Data Privacy Laws Targeting Biometric and Geolocation Technologies

*By Erin Jane Illman**

I. Introduction

Technology and the use of smartphones have created a world of anywhere, anytime convenience. Customers now demand the ability to make transactions on the go and expect to use geolocation data, or information about their specific location, to improve their experience. Mobile applications often use geolocation, and customers often rely on geolocation to obtain basic services from those apps, including receiving turn-by-turn directions, checking the weather, locating the nearest brick-and-mortar storefront, identifying the closest ATM, or receiving customer-specific advertising or deals offered by nearby retail and restaurant locations.

Along with the rise of geolocation, many applications now utilize biometric authentication, such as a fingerprint scan. Biometric authentication adds an additional layer of security. For example, a customer who seeks to make a purchase, access a mobile application, or perform various other mobile tasks and transactions may be required to provide a fingerprint scan before the application will allow the user to access personal and sensitive data.

These technologies are often seen as necessary to help safeguard personal data and serve as useful tools in identifying fraudulent transactions. As the advantages and popularity of geolocation and biometrics in the mobile industry increase, so have concerns of privacy advocates and regulators who are concerned that these technologies have the potential for abuse if data is compromised.

Traditionally, lawmakers have addressed the problem of data security primarily through legislation aimed at preventing or properly notifying consumers and regulatory agencies of the unauthorized disclosure and potential misuse of numerical or factual data associated with the user. Recently, however, lawmakers are focusing instead on the collection and use of data associated with the device, as well as that associated with the user's biological identifiers. There are obvious concerns with data that tracks an individual's location, as well as data associated with a person's biological characteristics, and states are beginning to take a more

* Erin Jane Illman is an ANSI Certified Information Privacy Professional (CIPP/US) and an attorney in the Charlotte offices of Bradley Arant Boult Cummings LLP. She can be contacted at eillman@bradley.com.

active role in regulating these types of data. This survey will explore the characteristics of geolocation and biometric data and its use, as well as the recent regulatory and legal focus on geolocation and biometric data privacy and consumer protection.

II. Biometric Legislation—Three States and Counting

Biometric data is generally defined as data associated with a unique individual biological characteristic, such as a fingerprint, retinal or iris scan, or voice pattern.[1] In other words, biometric data could include data associated with an individual's anatomy, biology, and/or characteristics of his or her physiology. There are general exceptions to what is considered a biometric identifier. For example, information collected for healthcare treatment, along with physical descriptions of an individual, signatures, and data related to diagnostic, genetic, or scientific testing, is typically excluded.[2] Biometric data is often referred to as a biometric identifier, which, as the name implies, is data associated with a person's biological marker that can later be used to identify that specific individual.

In 2008, Illinois became the first state to enact legislation to regulate the collection, use, and retention of biometric information with the passage of the Biometric Information Privacy Act ("BIPA").[3] Illinois' BIPA makes it illegal for a company to collect an individual's biometric identifier or information, unless the company first informs the person in writing and discloses the specific purpose and length of time for which the data is being collected, stored, or used. The company must also obtain written consent from the individual before it obtains the biometric data.[4] The term "biometric identifier" is defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[5] BIPA further requires the company in possession of the data to protect the security of the information.[6]

The use of biometric identifiers under BIPA has been the subject of litigation. In one recent case, plaintiffs alleged that Google created unique facial templates from photographs uploaded to Google Photos.[7] Google then used the templates to find and aggregate other photos of plaintiffs and to recognize their gender, age, race, and location. Plaintiffs claim that these biometric identifiers are within the definition of BIPA and that Google failed to obtain proper consent and failed to disclose a publicly available data retention schedule as required under BIPA.[8] Google countered that BIPA specifically states that biometric identifiers do not

