mechanism from which the encryption key is derived can take any number of forms—for example, it might be a passphrase, numeric code, or biometric data (like a fingerprint or a retinal scan)."[47] More importantly, encryption does not look like a barrier between the text and outside world or like a box that must be opened; instead, it is unintelligible data, transformed and rearranged that sits in plain view.[48]

---

41 *Id.*

42 *Id.*

43 *See* Jeanne Pinder, *The top 10 mobile banking trends for 2019*, BAI, (Jan. 14, 2019), https://www.bai.org/banking-strategies/article-detail/ten-mobile-banking-trends-for-2019.

44 *Id.*

45 Lemus, *supra* note 36, at 541. *See also* McGuire, *supra* note 11, at 445-46.

46 *See* Lex Gill, *Law, Metaphor, and the Encrypted Machine*, 55 OSGOODE HALL L.J. 440, 442 (2018). *See also* Aamir Lakhani, *For Financial Services, Encryption is Essential – But So Is Performance*, CSO (Jun. 26, 2018), https://www.csoonline.com/article/3284351/for-financial-services-encryption-is-essential-but-so-is-performance.html ("Encryption refers to converting plain text into secure code that can only be deciphered with a decryption key. This ensures that data in motion across the network and the web, as well as data at rest in the cloud or data center, cannot be seen by anyone without the key – even if it is stolen – adding a strong layer of security.").

47 Gill, *supra* note 46, at 442.

48 Gill, *supra* note 46, at 468-69. *See also* Elvy, *supra* note 33, at 436-37 (noting that biometric data can be stored as mathematical representations or authentication codes). Ng, *supra* note 34, at 428 (Biometric data can be stored in "one-to-one" matching systems, used for verification, or "one-to-many" matching systems, used for

The financial industry is amongst few industries that can readily access extremely sensitive, private data. As a result, it is also one of the most regulated industries in the world. Thus, banks must implement strong data security measures to comply with federal and state regulations.[49] The Gramm-Leach-Bliley Act of 1999 ("GLBA")[50] requires financial institutions to implement encryption to reduce the risk of alteration or disclosure of nonpublic personal information both in storage and in transit.[51] The encryption must meet specific guidelines to ensure sufficient protection for individuals' personal data.[52] Banks must encrypt sensitive information *received* from a transaction for a financial product or service and any information *acquired* from a transaction involving a financial service or product.[53]

Although financial institutions implement high-level encryption that could prevent hacking to a certain extent, encryption is not always perfect, or even sufficient to safeguard the data; legislatures, therefore, should not overlook the multitude of factors that could affect its function.[54] A breach is always possible.[55] "If encryption is so unbreakable, why do businesses and governments keep getting hacked?"[56] Although individuals know that authenticating with a biometric identifier brings in present risks, they do not expect to have exactly the same risks even after the relationship with the bank ends. Furthermore, even if the financial institution is one of the lucky ones that does not encounter a breach, the individual's biometric data is still at risk from possible third party privacy flaws. Because banks often outsource their services to third parties, the resulting agreements pose their own concerning set of risks to each individual's data.[57]

identification. "One-to-one" matching systems can be used to verify that the individual is who he claims he is before giving him access to a restricted area. "One-to-many" matching systems can additionally be used for identification of one individual by comparing his biometric data to a complete database of information).

[49] Luke Probasco, *Encryption Requirements For Banks & Financial Services*, TOWNSEND SECURITY (Apr. 25, 2017), https://info.townsendsecurity.com/encryption-requirements-for-banks-financial-services.

[50] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801-6809 (2012). *See infra*, PART IV., at 18.

[51] Probasco, *supra* note 49.

[52] Probasco, *supra* note 49.

[53] Probasco, *supra* note 49.

[54] Erin Fonte, *2017 U.S. Regulatory Overview of Mobile Wallets and Mobile Payments*, 17 WAKE FOREST J. BUS. & INTELL. PROP. L. 549, 558 (Summer 2017).

[55] *See* Dautovic, *supra* note 23.

[56] Yaron Guez, *6 Encryption Mistakes That Lead To Data Breaches*, CRYPTERON (Feb. 23, 2020), https://www.crypteron.com/blog/the-real-problem-with-encryption/.

[57] *See infra*, PART V., at 27.

C. Why Do We Use Biometrics Today?

Biometric data has become a useful tool in both the public and private sector.[58] Using unique characteristics to grant access only to the person with a match renders these personal identifiers as capable and reliable protection against unauthorized access.[59] However, these advantages also generate concerns that the public might not be ready to accept. For example, not many consumers know that, from a mere scan of a facial image, a program can deduce a user's sexual orientation or even identify individuals solely by their posture and clothing.[60]

The phase "big data" is often used, but users typically do not know the extent of their personal data's value."[61] Sensitive data is a highly wanted product on the open market, with studies showing that companies will earn more profits from selling and disclosing personal data than from traditional sales.[62] When using devices, mobile applications, or different services, consumers generate important data for companies, increasing the data value and variety.[63] Devices can even connect to each other, giving a company a whole picture of the user's life, from their home layout to their health, or even the most intimate information.[64] For example, when a consumer turns on the Roomba robotic vacuum, his expectation is for the vacuum cleaner to clean the house.[65] Instead, the "smart" vacuum cleaner also collects data about the home layout, wall locations, and different objects in the house.[66] Once companies gather all this data, they are allowed to, and actually do, process, compile, and store users' data for future transactions.[67] This allows them to offer better and more targeted services to the consumer. The convenience of having everything one click away persuades

58 McGuire, *supra* note 11, at 450-53.

59 McGuire, *supra* note 11, at 453.

60 Elvy, *supra* note 33, at 450-51.

61 *See* Elvy, *supra* note 33, at 448-49.

62 Elvy, *supra* note 33, at 435-37. Smartwatches, fitness trackers, mobile applications, used by consumer to track activity, generate more than $26 billion in revenues. The "big data revolution" creates an unprecedented volume of data. Agnieszka McPeak, *Disappearing Data*, 2018 WIS. L. REV. 17, 23-25 (2018).

63 Elvy, *supra* note 33, at 435-36, 438. Consumers' use of new "smart" devices generates health-related data about the user's activity or health; baby monitors generate information relating to sleep patterns.

