GDPR Case Study:
The Spanish Football League's Official App

Wyatt Howe

Abstract

For a year after June 2018, the official Android application of Spain's national football league contained a tracking capability which would activate during live matches and record audio snapshots every minute to determine if and where a portion of its ~10 million users were watching a match. Due to the large number of bars streaming games, the league devised this way to hunt down pirated broadcasts via users aggregate geopositioning data. After an equally long investigation, the Spanish Data Protection Agency (AEPD) concluded that the league's app had violated Articles 5 and 7 of the GDPR, and issued a fine for 250,000 euros for lack of transparent terms of use and inability for users to easily withdraw consent from the sensor data collection done by the app. It is uncertain whether the league has succeeded in their appeal.

1 Facts of the Case

On June 8 of 2018, the professional division (branded as La Liga) of Spain's national football league updated the privacy policy their official Android app and introduced into it a new 'feature'. Up until that point, geopositioning data observed by the device was used solely for guiding users to the nearest stadium. After the update, user's were prompted to allow the mobile device's microphone and geopositioning to help prevent fraud around illegal broadcasts [3, 8]. What the app didn't specify is that what that meant was to collect several seconds[1] of audio every minute during a game, using audio search techniques to generate an acoustic fingerprint [1, 4] which can be compared to the known fingerprints of game live-streams.

1.1 Timeline

Three days later, on June 11, 2018, Spain's data production agency (the AEPD) began an official investigation into the app, yet this news brought no immediate effect, and the league's app continued its monitoring up until the end of June the following year, which is when the league had planned on retiring the app's "experimental feature" from the start [3, 4]. After exactly a year of investigation, on June 11, 2019, the AEPD acted upon the GDPR, citing Article 5.1.a, regarding transparency of processing, and Article 7.3, which grants the right to withdraw consent, as being violated by the league's new privacy policy. the AEPD issued a fine of 250,000 euros [6]. The official resolution from the investigation shows that the AEPD had considered numerous other points of infraction, such as Articles 4 and 6, but due to the data in question being collected in aggregate over sufficiently many users, and a reasonable *legitimate interest* in terms of reducing pirate streams, these were ultimately excluded from the fine.

1.2 Technical Details

The league mentions [4, 8] a third party contracted to develop this software, but the league does not reveal the name of this other. It's not unreasonable to presume that this would be the data processor, although the the AEPD assigns the blame specifically to the data controller in this incident [1]. If we are to believe the claim that the league's method of comparing audio faithfully parallels that of Shazam and Facebook, this would mean the league has built a catalog of broadcast fingerprints out as a hash table where the key is the peak frequency normalized by an anchor point [1, 4]. Although the hashes would be computed server-side by the league, the preimage, the spectrogram sent by the user's device only contains 0.75% of the raw audio, and is insufficient for deriving any personally identifiable data [7]. The league itself issued an official statement on June 11, 2019, the day of the fine, which restates the app's terms of use and commitment to user privacy and emphasizes that the recorded data is transformed irreversibly before ever leaving the device; furthermore, the league attempts to justify their *legitimate interest* by citing the nationwide loss of football streaming revenue due to piracy as on the order of 150 million euros [5].

[1] Estimated about 10, based on Apple's Shazam algorithm [1] which the league cites as similar to their own technology.

2 Analysis

The point above centering around personally identifiable data is the league's main defense. In particular, the league defends not showing a microphone icon while recording as benevolent deception, and assures that the audio fingerprinting technology cannot capture human conversation [2, 4, 7]. This is in reference to the AEPD's contrasting observation that the app does show a globe icon while geopositioning is active, with the implication being the use of geopositioning (*i.e.* for finding a stadium) is expected.

The changes in the app were noticed almost immediately, with news reports appearing in the days after the change, and the controversy was rekindled the following June when the fine was announced. "You think you are following the game, but in reality you are spying." one user of the app says [8].

2.1 Impact and Suggested Solutions

However straightforward the third and fourth paragraph of the privacy policy at the time [8] may have detailed how the use of the microphone and geopositioning will impact users, the AEPD argues that the nature of mobile application is such that having unintuitive terms of use pose an unreasonable burden on users. Instead, the agency suggests the league is responsible for reminding its users *every time* the devices microphone and geopositioning would be utilized [2, 4].

An indicator for microphone and geopositioning in software may be complemented by hardware itself. Many laptop computers have an LED dedicated to announcing camera use, and some Android also share this capability which would take away developers' power to hide sensor-based data collection. One article questions the utility of location data in aggregate, claiming that a bar on the first floor would be indistinguishable to users watching the game in their upper floor apartment [7].

Interestingly, the scope of Spain's national football league's violation was not limited to just Spain. During the app's one-year experimentation period, the 2018 World Cup was held in Russia, and it's estimated that by that time the updated app had been installed 10 million times [3].

3 Discussion

The cause of the investigation is unclear, but it's not surprising the new feature was identified quickly.According to the GDPR Enforcement Tracker [6], out of 62 transparency related violations (usually either Article 5 or 13) labeled "insufficient fulfilment of information obligations", 38 of these were executed in Spain. This speaks to the regulatory power of the AEPD, which is two decades older than the GDPR and has additional data protection agencies established in three autonomous regions. Similar violations may be commonplace in other member states of the union but simply underinvestigated.

Perhaps the strongest argument against this type of hidden tracking is that it defeats the user's own purpose for using the app. The common user would not individually derive any benefit from this particular 'feature' of the app. If the bar *was* pirating their stream, the user may be concretely negatively affected by having to go elsewhere to watch. Yet, the nature of group viewing, is that multiple people are there. Users may have to confirm the access privileges as many as three times [1, 5], yet there will likely be a significant proportion of users who will still allow the league to collect data, especially given this particular app's popularity. Rather than benefit the data subject, it benefits the data controller, and this heavy bias is part of what motivated the drafting of the GDPR. Furthermore, no rational user knowing this, would still have a more difficult time disabling the data collection (via Android system preferences) than enabling it; this is the Article 7 violation. Beyond Article 7, the reality that violating the privacy of data subjects (bar customers) escalates to having a real impact on those around them, is the most startling of all [4].

References

[1] An industrial-strength audio search algorithm. https://www.ee.columbia.edu/~dpwe/papers/Wang03-shazam.pdf. Accessed: 2021-09-23.

[2] Agencia Española de Protección de Datos. Official resolution. https://www.aepd.es/es/documento/ps-00326-2018.pdf. Accessed: 2021-09-23.

[3] elDiario.es. https://www.eldiario.es/tecnologia/liga-futbol-microfono-telefono-aficionados_1_2079836.html. Published: 2018-06-10; Accessed: 2021-09-23.

[4] elDiario.es. https://www.eldiario.es/tecnologia/agencia-proteccion-datos-liga-microfono_1_1510607.html. Published: 2019-06-11; Accessed: 2021-09-23.

[5] La Liga. Official statement. https://www.laliga.com/en-GB/news/nota-informativa-138. Accessed: 2021-09-23.

[6] GDPR Enforcement Tracker. Professional football league. https://etid.link/ETid-47. Accessed: 2021-09-23.

[7] La Vanguardia. https://www.lavanguardia.com/deportes/futbol/20190611/462801653528/laliga-multada-app-espia-250000-euros.html. Accessed: 2021-09-23.

[8] XatakAndroid.com. https://www.xatakandroid.com/seguridad/app-oficial-liga-espi-tu-microfono-ubicacion-para-detectar-bares-que-ponen-futbol-licencia. Accessed: 2021-09-23.