STINSON

News & Insights

Biometrics in the Ballpark - How Teams and Leagues Can Mitigate Data Collection Risk

Article
05.05.2021

By Steve Cosentino and Ethan Sanders

At select ballparks across the country, fans can speed through security screen procedures using thumbprint scans. Sports venues from Madison Square Garden to CenturyLink Field now use biometrics to enhance game day experience. Major League Baseball in particular has led the charge with biometric ticketing through fingerprinting. Biometric security platforms from CLEAR process game entry at 13 of the 30 MLB ballparks. After swiftly entering the stadium, fans can purchase their favorite beverage or hotdog with the same thumbprint scan that is tied to the fan's credit card and biometric data profile.

Understandably, many professional sports teams and leagues prefer the use of biometric data in their ballparks for a variety reasons. It reduces the risk of theft by concessionaires, it confirms that an adult is of legal age to purchase alcoholic beverages, and it shortens wait times at concession stands. One of the most beneficial uses of this data, however, lies in a better fan experience. By tying transactions together using a common purchasing device, teams can better understand their consumers' buying preferences. This data allows teams to provide their guests with the items they want when they want them.

Amid concerns about the commercialization and use of biometric data, Illinois enacted the Biometric Information Privacy Act (BIPA) in 2008, requiring that private entities establish a retention schedule for biometric data, and providing guidelines for the deletion of biometric data. Under BIPA, individuals must consent to businesses obtaining their biometric data, and businesses must disclose their use and retention policies.

The BIPA has been around for a while but has only started to garner more attention recently with the proliferation of litigation taking advantage of BIPA's private right of action. The Six Flags theme park lost a BIPA claim resulting in a ruling that even technical violations of BIPA's requirements may be actionable.

Biometrics in the Ballpark - How Teams and Leagues Can Mitigate Data Collection Risk

Rosenbach v. Six Flags Entertainment Corp. No. 123186 (Ill. Jan. 25, 2019). In February of 2020, Facebook undertook a $550 million settlement concerning allegations that the social media giant violated BIPA through its service that tagged Facebook user photos using facematching software. That settlement was later rejected by Judge James Donato who approved a larger $650 million settlement this month. The year 2020 also saw a proliferation of BIPA lawsuits.

A year later, Texas passed the Capture or Use of Biometric Identifier Act (CUBI), imposing similar requirements for notice, consent, prohibitions on disclosures, and mandatory security measures. CUBI does include some exceptions to the selling and disclosure of biometrics. Certain exceptions track similar provisions in Illinois' BIPA, such as disclosures required by law; however, Texas' CUBI also includes a specific exception for "purposes of identification in cases of disappearance or death." See id. at (c)(1)(A). But even though Texas' CUBI may leave out some of the standout features of Illinois' BIPA—i.e., attorney generalfiled suits in lieu of the private right of action—CUBI does impose civil penalties of up to $25,000 per violation.

Washington passed H.B. 1493 in 2017 establishing data security requirements for biometric data. The Washington law, however, contains a very useful and broad "security exemption," which excludes those persons that collect, capture, enroll or store biometric identifiers in furtherance of a security purpose.

Some states have amended their data breach notification and response laws to address biometric data. Louisiana added biometrics to its data breach law in 2018. New York amended its data-breach notification in 2019 with the Stop Hacks and Improve Electronic Data Security (SHIELD) Act. The SHIELD Act does not contain a private right of action but it does add biometric information to the list of data elements that when combined with personal information trigger a data breach notification obligation. Likewise, Arkansas passed legislation in 2019 called the Personal Information Protection Act (PIPA) changing its definition of personal information in its breach-response laws to include biometric data.

Finally, 2020 brought new biometric privacy laws in Oregon, Arizona and California. Oregon broadened its Consumer Information Protection Act (OCIPA) to include biometrics in the definition of personal information. Arizona made similar additions in its Data Security Breaches Law. California passed the California Consumer Privacy Act (CCPA), which treats biometric information as an express category of Personal Information requiring data security protections and data subject access and deletion rights.

When analyzing the impact of these biometric data privacy laws on sports operations, organizations should consider the definitions of biometric data under the applicable laws. For example, the definition of biometric data under the CCPA is broader than under Illinois' BIPA. The CCPA definition includes imagery of the iris/ retina, fingerprint, hand/palm and face from which an identifier template can be extracted, as well as sleep, health or exercise data that contain identifying information, or with other identifying data, to

establish individual identity. Cal. Civ. Code § 1798.140(b). BIPA defines biometric identifier" to mean "a retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry." 740 ILCS 14/10. However, in a way, BIPA is broader than the CCPA because it has a definition for "biometric identifier" that means "information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." Under BIPA, digital representations of biometric identifiers, such as a randomized number used to represent a facial image, are also covered by the statute even if the image is deleted.

Sports teams face two key challenges in implementing biometrics in their venues. Consent is required under certain laws such as BIPA, and the consequences of violating BIPA can be a costly private lawsuit. Many other laws such as CCPA have data subject access, deletion and opt-out rights that need to be integrated into any biometrics application along with well-constructed mobile friendly privacy policies.

In every case, the paramount concern is information security. With millions of pieces of personal information being exposed in a number of large high profile data breaches in recent years, data elements such as contact information and even social security numbers are widely and inexpensively available on the black market. Biometric information has not reached that level of public availability. Security is certainly a balancing act for sports organizations, and while facial recognition and biometric scanning systems at parks may help reduce petty crimes and even terrorist threats at such public venues, the risk of massive data breaches and identity theft is high. Unlike traditional data breaches, breaches of biometric data are more severe, as there is no way to replace such data. As reported by the BBC, unlike text passwords or credit card information, "biometric information such as fingerprints could never be made private again once lost."

As sports franchises continue to look for advantages to increase revenue and boost fan engagement, sharper teams that focus on data security and privacy in their biometrics programs will benefit from the secure use of robust fan data enabling them to move to the top of the standings for fan experience wins.

CONTACT

Stephen J. Cosentino, CIPP

RELATED CAPABILITIES

Esports, Sports Technology & Wagering

Private Business

Sports & Recreation