64 Elvy, *supra* note 33, at 438-43. Baby monitors can gather information about sleep patterns, connect with other devices in a home, and acquire information regarding the temperature and health of the baby. Sex-toy devices collect real time data about the consumer's use.

65 Elvy, *supra* note 33, at 443.

66 Elvy, *supra* note 33, at 443.

67 Elvy, *supra* note 33, at 435-36.

consumers to give their consent to the transfer, sale, or disclosure of personal data, without actually knowing how their data is used.[68]

Access to consumer data brings better performance, resource productivity, and increased safety, allowing companies to identify and adapt their product to the consumers' expectations.[69] Yet, big data also represents a variety of risks. If not exercised properly, the enormous volume of data stored can have a detrimental impact on someone's life.[70] This information is valuable to both companies that can buy the data and to thieves that can steal the data.[71]

D. Risks of Biometric Data

The advancement in technology makes data breaches a real concern for governments, enterprises, and consumers.[72] Consumer convenience comes with a cost: the probability of a major breach in security.[73] Data breaches continue to grow each year; between 2005 and 2014, over 783 breaches were declared, which affected more than 85.61 million records.[74] These breaches are usually carried out by hackers and can compromise millions of records that contain personal consumer information or private data.[75] Between 2015 and 2016, the financial sector encountered a 937 percent increase in cyberattacks.[76]

---

[68] *See* Elvy, *supra* note 33, at 442.

[69] Nikole Davenport, *Smart Washers May Clean Your Clothes, But Hacks Can Clean Out Your Privacy, And Underdeveloped Regulations Could Leave You Hanging On A Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 263 (2017) (citing Jane Collis, *Internet of Things: Generating Opportunity Behind the Buzz Words in the Energy Sector*, DLA PIPER LLP CLIENT ALERT (Nov. 3, 2015), http://www.lexology.com/library/detail.aspx?g=0675dcaf-a0b4-4133-8e94-05ca96477362).

[70] Packin, *supra* note 10, at 1264.

[71] Kelsey Sherman, *Biometrics: The Future Is In Your Hands*, 50 LOY. L.A. L. REV. 663, 685 (2017).

[72] Juliana De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN (blog) (Sep. 17, 2020), https://digitalguardian.com/blog/history-data-breaches; Camino Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Aug. 28, 2019), https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736.

[73] De Groot, *supra* note 72.

[74] De Groot, *supra* note 72. ("In 2005, 157 data breaches were reported in the U.S., with 66.9 million records exposed. In 2014, 783 data breaches were reported, with at least 85.61 million total records exposed, representing an increase of nearly 500 percent from 2005. That number more than doubled in three years to 1,579 reported breaches in 2017.").

[75] De Groot, *supra* note 72.

[76] Melissa Knerr, *Password Please: The Effectiveness of New York's First-in-Nation Cybersecurity Regulation of Banks*, 1 BUS., ENTREPRENEURSHIP & TAX L. REV. 539, 541 (Fall 2017).

While the advantages of data collection allow companies to offer more tailored products, it also raises critical privacy concerns emanating from users' inability to control the data.[77]

In 2014, Yahoo! was the victim of one of the largest breaches to date.[78] The attack compromised the names, dates of birth, telephone numbers, and email addresses of 500 million users.[79] Following this breach, Yahoo! upgraded its security system and decided to introduce biometric technology by allowing users to access their account by scanning their fingerprints.[80] Similarly, Equifax was the victim of a breach after it spent over $1 million to counter legislation meant to improve data security.[81] This breach affected almost half of the U.S. population and the exposed individuals will be affected for the rest of their lives.[82] Likewise, in 2018, Marriott International was the victim of a cyberattack, which left approximately 500 million customers with their data stolen.[83] This breach started in 2014 and the hackers had access to the database for years before the breach was discovered.[84] Government offices are targets of significant breaches as well.[85] In 2015, a significant breach affected the Office of Personnel Management, targeting information about security clearances for the federal workforce.[86] This Office is in possession of highly sensitive information on U.S. government personnel.[87]

Data breaches such as these create an urgent need for more secure systems. In response, companies have invested in biometric technology, which transforms individuals' biometrics into digital keys that secure

---

[77] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 3, 5 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokerscall-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (discussing how data brokers obtain consumer information).

[78] Sherman, *supra* note 71, at 663.

[79] Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Apr. 17, 2020), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[80] Sherman, *supra* note 71, at 663.

[81] McKay Smith & Garrett Mulrain, *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, 9 J. NAT'L SECURITY L. & POL'Y 549, 551-552 (2018).

[82] *Id.* at 556.

[83] Swinhoe, *supra* note 79.

[84] Swinhoe, *supra* note 79.

[85] *See* Smith, *supra* note 81, at 563.

[86] Smith, *supra* note 81, at 563.

[87] Smith, *supra* note 81, at 563.

the account.[88] The security advantages of biometric identifiers are straightforward: while passwords can be stolen, lost, or cracked, biometric data belongs to one individual who already possesses a built-in password.[89] Because of the unique characteristics of each person, the use of biometrics introduces a higher standard of security, making password reproduction difficult.[90] Biometrics cannot be changed, forgotten, or lost, so they are a practical method for securing an account.[91] The use of biometrics also brings user convenience by freeing customers from remembering multiple passwords; users have their "passwords" with them at all times.[92] But whether this is a safer option is not an easy answer.[93] Part V will present the security problems that biometric data gathering poses to consumers.[94]

E. Biometric Data in Financial Institutions

Financial institutions are getting more comfortable digitizing their services to enhance consumer experience. Experts point to a new trend of using biometric data in the financial industry, the dominance of voice banking,[95] and the growth of biometric authentication.[96] Innovation is shaping the way we see the world and how we engage in simple transactions. More and more financial transactions are being executed online, which increases the risk of sophisticated attacks.[97] The solution, accepted by both institutions and consumers, is biometric identification, a convenient and secure replacement for traditional passwords.[98]

Biometric technology is no longer a commodity; it is a growing necessity for financial institutions, forcing banks to invest more in innovative services and to deliver secure transactions.[99] For example, MasterCard implemented the MasterCard Identity Check that uses facial

[88] Mike Faden, *Biometrics' Growing Role in Payment Services*, AMERICAN EXPRESS, https://www.americanexpress.com/us/foreign-exchange/articles/use-of-biometrics-for-payment-services/. *See also* Lemus, *supra* note 36, at 538.

[89] *See* Hansen, *supra* note 34.