1. *See, e.g.*, 740 Ill. Comp. Stat. 14/10 (2016).
2. *See, e.g.*, *id.*
3. *Id.* 14/1–14/99.
4. *Id.* 14/15(b).
5. *Id.* 14/10. The definition excludes various other biological-related identifiers, such as photographs, height, weight, hair color, and eye color. *See id.*
6. *Id.* 14/15(e).
7. Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1090–91 (N.D. Ill. 2017).
8. *Id.* at 1091–92.

include photographs.[9] Google further argued that face-scan measurements of photographs do not qualify as biometric identifiers under BIPA, only face scans done in person. Nevertheless, on February 27, 2017, the U.S. District Court for the Northern District of Illinois entered an opinion and order stating that "nothing in the text of the Privacy Act [BIPA] directly supports . . . [Google's] interpretation. Nothing in the statute says, one way or the other, *how* the biometric measurements must be obtained (or stored, for that matter) in order to meet the definition of 'biometric identifier.'"[10] The court's decision in *Rivera* makes it clear that data obtained from non-biometric sources, such as photographs, may still be considered a biometric identifier under BIPA.[11]

Texas enacted a statute that regulates biometrics, which became effective in April 2009, titled the Capture or Use of Biometric Identifier Act ("CUBI").[12] CUBI requires companies to notify individuals and receive consent before collecting biometric information, but does not specify how notice must be conveyed or how consent must be obtained.[13] The statute's definition of "biometric indentifier" is almost identical to that of the Illinois BIPA.[14] CUBI also precludes a company that possesses biometric data obtained for commercial purposes from selling, leasing, or otherwise disclosing the information unless a limited exception applies.[15]

On May 16, 2017, Washington became the third state to enact a biometric privacy law.[16] Washington's new law, which became effective on July 23, 2017, defines biometric data as that which is "generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[17] The statute requires businesses that col-

9. *Id.* at 1092; *see* 740 ILL. COMP. STAT. 14/10 (2016) ("Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.").

10. *Rivera*, 238 F. Supp. 3d at 1095.

11. Other recent cases have addressed claims under BIPA. *See, e.g.*, Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499 (S.D.N.Y. 2017) (dismissing BIPA claims against a videogame maker related to a feature in the NBA 2K videogame series that allows users to scan their faces and create a personalized virtual avatar for in-game play, finding lack of standing and absence of injury); McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016) (dismissing complaint alleging that Smarte Carte violated BIPA by failing to obtain advance consent and inform plaintiff it would retain her fingerprint data and for what period of time due to lack of standing and failure to allege sufficient harm); *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155 (N.D. Cal. 2016) (denying motion to dismiss claims that Facebook violated BIPA by virtue of its facial recognition software, which collects and stores biometric information, in the form of face templates extracted from photographs uploaded to the website, in connection with its "Tag Suggestions" feature, without first obtaining informed written consent).

12. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2015).

13. *Id.* § 503.001(b).

14. *Id.* § 503.001(a).

15. *Id.* § 503.001(c).

16. H.R. 1493, 65th Leg., 2d Spec. Sess. (Wash. 2017) (to be codified at WASH. REV. CODE §§ 19.001.001–19.001.004).

17. *Id.* § 3(1) (to be codified at WASH. REV. CODE § 19.001.002(1)).

lect biometric identifiers to provide notice and obtain consent from an individual before collecting, converting, and storing biometric data for later comparison and matching to an individual.[18] The statute does not address or appear to apply to anonymous, de-identified biometric data.

Washington's law ends an eight-year drought on legislation as it relates to biometric data and appears to have signaled a renewal of interest in addressing consumer data privacy issues related to biometric data. As of mid-2017, five additional states have introduced bills governing the collection, use, and retention of biometric data. Massachusetts legislators are currently considering a bill that would add biometric information to its definition of "personal information," which is already regulated and safeguarded.[19] In New Hampshire, a proposed bill would impose restrictions on businesses that collect, use, or retain biometric data. The New Hampshire bill also creates a private right of action for any violation of the proposed law.[20] Alaska has proposed legislation that would impose a heightened consent requirement for the use, collection, or retention of biometric data.[21] Connecticut, meanwhile, has proposed legislation that would ban the use of facial recognition software for marketing purposes.[22] A fifth state, Montana, recently introduced a bill to impose heightened notice and consent requirements and to limit the sale and retention of biometric data.[23] While these bills are merely under consideration and may or may not be enacted, there appears to be a legislative focus on these issues. As more legislation pertaining to biometric data is passed, additional states will begin to focus on these technologies and the implications on consumer data privacy.

