OCBJ.COM

ORANGE COUNTY BUSINESS JOURNAL

Vol. 41, No. 26 — THE COMMUNITY OF BUSINESS™ — June 25-July 1, 2018 • $1.50

CALLAHAN & BLAINE

Identifying What Constitutes Biometric Information

In April 2018, Facebook CEO Mark Zuckerberg sat before Congress to answer questions about Cambridge Analytica. Mr. Zuckerberg's testimony became front-page news. And rightfully so; Cambridge Analytica obtained the personal data of 87 million Facebook users worldwide, 70 million of those users are from the United States.

For millions of Facebook users, the Cambridge Analytica scandal invoked never thought of questions: Who, besides Facebook, has access to my personal information? Why does Facebook have it? What is Facebook going to do with my personal information? And how did Facebook obtain it in the first place?

For a variety of reasons, these are difficult questions to answer. One reason for this difficulty is that the United States lacks a universal definition of personal information. While most people know to safeguard their bank account information and social security numbers, fewer people understand that personal information extends to biometrics—or measurements related to human characteristics, such as fingerprints, voiceprints, iris scans, and retina scans.

So before answering who has my personal information, why do they have it, what are they going to do with it, and how did they even get it, there is a threshold question to answer: what is personal information?

The GDPR's Definition of Personal Information Includes Biometric Information

In the European Union, the answer to that question is universally defined. The General Data Protection Regulation (GDPR) defines "personal data" as "any information relating to an identified or identifiable natural person." [Art. IV(1)]. The GDPR in turn defines "an identifiable natural person" as one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [Art. IV(1)]. The GDPR's definition of personal information is very broad; it includes genetic data and biometric information. While such a broad definition invokes questions of its own, whether any type of biometric information is also considered personal information should not be one of them.

Unlike in the European Union, the United States lacks a universal definition. Each state is therefore left to define personal information independently. In 2008, the Illinois Legislature enacted the Biometric Information Privacy Act (BIPA), which defined biometric information specifically.

BIPA's Definition of Biometric Information

BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." [740 ILCS 14/10]. Notably, "biometric information does not include information derived from items excluded under the definition of biometric identifiers" (i.e. photographs). [740 ILCS 14/10].

BIPA's definitions of "biometric identifiers" and "biometric information" therefore create ambiguity whether biometric information includes information derived from digital photographs (i.e. scan of face geometry) notwithstanding BIPA's express exclusion of photographs from its definition of biometric identifier. [740 ILCS 14/10]. This ambiguity now appears resolved following judicial interpretation.

Shutterfly, Facebook, and Google each were named as defendants in separate putative class actions alleging violations of BIPA. These class actions followed a similar framework: (1) BIPA requires, among other things, that a company provide notice before it collects and stores biometric information; but (2) Shutterfly, Facebook, and Google captured and stored biometric information by conducting face scans of the respective plaintiffs from digital photographs without providing the requisite prior notice. [740 ILCS 14/15].

Predictably, Shutterfly, Facebook, and Google each moved to dismiss the respective class actions brought against them, arguing that BIPA does not protect information derived from photographs. All three were unsuccessful, however. *See Norberg v. Shutterfly*, 1:15-cv-05351 (N.D. Ill. June 23, 2015) (by alleging that Shutterfly used the plaintiff's personal face pattern to identify him in a photograph, the plaintiff stated a claim under BIPA); *In re Facebook Biometric Information Privacy Litigation*, 15-cv-03747-JD (N.D. Cal. May 5, 2016) (reasoning that "photographs" are better understood to mean paper photographs, as opposed to digital ones); *Rivera v. Google, Inc.*, 1:16-cv-02714 (N.D. Ill. Feb. 27, 2017) (reasoning that Google creates a set of biology-based measurements ("biometric") used to identify a person ("identifier") and a face template is a "scan of … face geometry," as defined under BIPA).

California's Proposed Definition of Biometric Information

California is poised to avoid the uncertainty surrounding whether face scans of digital photographs constitutes biometric information. The California Consumer Privacy Act, currently waiting whether it obtained enough signatures to appear on the November ballot, defines "biometric data" as "an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid, which can be used, singly or in combination with each other or with other identifying data to establish individual identity." [The California Consumer Privacy Act of 2018 § 1798.106 (a)]. The definition expressly includes, without limitation, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings. [The California Consumer Privacy Act of 2018 § 1798.106 (a)].

While the California Consumer Privacy Act, if passed, would eliminate the ambiguity of whether face scans of digital photographs constitute biometric information, more problems persist. Its broad scope is all but certain to require judicial interpretation to determine, for instance, under what circumstances behavioral characteristics constitute biometric data.

But perhaps the greater problem is the lack of uniformity in the United States as to what constitutes biometric information. As of now, only three states, Washington, Texas, and Illinois have biometric privacy statutes in effect. And only Illinois allows for a private right of action. The lack of uniformity unfairly exposes companies operating in Illinois to lawsuits challenging their biometric collection practices, when regulations in other states are different or altogether nonexistent. And absent uniformity, consumers are left guessing what constitutes biometric information. Without knowing the answer, companies and consumers alike cannot take the appropriate steps to safeguard that information.

Until there is a uniform answer for the threshold inquiry—what is personal information—consumers are hard-pressed to answer who has their personal information, why they have it, what are they going to do with it, and how did they get it in the first place?

Kamran Salour
Kamran Salour is a Senior Trial Attorney with Callahan & Blaine where he represents and defends clients in business disputes. His experience extends to cyber security, privacy, and data protection matters. He is a certified information privacy professional for the U.S. Sector (CIPP/US) and a frequent commentator on biometric privacy law.