[90] Faden, *supra* note 88.

[91] Sherman, *supra* note 71, at 667.

[92] Faden, *supra* note 88.

[93] Stroup, *supra* note 26.

[94] *See infra* PART V., at 27.

[95] *See* Hansen, *supra* note 34.

[96] Pinder, *supra* note 43.

[97] *Brief: The Latest In Biometric Banking And Payments*, MOBILE ID WORLD (May 24, 2018), https://mobileidworld.com/brief-biometric-banking-payments-905240/.

[98] *Id. See also* Pinder, *supra* note 43 (noting that financial institutions' customers are willing to accept the replacement of passwords with biometric identifiers due to the convenience of the process).

[99] Pinder, *supra* note 43.

recognition for security authentication.[100] Likewise, Visa USA Inc. and MasterCard International plan to prevent fraud by using point-of-sale finger-scanners, which verify whether the customer is the authorized credit card user.[101] Citibank and other banks and credit unions implemented voice biometric recognition, which identifies the customers based on their voices and eliminates the need to vocalize personal details over the phone.[102] U.S. Bank entered into a partnership with Amazon Alexa that allows customers to complete banking transactions using voice recognition.[103]

The innovations do not stop here. Many countries have already taken biometrics a step further, by introducing the Biometric Automated Teller Machine ("ATM").[104] South Africa,[105] India,[106] and China[107] are only a few of the countries in which financial institutions allow individuals to log into their accounts with nothing else but their presence. Although the United States has not implemented such a system yet, the innovation and desire to exceed consumer expectation is already pressing financial institutions to inquire into these systems.[108] Because the question is not "if," but "when," this technology has the potential to endanger consumers' privacy because consumers will face not only sharing the biometrics for authentication with their bank, but most likely with all banks.[109]

On a technical level, these technologies work by extracting the digital code from the consumer's biometric data and storing it either in

100 Sherman, *supra* note 71, at 664.

101 McGuire, *supra* note 11, at 455.

102 Sherman, *supra* note 71, at 668; *see also* Hansen, *supra* note 34.

103 *See* Stewart, *supra* note 22, at 356.

104 Alex Perala, *South African Bank Becomes Biometric ATM Pioneer*, FINDBIOMETRICS (May 7, 2018), https://findbiometrics.com/south-african-bank-biometric-atm-505075/.

105 *Id.*

106 Alex Perala, *Indian Authorities Developing Solar-Powered, Biometric ATM*, FINDBIOMETRICS (May 8, 2017), https://findbiometrics.com/indian-solar-powered-biometric-atm-4050895/.

107 Tracy Hu, *Finger Tech Points to Easier, More Secure Access to ATMs*, STANDARD (Jan. 31, 2018), www.thestandard.com.hk/section-news.php?id=192343&sid =11.

108 *See generally*, Robin Arnfield, *How biometric ATMs are entering mainstream use*, PAYMENTSOURCE (March 20, 2019), https://www.paymentssource.com/news/how-biometric-atms-are-entering-mainstream-use.

109 Financial institutions allow customers of other organizations to make certain transactions at their physical branches for which the customer must authenticate. In order to complete the transaction for another bank's customer, the biometric ATM would accept an individual's biometric for authentication. *See generally*, Steven Melendez, *Can a Debit Card From a Different Bank be Used at Another Bank?*, POCKET SENSE (May 19, 2020), https://pocketsense.com/can-debit-card-different-bank-used-another-bank-13211.html.

the financial institution's or a third party's database.[110] Although the data is encrypted, the legal framework in which we protect biometric data does not render sufficient protection. Given the nature of the information, new regulations that treat such information with extreme caution are necessary. The retention of biometric data should be limited, especially when the consumer's expectation matches this formula. Requiring the automatic deletion of such data after the consumer ends the relationship with the financial institution would make the technological development safer.

IV. CURRENT REGULATIONS AS APPLIED TO FINANCIAL INSTITUTIONS

"No victim is too big or too small. Everyone is a cyber-attack target, and it is only a matter of time before you become a victim."[111] When looking at the motives behind cyber-attacks, there is a clear pattern: money.[112] Accordingly, the financial industry, "a large pile of money," is the most vulnerable to hacks.[113] At the federal level, the United States does not have a general statute that protects biometric data. Instead, there are a few industry-specific laws that govern the use and collection of traditional data within the educational, commercial, financial, and healthcare industries.[114] GLBA, adopted in 1999, regulates financial institutions' use and collection of certain personal information, but not biometric data.[115]

The European Union ("EU") enacted the General Data Protection Regulation ("GDPR"),[116] one of the strictest regulations on data privacy that applies not only to EU organizations, but also to extraterritorial organizations.[117] Across the ocean, in the United Sates, a few states perceived the lack of regulations as a major problem and responded by enacting state laws that, to a certain extent, protect biometric data.[118]

---

110 McGuire, *supra* note 11, at 474.

111 Joseph Carson, *Key Takeaways from the 2019 Verizon Data Breach Investigations Report*, THYCOTIC (May 21, 2019), https://thycotic.com/company/blog/2019/05/21/2019-verizon-data-breach-investigations-report-takeaways/.

112 *Id.*

113 Chang, *supra* note 28, at 1218.

114 Stewart, *supra* note 22, at 364.

115 *See* Stewart, *supra* note 22, at 364; *see* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§6801–6809 (2012); *see infra*, PART IV. A., at 18.

116 EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679, 2016 O.J. (L 119) 1 [hereinafter "GDPR"]; *see infra* PART IV. B., at 20.

117 Jonathan Trebble-Greening, *Raising the Stakes: Creating an International Sanction to Generate Corporate Compliance with Data Privacy Laws*, 2019 COLUM. BUS. L. REV. 763, 773-74 (2019).

118 *Id.* at 774.