Data breach notification laws have historically focused on numerical or other personally identifying information. These laws have defined protected personal information to include personal data such as Social Security numbers, account numbers, and date of birth.[24] They generally do not include biometric information such as fingerprints, although there are some exceptions. For example, in 2015, the Connecticut legislature enacted a requirement that state contractors protect and report breaches of "confidential information" that is defined to include biometric data.[25] This renewed focus on biometric data may signal a potential expansion of current state data breach laws to include biometric data.

The focus on biometric data is not unwarranted, particularly given the rise in the development of digital identities. A digital identity is a digital version of your identity, in lieu of identity cards that you carry around. Given a growing marketplace for digital identities, many companies already use some form of digital

18. *Id.* § 2 (to be codified at Wash. Rev. Code §§ 19.001.001, 19.001.002).
19. H.R. 1985, 190th Gen. Ct. (Mass. 2017).
20. H.R. 523, 165th Gen. Ct. (N.H. 2017).
21. H.R. 72, 30th Leg., 1st Sess. (Alaska 2017).
22. H.R. 5522, 2017 Gen. Assemb., Jan. Sess. (Conn. 2017).
23. H.R. 518, 65th Leg. (Mont. 2017).
24. *See, e.g.*, Ariz. Rev. Stat. Ann. § 18-545(L)(6) (2016); Ky. Rev. Stat. Ann. § 365.732(1)(c) (LexisNexis Supp. 2016); Tenn. Code Ann. § 47-18-2107(a)(4) (Supp. 2016).
25. 2015 Conn. Legis. Serv. P.A. 15-142 (S. 949) (to be codified at Conn. Gen. Stat. § 4e-70(a)(4)).

identity to verify payment information or provide other services. Some companies anticipate that digital identities will replace all forms of paper identification. As companies look to the future, many believe that drivers' licenses, passports, and other forms of identification will be replaced with digital identification that can be accessed and verified from anywhere in the world with a single fingerprint or eye scan.

On June 22, 2017, the National Institute of Standards and Technology ("NIST"), a part of the U.S. Department of Commerce, finalized a four-volume guidance document called *Digital Identity Guidelines*.[26] The *Guidelines* define "biometrics" as any "[a]utomated recognition of individuals based on their biological and behavioral characteristics."[27] Focusing on the "enrollment and verification of an identity for use in digital authentication," NIST recommends that biometrics be collected in the initial enrollment process, or when the customer signs up to create a digital identity, to later help prevent a registered subscriber from repudiating the enrollment and to help identify those who commit enrollment fraud.[28] The *Guidelines* require that any biometric data must be protected to ensure confidentiality, integrity, and attribution of the information source.[29] The rise in the use of these digital identities and the biometric data stored with them will likely be the subject of further regulation.

This new model of identity verification has many privacy advocates on edge. Biometric data, unlike traditional personal numerical identifiers, cannot be replaced or modified if compromised. Victims of identity theft can change their account numbers or taxpayer ID numbers, but facial geometry and fingerprints cannot be replaced. Privacy advocates therefore argue that biometric data must be prioritized in legislation and regulatory oversight.

