Biometric Information as Personal Information—A Brave New World of Regulatory Compliance

Marian A. Waldmann Agarwal and Adam J. Fleisher

04/04/2017

Privacy + Data Security

Client Alert

Participants in the consumer economy generally identify individuals by using characteristics that are associated with the individual such as: name, mailing address, phone number, driver’s license number, financial account numbers, or Social Security number—or by a device (such as by a cookie, a device identifier, or the unique characteristics of that device at a given point in time). In recent years, however, as computing power and technology have improved, a new way to identify individuals—by their innate physical, or “biometric,” information—has entered the market and appears on the cusp of becoming more widely adopted.

A core question is: what is the biometric information that needs protection? A voice recording for purposes of monitoring a customer service call, for example, is a far cry from a “voiceprint” that can be used to match a recorded voice to a person. If the two were conflated for purposes of regulation, it would create tremendous compliance challenges for existing services while also possibly stifling innovation in the field of biometrics.

Legislation taking shape varies but has tended to follow one of two possible approaches: (1) a risk-based approach that limits protections to some subset of biometric information generally based on whether it can be used to uniquely identify or authenticate an individual; or (2) adding to or interpreting the definition of personal or sensitive personal information to include biometric information resulting in biometric information being covered by existing data protection laws.

Companies seeking to employ biometrics to expand product offerings or increase data security or authentication might be surprised at the restrictions that apply in the various jurisdictions where they operate. We review existing restrictions in the United States, Europe, Canada, and Asia below to give a sense of potential pitfalls and concerns presented by use of biometrics in the global marketplace.

United States Considerations

In the United States, thus far, two federal agencies have issued guidance, and a handful of state laws apply to biometric information. Consistent with other U.S. regulation of personal information, biometric laws and guidance are fairly narrowly tailored to address specific types of biometric information that present a risk of harm to the individual if compromised.

At the federal level, there is only non-binding guidance addressing the use of any types of biometric information. Rather than explicitly defining biometric information, guidance issued by the Federal Trade Commission (FTC) and the Department of Commerce National Telecommunications and Information Administration (NTIA) is concerned with the use of biometric information to uniquely identify or authenticate an individual. The FTC, which generally asserts oversight of the privacy and data security practices of consumer-facing companies in the United States under Section 5 of the FTC Act, has provided general guidance about the collection and use of biometric information for facial recognition technologies in particular. The guidance is largely based on concepts found under the Fair Information Practice Principals. In general, the FTC’s position
appears to be that notice is required for collection and analysis of biometric information and that express consent is needed prior to identifying a particular individual based on biometric information alone (i.e., matching a facial geometry scan to a database to tie the scan to a known individual). The FTC’s approach here appears calibrated based on the sensitivity of how the information will be collected and used—but not necessarily the inherent nature of the information itself. The NTIA’s best practice recommendations, issued in June 2016, include transparency, data management, use limitations, security, data quality, and problem resolution. While the NTIA encourages companies that use facial recognition for unique identification purposes to describe how and why the entity collects, uses, and shares the information, the recommendations do not appear to call for affirmative notice or consent to any uses—with the sole exception of sharing with unaffiliated third parties—making these practices far more permissive than the existing state laws.

Two U.S. states, [1] Illinois and Texas, have laws specifically imposing conditions on the collection, use, disclosure, and security of “biometric information” [2] with the focus on biometric information that can be used to identify an individual. A number of other states have draft legislation circulating. Illinois’ Biometric Privacy Act (BIPA) imposes EU-style data protection, requiring prior notice, written consent, a “reasonable standard of care” to protect such information, and retention and disclosure restrictions for biometric identifiers (a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) and biometric information defined as any information “based on an individual’s biometric identifier used to identify an individual.” [3] The Texas law imposes similar limitations on the collection, use, and disclosure of biometric identifiers but does not require written consent.

Although BIPA was passed in 2008, the application of facial recognition software to photographs on various social media sites has resulted in a flurry of more recent case activity. Shutterfly, Google, and Snapchat are among the social media companies currently facing class action lawsuits under BIPA relating to their alleged practices of scanning the faces in photographs. The lawsuits have focused on jurisdictional issues in addition to the question of what constitutes a biometric identifier under BIPA. In February, a district court in Chicago rejected Google’s motion to dismiss the suit, which alleges that plaintiff’s photos were scanned to create face templates without consent. Google unsuccessfully argued that face templates created from a photograph were not “biometric identifiers” under BIPA and that, because the actions took place outside of Illinois, BIPA did not apply. The Google ruling is consistent with the progress in the Shutterfly case. Shutterfly also lost a motion to dismiss where it argued, in part, that BIPA did not cover facial geometry scans of photographs.

While the FTC has moved cautiously, these cases suggest possible beginnings of a privacy regime in the United States that could impose specific conditions on the manipulation of biometric information capable of identifying an individual.