Nevertheless, these regulations differ in the level of protection provided to personal data subjects and make it confusing for companies, including financial institutions, to determine the exact regulation applicable.[119]

Part IV of this Comment will present why the current regulations do not sufficiently protect consumers' biometric data once their relationship with a bank terminates, with a focus on GLBA, GDPR, and New York and California state laws.[120]

A. Gramm-Leach-Bliley Act of 1999

"It is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers' nonpublic personal information."[121] Enacted with the purpose of removing barriers among banks, insurance companies, and brokerages, GLBA brought new consumer protection measures to consumers' "nonpublic personal information."[122] GLBA's definition of "nonpublic personal information" includes "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution," other than publicly available information.[123] Thus, this definition would include passwords or any method of authentication used by a customer to access an account. GLBA established new obligations for financial institutions[124] that relate to privacy notice to consumers, disclosure of information to third parties, and safeguards against unauthorized access.[125]

GLBA also established guidelines regarding consent and disclosure that financial institutions must provide to their customers: an initial and annual clear and conspicuous notice describing information-sharing procedures.[126] The notice must include the personal information

119 *Id.* at 774-75.

120 *See infra* PART IV. C., at 24.

121 Gramm-Leach-Bliley Act § 501, 15 U.S.C. § 6801 (2012).

122 *See* Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 BERKELEY J. INT'L L. 939, 947 (2006). "Nonpublic personal information" is "personally identifiable financial information" acquired from the consumer while performing a transaction. *Id.*

123 *See* Gramm-Leach-Bliley Act § 509(4)(A).

124 GLBA defines financial institution as "any institution the business of which is engaging in financial activities." Packin, *supra* note 10, at 1255.

125 Meena Aharam Rajan, *The Future of Wallets: A Look at the Privacy Implications of Mobile Payments*, 20 COMMLAW CONSPECTUS 445, 459 (2012). *See also* Fonte, *supra* note 54, at 591.

126 Fonte, *supra* note 54, at 591; Boyd, *supra* note 122, at 947. The Federal Trade Commission ("FTC") is responsible with enforcing GLBA's provisions and it imposes

collected, any practices regarding the disclosure of such information to non-affiliated third parties, and policies meant to protect the confidentiality and security of the customer's information.[127] GLBA also provides that a financial institution cannot share the personal information with a non-affiliated third party unless it provides the consumer with an opportunity to "opt-out" and a notice of that right.[128] Although seemingly a great protection, this rule has many exceptions that only diminish the protection of data.[129]

Enacted in 1999, when the use of biometrics was primarily limited to governmental use, the Act does not make any reference to biometric data.[130] Whether the definition of "nonpublic personal information" includes such data and the extent of its protection, if any, is uncertain. At the time of enactment, technology, like computers, was just taking widespread foothold and biometric data use was limited to certain governmental uses.[131] GLBA's drafters could not have predicted or understood the modern-day use of biometric data.

Further, GLBA makes a noticeable difference between *customer* and *consumer* regarding the level of protection afforded to each.[132] Under GLBA, a "consumer" is an "individual who obtains or *has obtained* a financial product or service from [a financial institution] that is to be used primarily for personal, family or household purposes, or that individual's legal representative," while a "customer" is a consumer who has a "*continuing relationship*" with the financial institution.[133] In other words, someone that *has obtained* a financial product or service, but has terminated the *continuing relationship* with the financial institution, is considered a consumer, and not a customer. This distinction between

specific standards that can assure the confidentiality and security of the customers' record. Julia C. Schiller, *Informational Privacy v. The Commercial Speech Doctrine: Can the Gramm-Leach-Bliley Act Provide Adequate Privacy Protection?*, 11 COMMLAW CONSPECTUS 349, 356-57 (2003).

127 Boyd, *supra* note 122, at 947.

128 Boyd, *supra* note 122, at 947. The "opt-out" rule allows the consumer to choose not to share the personal information with nonaffiliated third parties.

129 Schiller, *supra* note 126, at 358-59. One of the exceptions when the financial institution is not required to provide an opportunity to opt-out is when it shares the personal information with its affiliates. Moreover, the requirement may not apply even when the information is shared with a nonaffiliated third party that performs services of marketing for the financial institution, although the third party must agree to maintain confidentiality.

130 *See infra* PART III., at 6.

131 *See generally*, Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE.COM, https://www.biometricupdate.com/201802/history-of-biometrics-2.

132 *See* 16 C.F.R. § 313.3(e)(1), (h)-(i)(1) (2011).

133 16 C.F.R. § 313.3(e)(1), (h)-(i)(1) (emphasis added).

customer and consumer is important when looking at GLBA's safeguard requirements.[134]

Financial institutions must ensure data security by assessing risks, creating and monitoring safeguard programs, and guaranteeing the confidentiality of the *customer*'s personal data.[135] A financial institution is not required to safeguard the data once the customer becomes a *consumer* by terminating the relationship with the financial institution. In this case, to comply with record retention requirements, the financial institution can, and must, retain the data, but it does not have to assure full protection. Furthermore, a financial institution does not need to implement the highest standards of protection.[136] It needs to implement only the security measures that the institution determines is appropriate.[137] GLBA also allows states to impose their own regulations with regard to privacy laws, which contributes to discordance across the country.[138] For example, in Connecticut, where the state law does not require institutions to implement intensive security measures, Citibank was the victim of a security breach that affected more than 360,000 customers because of an undetected vulnerability.[139] It is fair to say that if some states do not perceive the lack of regulations as a major problem, their citizens will remain vulnerable to attacks. This is important because most consumers do not read or understand banking privacy policies.[140] When acquiring a product, most individuals do not look beyond what the institution tells them, therefore, the consumers lack the necessary knowledge.[141] If a product or service is popular, potential consumers are less likely to spend time reading the terms and conditions; consumers will instead assume that the terms are reasonable.[142] Even when they do freely consent to personal data disclosure, consumers do not realize the ramifications of such a decision or the nature of the data-trade agreement.[143]

134 Rajan, *supra* note 125, at 460.

135 Rajan, *supra* note 125, at 460.

136 Schiller, *supra* note 126, at 363-64.

137 Schiller, *supra* note 126, at 363.

138 Chang, *supra* note 28, at 1209.

139 Chang, *supra* note 28, at 1209.

140 *See* Schiler, *supra* note 126, at 362 (explaining a study regarding the readability of privacy notices found that they were written at a third-year college level or above, while the accepted standard for the general public is an eighth-grade reading level.); *see also* Packin, *supra* note 10, at 1278.

141 *See* Elvy, *supra* note 33, at 442.

142 Packin, *supra* note 10, at 1279.

143 Elvy, *supra* note 33, at 442.

Biometric data is different because it is unique to each individual and incapable of being changed, therefore, the legislatures must treat it differently from any other type of data.[144] Consumers, without a regulators' aid, have no power to prevent the collection of such data.[145] The consumer must have the right to decide whether to allow the collection, use, or disclosure of the data.