III. Geolocation Legislation—Expect New Consent and Disclosure Requirements

The location of a mobile device may be determined by the interaction of that device with global positioning satellite signals, cell tower signals, or Wi-Fi access points. In June 2017, the Geolocation Privacy Protection Act ("GPPA") passed in

26. Paul A. Grassi et al., Digital Identity Guidelines (2017) (NIST Special Publication 800-63-3), https://doi.org/10.6028/NIST.SP.800-63-3 [hereinafter Digital Identity Guidelines]; Paul A. Grassi et al., Digital Identity Guidelines: Enrollment and Identity Proofing (2017) (NIST Special Publication 800-63A), https://doi.org/10.6028/NIST.SP.800-63a [hereinafter Enrollment and Identity Proofing]; Paul A. Grassi et al., Digital Identity Guidelines: Authentication and Lifecycle Management (2017) (NIST Special Publication 800-63B), https://doi.org/10.6028/NIST.SP.800-63b; Paul A. Grassi et al., Digital Identity Guidelines: Federation and Assertions (2017) (NIST Special Publication 800-63C), https://doi.org/10.6028/NIST.SP.800-63c.

27. Digital Identity Guidelines, *supra* note 26, at 49. Furthermore, the *Guidelines* include biometrics as protected "Personal Data," "Personal Information," and "Personally Identifiable Information." *See id.* at 56.

28. Enrollment and Identity Proofing, *supra* note 26, at ii, 32–34. The *Guidelines* provide "technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose." *Id.* at ii.

29. *Id.* at 7.

both houses of the Illinois legislature and is expected to be signed into law.[30] This legislation would prohibit certain tracking of another's location. Specifically, the GPPA provides that "a private entity may not collect, use, store, or disclose geolocation information from a location-based application on a person's device" unless it first provides notice and receives the person's "affirmative express consent."[31] "Geolocation information" is defined as "information that: (i) is not the contents of a communication; (ii) is generated by or derived from, in whole or in part, the operation of a mobile device, including, but not limited to, a smart phone, tablet, or laptop computer; and (iii) is sufficient to determine or infer the precise location of that device."[32] The notice must include "the specific purposes" for which the geolocation information will be "collected, used, or disclosed."[33]

Once the GPPA is in force, companies that track the location of customers through their mobile devices should review their permission process to ensure that customers are providing adequate consent under the statute. These new requirements may complicate the innovative nature of products and services offered by companies. For instance, if a company tracks the location of a customer through an application, but that application or service is expanded and the location is shared with additional parties, the company may have to notify the customer and obtain her consent. Companies must constantly reassess their notification obligations throughout the lifecycle of a product or service that utilizes geolocation.

A proposed Geolocational Privacy and Surveillance Act ("GPSA") was introduced in Congress on February 15, 2017.[34] The GPSA "seeks to establish a legal framework that gives government agencies, commercial entities, and private citizens clear guidelines for when and how geolocation information can be accessed and used."[35] The bill would prohibit companies from disclosing geographical tracking data without the customer's permission.[36] The bill also proposes a process that would allow government agencies to secure a warrant to obtain geolocation information.[37]

IV. What's Next? Expect More Legislation

As technology advances and becomes more commonplace, it is likely to continue to draw the attention of regulators, particularly state regulators. In the last twelve months, states have taken the laboring oar in addressing privacy issues

30. H.R. 3449, 100th Gen. Assemb., 1st Sess. (Ill. 2017).
31. *Id.* § 10(a).
32. *Id.* § 5. "'Geolocation information' does not include Internet protocol addresses." *Id.*
33. *Id.* § 10(a)(2).
34. H.R. 1062, 115th Cong., 1st Sess. (2017).
35. *Geolocation Privacy Legislation*, GPS.GOV (Aug. 14, 2017), http://www.gps.gov/policy/legislation/gps-act/.
36. *Id.*
37. *Id.*

relating to data collection from newer technologies such as geolocation and biometric data.

This trend is likely to continue. Businesses that have traditionally used technology as a "back room" tool are now fully embracing new technologies as a revenue-generating product. In fact, some sectors, such as banking and financial services, have created innovation labs and technology divisions that focus solely on improving the customer experience through technological advances. As more and more businesses take on the role of tech companies, legislation is bound to follow.