European Union Consideration

As opposed to the approach in the United States, European Union (EU) law and guidance seems to indicate that biometric information is personal information and certain types of biometric information—those used to identify an individual—are sensitive personal information. The EU Data Protection Directive 95/46/EC, which addresses the personal information processing, does not explicitly include biometric information in its definition of “personal data.” “Personal data” is broadly defined as “any information relating to an identified or identifiable natural person.” Based on that definition, the Article 29 Working Party (WP29) issued an Opinion that biometric data is considered personal data because it can be used to identify a specific individual. And the WP29’s Opinion on developments in biometric technologies further elaborates that “[b]iometric systems are tightly linked to a person because they can use a certain unique property of an individual for identification and/or authentication….biometric data, by their very nature, are directly linked to an individual.” The Directive will be replaced by the General Data Protection Regulation (GDPR) in May 2018. While the GDPR maintains an almost identical definition
of “personal data,” it explicitly includes genetic data and biometric data processed for the purpose of uniquely identifying a natural person as special categories of personal data, which are subject to additional protections and restrictions under the regulation. [4]

A number of EU Member State data protection authorities have affirmed or otherwise signaled their agreement with the more general position that biometric information is personal information, including Belgium, France, [5] Italy, the Netherlands, and the United Kingdom. To the extent that these data protection authorities have articulated the reasoning underlying their positions, they tend to focus generally on the fact that this biometric information relates to an identified or identifiable person or can be used to actually identify a person. Of course, this raises the question of whether any piece of information about a person’s physical characteristics, such as the recorded sound of a voice, could in its own right be personal information.

**Canadian and Asia-Pacific Considerations**

In general, similar considerations apply outside of Europe. In Canada, for example, biometric information is addressed, in part, by guidance from the Canadian Office of the Privacy Commissioner (OPC), which affirms that it is personal information, referring in particular to recorded characteristics such as face, fingerprints, or a voiceprint. Again, this approach is unclear as to whether any information about a person’s physical characteristics is personal information.

Australia has taken an approach similar to the GDPR. Under the Australia Privacy Act 1988, amended in 2014, biometric information to be used for purposes including verification or identification and biometric templates are explicitly defined as sensitive personal information. As a result, this information is subject to more stringent protections than personal information generally, including the requirement that consent be obtained to its collection. The enhanced restrictions are use-specific and do not assume that any and all biometric information collected is sensitive information. In particular, the concept of a biometric template addresses the fact that some information relating to biometrics, such as the photographs central to the BIPA cases, might be collected, but does not become sensitive—and subject to heightened data protection limitations—until it is used as an identifier through the creation of a “template.”

In Japan, recent amendments to the Japanese Personal Information Protection Act expanded the definition of personal information to include “individual identification codes” (commonly referred to in the media as including biometric data such as facial recognition and fingerprints). After the law passed, an expert panel determined that these identification codes, and therefore personal information, also include information regarding an individual’s genome. This specific classification potentially limits the ability to use and share genomic information, including information about diseases; news articles have noted concerns among researchers that restrictions could impair medical innovations.

Hong Kong’s Office of the Privacy Commissioner for Personal Data issued Guidance on Collection and Use of Biometric Data in 2015 (“Guidance”), which states that biometric information is personal information subject to the Personal Data (Privacy) Ordinance. In addition, certain types of biometric information may be sensitive personal information, for example, where it relates to race, health, mental condition, or criminal investigations. Biometric information includes physiological information (these cannot be changed and the Guidance lists “DNA, fingerprints, palm veins hand geometry, iris, retina and facial images” as examples) and behavioral information (which may change and include “handwriting pattern, typing rhythm, gate and voice pattern”). Biometric information must be protected based on its level of sensitivity, which can be determined by considering the following factors: uniqueness, likelihood of changes with time, multiple use purposes, capability to be covertly collected, and impact to individual if disclosed. The Guidance addresses notice, consent, and other
privacy requirements for collecting biometric information; it also encourages conducting a privacy impact assessment when determining whether biometric information collection is necessary and not excessive.

As these examples suggest, there is a budding tension between privacy regimes governing biometric information that focus on use cases as opposed to imposing requirements for simply collecting this information (for example, to the extent all biometric information is deemed personal information). The more information swept into these categories, the greater the challenge to innovation and, perhaps inadvertently, the greater risk of sweeping up current, commonly accepted practices, such as any recording of a voice or any photograph stored digitally.

Any organization that is considering—or is already engaged in—the collection or use of biometric information or information that could be deemed biometric information, particularly for identification purposes, should:

1. Assess whether information that is being collected could be considered biometric information;
2. Consider which laws might be applicable (some of the laws have a broader reach than assumed at first blush);
3. Determine whether any privacy laws of general applicability or laws specific to biometric information such as the Illinois BIPA may be applicable; and
4. Monitor developments in this area as the laws are likely to proliferate.

[1] In addition to these specific laws on biometric information, a number of state privacy laws explicitly define “personal information” to include specific biometric information, such as fingerprints or retina scans, resulting in privacy and data security applications to such information. North Carolina’s breach notification law defines “personal information” to simply include “biometric data” with no further clarifications.

[2] A 1978 California law focused on the use of lie detector technology addresses voice prints (without defining the term); this law could be interpreted to apply to some uses of voiceprint data—a subcategory of biometric information—in some instances.


[4] See General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), Art. 9(1). The GDPR defines “biometric data” as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.” See id. at Art. 4(14).

[5] The French data protection authority (“CNIL”) recently revised its framework for the registration and authorization of biometric systems that are used to control access to employers’ premises and systems, though it is consistent with this general treatment of biometric information as personal data. French law previously distinguished between information that individuals may reveal without their knowledge (e.g., fingerprints left on an object) and information that may be collected only with their knowledge (e.g., biometric data that are collected by placing a hand in a scanning device). In contrast, the new approach treats all biometric information the same regardless of how collected and imposes different obligations based on whether individuals can control their “biometric template.”