B. General Data Protection Regulation: The European Union

While the United States lacks general regulations of biometric data at the federal level, the EU has adopted regulations for "any entity's accumulation of large amounts of data," increasing consumers' protection throughout Europe and beyond.[146] The GDPR, one of the strictest of Europe's regulations, applies to EU organizations and globally to any organization that offers goods or services to EU subjects; the GDPR regulates companies that have access to the personal data of EU residents, regardless of the company's location.[147] Because of this, the GDPR will affect markets in the United States, including American financial institutions.[148]

Under the GDPR, "personal data" includes "any information . . . concerning an identified or identifiable natural person," a different concept from the type of data that encompasses the authentication of an individual in the United States, such as driver's license number, financial account, or Social Security Number.[149] Thus, the GDPR protects a wide range of data, from very obvious identifiers such as a name, account number, or IP address, to any data that could be tied to an individual,

144 *See* Sherman, *supra* note 71, at 670; Kelly Sheridan, *Biometric Data Collection Demands Scrutiny of Privacy Law*, INFORMATION WEEK IT NETWORK (Oct. 2, 2020), https://www.darkreading.com/endpoint/biometric-data-collection-demands-scrutiny-of-privacy-law/d/d-id/1339079.

145 *Id*.

146 STEPHEN P. MULLIGAN, WILSON C. FREEMAN & CHRIS D. LINEBAUGH, CONG. RESEARCH SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 40 (Mar. 25, 2019); *see also* Trebble-Greening, *supra* note 117, at 771-72 (explaining GDPR, which replaced Data Protection Directive (95/46/EC) of 1995, carries heavy penalties, fines up to $22.5 million, for any entity that abuses citizens' personal data).

147 Trebble-Greening, *supra* note 117, at 773-74.

148 Tyler Stites, *Development in Banking & Financial Law: XI. Data Protection on the Doorstep: How the GDPR Impacts American Financial Institutions*, 38 REV. BANKING & FIN. L. 132, 139 (Fall, 2018); *see also* Lindsay A. Seventko*, GDPR: Navigating Compliance as a United States Bank*, 23 N.C. BANKING INST. 201, 208-09 (March 2019) (GDPR is more comprehensive than any U.S. privacy law; any institution that operates or solicits customers abroad needs to update its privacy policies and afford the same level of protection. These new regulations could also influence competition in the financial institutions.).

149 Seventko, *supra* note 148, at 211; GDPR, *supra* note 116, at Recital 26.

even pseudonymous data.[150] The GDPR not only protects data that can directly identify an individual, the law also protects any unidentifiable data that, in the aggregate with other such data, results in indirect identification.[151]

The GDPR employs an innovative measure that requires customer consent on how, and by whom, their personal data will be used.[152] The consent requirement forces institutions to abandon the inclusion of a "laundry-list" of permissions which are usually buried deep within terms and conditions.[153] Banks that adopt the use of biometric identifiers for account access must be transparent with how the data is stored, used, and shared with third-party developers for marketing purposes.[154] The customer must affirmatively consent to *each* collection and to *each* process of personal data that the institution deems necessary for the initial or permissible purpose.[155] A consumer must be able to clearly and easily find these purposes in the form.[156] A broad interpretation of the word "necessary" allows banks to avoid the GDPR's application by including many purposes in their terms, resulting in a lack of actual change in their data processing.[157] For example, banks may argue that using such data is necessary to further a permissible

[150] Seventko, *supra* note 148, at 212, 220 (explaining that data subjects maintain some rights over their data including: the right to erasure, the right to use, the right to edit, the right to portability, and the right to restrict). *See* GDPR, *supra* note 116, at Article 4, ¶5 (The GDPR defines pseudonymization as "the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information.").

[151] Seventko, *supra* note 148, at 212.

[152] *See generally A Step-by-Step Checklist for Meeting GDPR Consent Requirements*, FOCAL POINT DATA RISK (Feb. 27, 2018), https://blog.focal-point.com/a-step-by-step-checklist-for-meeting-gdpr-consent-requirements. Under GDPR, consent requires customers to be made fully aware, in a clear, concise and transparent manner, of how their personal data will be used and by whom. Essentially, it must be: (1) separate; (2) in clear and plain language; (3) as easy to withdraw as it is to give; and (4) not a required contractual condition if it the provision is not necessary for completing the processing.

[153] Seventko, *supra* note 148, at 218.

[154] Seventko, *supra* note 148, at 219; *See also* Sylvain, *supra* note 21, at 1092-93 (noting that companies cannot share the user's information with a third party for a purpose that is "incompatible" with the initial purpose for which the user shared the data).

[155] *See* Seventko, *supra* note 148, at 216 (stating process will be considered necessary if the banks can show that the results of the processing would not be achieved without the processing).

[156] Rebecca Sentence, *Six agreeable examples of GDPR ready opt-in forms*, USER ZOOM, https://www.userzoom.com/ux-library/six-agreeable-examples-of-gdpr-ready-opt-in-forms/ (presenting effective opt-in forms for user's consent under GDPR).

[157] *See* Seventko, *supra* note 148, at 216-19.

purpose, such as public interest, historical research, or advertising.[158] Moreover, the regulations lack any reference to whether the biometric identifiers are afforded the same extent of protection as extended to traditional passwords when they face risks of which the consumer is unaware.[159]

The GDPR's most innovative provision is the right to be forgotten, which gives customers the right to ask for the erasure of their data.[160] Although financial institutions view such requests as problematic because they conflict with their record retention policies, this can be viewed as a solution that incentivizes financial institutions to reorganize their data retention procedure.[161] The GDPR's right to be forgotten provision requires banks to update their data more often, establish limited purposes for data retention, avoid clusters of useless information, and set up systems that would facilitate deletion when the retention period expires.[162]

Although the measure is a step closer to better protection, giving the customer at least some rights to his or her own information, it still fails to provide sufficient protection to customers who ended the relationship with the financial institution. Generally, customers do not know the extent of data that the bank holds, or what type of information institutions must retain to meet their recordkeeping requirements.[163] A former customer should not risk inadequate protection that could irreversibly compromise their biometric data simply because such a risk is not easily discerned. Furthermore, while an erasure request from a current customer could create difficulties for any future transactions, automatic deletion of biometric identifiers for former customers does not pose any operational difficulties to the financial institution.

C. State Privacy Laws: New York and California

---

158 Seventko, *supra* note 148, at 219. If the data is collected in a lawful manner, it does not need to be deleted after it is no longer necessary and can be used for different purposes without the need of additional consent; *see also* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 484, 550-52 (2019).

159 *See* Seventko, *supra* note 148, at 219.

160 Seventko, *supra* note 148, at 220-21; Wachter, *supra* note 158, at 550-51 (explaining that the GDPR allows customers to request deletion of their personal information when they withdraw their consent, when they object to data processing, and the bank does not have legitimate grounds for the data, or when the data is no longer needed).

161 *See* Seventko, *supra* note 148, at 220-21.

162 Seventko, *supra* note 148, at 220-21.

163 Maja Majewski, *How Do Banks Work?*, SIMPLE, https://www.simple.com/blog/how-do-banks-work.

The inadequate federal protection of biometric data has forced states to either incorporate biometric data into the definition of personal information, or to specifically address the collection of biometric data and recognize the unique characteristics of such information through legislation.[164] With the GDPR serving as an example, several states implemented similar policies that demand heightened protection of their citizens' personal and biometric data.[165] Although, in the financial industry, the GLBA allows states to afford greater protection to their citizens, a majority of state legislatures that enacted laws to protect biometric data chose not to enforce them against financial institutions or their affiliates subject to the GLBA.[166]

New York became the first state to enact cybersecurity legislation for financial institutions to protect biometric data against cyberattacks, recognizing that digital innovation comes with sophisticated threats.[167] The New York State Department of Financial Services ("NYDFS")[168] implemented a cybersecurity regime that imposes certain minimum requirements on financial institutions and their third party service providers.[169] The NYDFS requires financial institutions to maintain cybersecurity programs that protect the confidentiality of the institution's electronic database in order to safeguard consumer information.[170] Although a promising initiative, New York's regulation might not afford the much-needed protection against both data breaches and unauthorized third-party use.[171] Entities covered under NYDFS' regime conduct their own risk assessment for the means of establishing the required cybersecurity program; however, this is nothing more than a process that grants institutions a great deal of leeway in deciding what is necessary.[172] Although the system must include procedures for data retention and policies for the disposal of

164 Sherman, *supra* note 71, at 672-76. The Illinois Biometric Information Privacy Act, enacted in 2008, defines "biometric identifier" as retina or iris scan, voiceprint, fingerprint, face or hand scan geometry. Under this law, writing samples, signatures, photographs, or physical descriptions are not biometric identifiers. Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/25(c) (2008).

165 Stites, *supra* note 148, at 142; *see also* Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6807(b) (1999).

166 *See, e.g.*, Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/25(c) (2008).

167 Knerr, *supra* note 76, at 540-41.

168 N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2017) [hereinafter "NYDFS"].

169 *See* Knerr, *supra* note 76, at 542.

170 Knerr, *supra* note 76, at 542, 544-45 (explaining program must perform certain cybersecurity tasks and should have an incident response plan to respond and recover from any event that could affect the electronic database confidentiality).

171 *See* Knerr, *supra* note 76, at 543.

172 *See* Knerr, *supra* note 76, at 543.

unnecessary data, ultimately, the financial institution *subjectively* decides what is "necessary."[173]

Under the NYDFS, the scope of "nonpublic information" is broader than under the GLBA as it encompasses all nonpublic electronic information, including information that is not personally identifiable or financial.[174] Although NYDFS is a good starting point for cybersecurity regulation, the regulation allows too much freedom for financial institutions to set their own compliance standards and does not go far enough to protect the biometric data of former customers.

California also took a big step in protecting customer data by adopting many of the GDPR's provisions and setting a heightened standard for compliance.[175] Because many financial institutions are incorporated in California, and even more do business there, the California Consumer Privacy Act of 2018 ("CCPA") was an important change with the potential to affect most of the United States' financial institutions.[176] Unfortunately, the CCPA did not meet its potential. Instead of changing its practices and adopting heightened protections for consumers, financial institutions only changed their standards for California residents.[177] Regardless, even if banks were to apply the regulations nationwide, the CCPA is still limited in application because it only provides narrow protection for financial data.[178] Particularly, the CCPA has a carve-out for institutions regulated by the GLBA—but only

[173] Knerr, *supra* note 76, at 544-46. The system must include schedules for monitoring and testing the program's effectiveness, restrictions on in-house developed applications, and encryption to protect confidential information. The financial institution must also retain all compliance information for five years after the relationship ends and a record of identified risks, remediations, and account of how future risks will be addressed.

[174] Michael Krimminger, *New York Cybersecurity Regulations for Financial Institutions Enter Into Effect,* HARV. L. SCH. F. ON CORP. GOVERNANCE (Mar. 25, 2017), https://corpgov.law.harvard.edu/2017/03/25/new-york-cybersecurity-regulations-for-financial-institutions-enter-into-effect/. The GLBA's protection of nonpublic personal information is limited to personally identifiable financial information. NYDFS protects business-related information—information that, together with other data, could indirectly identify the customer and health care information.

[175] Stites, *supra* note 148, at 142.

[176] Stites, *supra* note 148, at 143; *see, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2018).

[177] *See, e.g.*, BANK OF AMERICA, *California Consumer Privacy Act Disclosure*, (Jan. 1, 2020), https://www.bankofamerica.com/security-center/ccpa-disclosure/.

[178] Luke Dembosky et al., *The California Consumer Privacy Act: Compliance Strategies for Financial Institutions*, DEBEVOISE & PLIMPTON (May 2, 2019), https://www.debevoise.com/insights/publications/2019/04/the-california-consumer-privacy-act.

regarding information collected "pursuant to" the GLBA.[179] Thus, everything outside the scope of the GLBA will be regulated by the CCPA's broad definition of "personal information."[180] Although the CCPA grants consumers the opportunity to ask financial institutions to delete their personal information and to not sell it to third parties, consumers' biometric data does not fall under the CCPA's protection.[181] Rather, biometric data only falls under the GLBA as being nonpublic personal data arising from a customer-bank relationship.[182]

Unfortunately, none of these regulations sufficiently protect biometric data after the customer becomes a consumer. The legislature should value the privacy of citizens more than the interests of businesses and make a clear distinction between a financial institution's on-going and former customers.

V. SECURITY PROBLEMS IN THE BIG DATA WORLD

"Big data" is an "unstoppable natural force" of information that companies rush to process.[183] This data overflow presents novel issues for financial institutions regarding consumer privacy. Even if banks do not sell consumers' personal information, the GLBA allows banks to release this data to third parties that either act on the bank's behalf or share a marketing arrangement with the bank.[184] When biometric data is securely stored by a company, the information is still part of the company's consumer database and could be disclosed to third-parties by assignment.[185] In other words, third parties have access to personal information and consumers are either unaware or powerless to do anything about it. Even more alarming is the fact that consumers who have terminated their relationship with a bank are just as vulnerable to

[179] David J. Oberly, *Analyzing the California Consumer Privacy Act's Impact on Financial Institutions*, CREDIT UNION TIMES (Aug. 26, 2019, 12:17 PM), https://www.cutimes.com/2019/08/26/analyzing-the-california-consumer-privacy-acts-impact-on-financial-institutions/?slreturn=20190819214005.

[180] *Id*; Dembosky, s*upra* note 178 (defining personal data under the CCPA as any data 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.").

[181] *See* Dembosky, *supra* note 178.

[182] *See* Dembosky, *supra* note 178. *See supra* note 133. Under GLBA, a "consumer" is an "individual who obtains or *has obtained* a financial product or service from [a financial institution] that is to be used primarily for personal, family or household purposes, or that individual's legal representative," while a "customer" is a consumer who has a "*continuing relationship*" with the financial institution.

[183] Gill, *supra* note 46, at 462-63.

[184] McGuire, *supra* note 11, at 465-66 (noting that telemarketers have access to private information).

[185] Elvy, *supra* note 33, at 458-59. The assignee could use the data to identify the individuals.

having their information, including biometric data, distributed to third parties.

But why do private and public institutions have access to so much data in light of regulations that emphasize the importance of consumer consent? One answer could be that institutions determine the extent of their access to personal information through their privacy policies and, more often than not, these provisions authorize the sale, transfer, or disclosure of consumer data to third parties.[186] The extent of the individual's consent determines whether he or she can be held accountable for the use of personal data by the contracted party.[187] Yet, this principle *assumes* that contract provisions are unambiguous and that individuals actually understand what they consent to. History teaches that this assumption is far from reality.[188]

Financial institutions improve their products by outsourcing their services to third parties and allowing these third parties to access consumer information.[189] For example, third parties typically run an institution's mobile applications, which gather and store customer information.[190] As financial institutions become more digitized, their platforms have enormous capacity to indefinitely store digital records—including individuals' personal information.[191] Even more alarming is that there is no regulation requiring financial institutions to delete this sensitive information. For example, more banks are using FaceID to authenticate users, and unfortunately, more banks are sharing this data with third party developers for marketing purposes.[192] Users may not be aware of the risks or extent of this subsequent data use at the time consent is given.[193] The ambiguity of consent agreements, coupled with

[186] Elvy, *supra* note 33, at 440-41. Clear, a company that collects and uses biometric data for customer authentication, allows the customers' biometric data to be transferred to a new company pursuant to a buy-out of the company. Amazon and Apple have privacy policies that mirror Clear's.

[187] *See* Anne S.Y. Cheung, *Moving Beyond Consent For Citizen Science in Big Data Health and Medical Research,* 16 NW. J. TECH. & INTELL. PROP. 15, 16-17 (2018).

[188] *See* Schiller, *supra* note 126, at 356 (discussing a lawsuit where a bank that assured data confidentiality disclosed its customers' personal information to a telemarketing firm).

[189] Isabel Peres, *The Evolution Of Banking: A Flexible Fiduciary Duties Approach Will Help Better Protect Mobile Banking Consumers*, 2015 U. ILL. J.L. TECH. & POL'Y 211, 221 (2015).

[190] Moussa, *supra* note 13, at 352.

[191] Moussa, *supra* note 13, at 347.

[192] Seventko, *supra* note 148, at 219.

[193] Cheung, *supra* note 187, at 15.

the unknown value of personal data, prevents consumers from fully understanding the scope of their consent.[194]

Even when users are careful, biometric identifiers generate risks because most of the time this data gathering occurs without an individual's knowledge.[195] Although the regulations require third parties with access to non-public personal information to implement and maintain appropriate security measures, this does not always happen.[196] Many of these third-party companies guarantee high security and have "no third-party access" policies, but breaches still occur.[197] Companies are well aware of such threats and try to limit potential liability by entering into warranty and licensing agreements with customers.[198] So, while banks cannot limit liability directly, they do so indirectly. This danger manifests when companies store sensitive information in databases and servers susceptible to hacking and data exfiltration.[199] Indeed, recent cases illustrate the lackluster security that these third-party platforms maintain. In 2018, JP Morgan Chase sued Landry, a hospitality chain, over a data breach caused by a faulty program installed on payment devices.[200] In 2015, various banks also sued Wendy's for a breach when malware attacked its point-of-sale system, granting unfettered access to third-party vendor credentials.[201]

Although biometric authentication comes with many advantages, users tend to worry once they discover the amount of personal information institutions can access.[202] More than half of all users choose not to install applications that use personal data after learning of the inherent danger in doing so.[203] The idea of someone stealing biometric data is not as absurd as some companies would lead customers to believe.[204] Just as hackers have found ways to steal passwords and other

194 Elvy, *supra* note 33, at 442-43.

195 *See* Elvy, *supra* note 33, at 452.

196 Fonte, *supra* note 54, at 594-95.

197 Elvy, *supra* note 33, at 453.

198 Elvy, *supra* note 33, at 453. For example, when Apple implemented Touch-Id, a program using a "mathematical representation" of scanned fingerprints, it assured users of the impossibility that someone could reverse engineer their fingerprints. However, Apple still limited its liability for "damage to, compromise, or corruption of data."

199 *See* Elvy, *supra* note 33, at 453-54.

200 Joseph V. DeMarco & Brian A. Fox, *Data Rights and Data Wrongs: Civil Litigation and the New Privacy Norms*, 128 YALE L.J. 1016, 1019 (2019). The program read the cardholder's name, expiration data, card number, and CVV number.

201 *Id.*

202 Lemus, *supra* note 36, at 541.

203 Lemus, *supra* note 36, at 541.

204 Stroup, *supra* note 26.

account information, hackers will find ways to steal biometrics.[205] One difference between traditional data and biometric data is the means of replacing compromised information.[206] A breach affecting customer's traditional passwords might not conclude in a full recovery because prosecution cannot undo the harm already caused, but passwords can still be changed and identity theft reports filed.[207] In contrast, biometric identification can never be changed.[208] With just one breach, half of the U.S. population could lose their most personal data, which cannot be replaced. A database containing biometric information must be both adequately protected and purged of sensitive information when such information no longer benefits the consumer.

VI. Proposal for Automatic Deletion of Biometric Data Stored by Financial Institutions After the Consumer-Bank Relationship Terminates

While biometric identification is a fast-emerging technology with many advantages, it also has the potential to bring about a multitude of problems for private citizens. In order to avoid some of these problems, the government should either: (1) amend the GLBA to prevent financial institutions from storing biometric data after the customer-bank relationship ends; or (2) enact a comprehensive federal law that regulates the collection and use of biometric data, including a requirement to automatically delete a user's biometric data when users close their account with an institution. Reality shows that biometric data is necessary during an on-going customer relationship, but such data has no value to the customer or government once the account closes. Automatically deleting biometric data at the end of a business relationship would not affect the retaining principle or the financial institution's relationship with third parties because the data does not qualify as necessary data under the retaining requirements.

Banks generally retain consumers' biometric information with the goal of allowing users a better experience and faster access to their accounts. Thus, once consumers terminate their relationship with a bank, they expect the institution to delete their data. Even if consumers later resume their business with the institution, the first few authentications can be conducted by traditional means. In a digitalized world, government's reliance on outdated statutes in protecting biometric data is inadequate. Although financial institutions are highly

205 *See* Stroup, *supra* note 26.
206 Stroup, *supra* note 26.
207 Smith & Mulrain, *supra* note 81, at 564.
208 Stroup, *supra* note 26.

regulated and often voluntarily establish high standards of compliance, the battle for "big data" can persuade them to replace these standards and become complacent. Because financial institutions rarely experience data breaches, they believe that they have established appropriate strategies and are able to keep customer information safe.[209] But the dangers posed by payment industries are considerable; banks should always be alert, with the highest degree of security, and retain only the necessary data.[210] It is glaring that a smart hacker will try to hit where the money is.[211]

Although the use of biometric identification technology is more secure, the technology is still too new to be able to make an exact prediction of future problems.[212] History teaches us that nothing is impossible, and that applies to biometric data as well.[213] If a hacker found a way to steal a password, he can find a way to steal the biometric data. The difference is that passwords and cards can be replaced, but no one can issue a new set of biometrics.[214] The need of protecting individuals' privacy outweighs financial institutions' value in such data. Unfortunately, the intense commercial activity obscures the source of the data, which is human beings who lost the access and control over their own personal information.[215] Companies' shifts toward "data grab" assures them "a cut" to valuable information and their position in the market.[216] This is even more alarming when statistics show that private individuals create approximately 70 percent of data; and most of it—80 percent—is stored by enterprises.[217]

Retaining the biometric data after the consumer terminates the relationship with the financial institution presents concerns regarding the individual's privacy due to the ease of transferability involved. Consumers are in a vulnerable position due to lack of information and control, which creates a moral duty for institutions and legislators to take reasonable precautions to avoid harming the consumer.[218] An

209 *See* Packin, *supra* note 10, at 1267.

210 Packin, *supra* note 10, at 1267.

211 *See* Packin, *supra* note 10, at 1267 ("If you're a terrorist, what better way to get in to disrupt the financial condition of the United States of America than go to one of their back rooms.").

212 *See* Stroup, *supra* note 26.

213 *See* Stroup, *supra* note 26.

214 *See* Stroup, *supra* note 26.

215 Gill, *supra* note 46, at 463.

216 Fonte, *supra* note 54, at 566.

217 De Groot, *supra* note 72.

218 *See* Hilary G. Buttrick, Jason Davidson, & Richard J. McGowan, *The Skeleton of a Data Breach: The Ethical and Legal Concerns*, 23 RICH. J.L. & TECH. 2, 7-8 (2016).

individual that just ended the relationship with the financial institution knows that the biometric data shared with the organization is unique and immutable, but does not expect the bank to hold on to such data in perpetuity.[219] It would also be highly unlikely for the individual to voluntarily allow such a retention.

While CCPA sounded promising, due to its strong incentive to push financial institutions to think twice about limiting their data retention to only necessary information, banks chose not to impose such principles nationwide; instead, they only apply the restrictions to the State of California or California citizens.[220] This limitation shows the desirability of a uniform biometric law at the federal level that would give consumers the right to direct or delete their data and, at the same time, require institutions to automatically delete the data. The automatic deletion would also encourage fewer data transactions between institutions because banks would become more careful when contracting with third parties by making sure that the automatic deletion is possible. The limitations imposed by financial institutions when implementing CCPA also show that banks find the data produced by the customers valuable and try their best to limit the application of data-protective regulations.

Legislators must assure an environment that supports the development of technology, but at the same time improves the protection of personal information.

VII. CONCLUSION

The current regulations discussed herein do not adequately protect the privacy of biometric information acquired by financial institutions.[221] The growing increase in biometric use in financial industry coupled with the high vulnerability of mobile banking applications raises many concerns, bringing banks first in line for much-needed legislation.[222] In an emerging economy, implementing new technologies can spur economic growth, but the legislature must face these challenges. Resistance to implementing new regulations because something "bad" did not yet happen leaves society vulnerable. The

219 *See* Ashton McKinnon, *Sacrificing Privacy for Convenience: The Need for Stricter FTC Regulations in an Age of Smartphone Surveillance*, 34 J. NAT'L ASS'N L. JUD. 484, 503 (Fall 2014).

220 *See* BANK OF AMERICA, *supra* note 177.

221 McGuire, *supra* note 11, at 475.

222 Chang, *supra* note 28, at 1207, 1219. Mobile banking applications for IOS systems are vulnerable to attacks because of their "unsecured security communications and data storage, vulnerabilities in the code, failure to authenticate certificates and running on phones despite the phones being jailbroken."

present regulations applying to financial institutions do not sufficiently protect individuals' biometric data and, considering the high level of privacy and customers' expectations, regulations providing for an automatic deletion of such data when the customer closes its account are necessary.