GDPR Case Study: Examining League’s Defense of Collecting Recording and Geopositioning Data in Spain

Akshat Mahajan
Brown University

Abstract

The Spanish professional football league offered a mobile application that would periodically geolocate and capture sound recordings of the user’s environment, for the stated purpose of identifying pirated television broadcasts in the vicinity. The Spanish data protection agency eventually levied a fine of 250,000 euros against League, on the basis that League was insufficiently transparent about its data collection and processing (Article 5 of the GDPR).

1 Introduction

The Campeonato Nacional de Liga de Primera División (referred to as League hereafter) offered an official app for fans of the Spanish professional football league. The app offered notifications, news, and device-specific personalization relevant to football teams and upcoming football games in League. Users were not required to create accounts with League nor did the app ask for any personally identifying information [2]. All appeared innocuous.

However, on June 8th 2018, in its terms and conditions, League’s Android app was updated to include the following surprising clause [2]:

> Protect your team! By clicking here, you accept that League treats your personal data, including those obtained through the microphone of your device mobile and geopositioning, to detect fraud in football consumption in unauthorized public establishments...

Users on Android 6 (or higher) devices were now required to grant access to microphone and location data, once through the device’s operating system, and once within the application. League would then activate a recording function in the application during match broadcasts, even if the application wasn’t open on the device, and sample the device’s latitude and longitude (but, as will become important later, not its altitude [2]). Recording data was fed through a one-way audio hash [2] that stripped 99.25% of the initial incoming data [4], and stored in that hashed form as an audio fingerprint. Location data was automatically converted into input for an area heat map visualization at League’s Business Intelligence office, losing the precision of longitude and latitude associated with any individual device [2].

The purpose of all of this was to identify gatherings where League matches were being illegally broadcast through pirated channels — the phone apps attempted to listen for a specific audio signal beamed by the match broadcast, and the location data was used to infer whether the area was licensed to broadcast the channel or not if the signal was detected. Although the app had some 4.2 million estimated active users and ten million total users at the time, only 50,000 devices within the territory of Spain were ever sampled from in this manner during any match broadcast [2]. It is not known how many unique devices were involved over all of the matches broadcast while this feature was enabled. League did not offer users a way to opt out of this feature through the application itself, and relied on generic system displays (such as a “geolocation active" icon) to indicate when this collection was occurring [2].

Public reaction was largely negative: numerous news publications accused League of spying on users [4] [3], and on June 19th 2019 the Agencia Española de Protección de Datos, the Spanish data protection agency, received a letter from a consumer rights’ nonprofit organization called FACUA [2] outlining concerns that recording data could be used to reveal the personal data of third parties (the AEDP had already opened an investigation on June 11th of that year, for causes unknown). After reviewing League’s contracts with processing partners, discussing a brief of defense filed by League, hearing expert testimony, and conducting tests on the application to determine violations, the AEDP charged League with being insufficiently transparent under Article 5 of the GDPR in June 2019, an year later [2] [4].

2 GDPR Violations

The AEDP investigated the following possible claims against League:

- If users could not revoke consent for the recording/geolocating functionality under Article 7 [4]. League successfully defended itself by claiming that users were free to revoke consent through system settings and by emailing League, although it did not comment on whether the application would continue to work if consent was revoked [2].

- If users were made aware of the purpose and collection of the functionality (under Article 5) [2]. League partially defended itself by arguing that the use of a generic device-provided geoposition icon during recording was sufficient to indicate geolocation was occuring, and that its terms and conditions indicated where and how the geoposition data was used. However, it could not successfully defend the absence of a similar recording button to indicate when the microphone was active, nor could it make the claim that users knew in advance that they were going to be sampled.

- If personal data was pseudonymized or anonymized under the definitions laid out in Article 4 [2]. League successfully defended this charge by pointing out that the only explicitly identifying information they collect — device IP, device model, and phone operating system — is anonymized in their records as a user identifier that cannot be linked back through any records [1] [2]. Because the location data they collected did not include altitude and because of its conversion into a heat map, League claimed it was not able to identify individual devices using the data. Finally, the actual recording data was stored in such a way that retrieving the actual contents of the audio data from it was not possible, allowing League to claim it did not constitute identifiable information.

- If the data was collected for legitimate purposes (under Article 6((f)) [2]. League argued that the absence of a profit motive and the purpose of combating digital piracy explicitly referred to in the terms and conditions made this feature a legitimate lawful interest. [2]

In the end, the AEDP was only able to make part of the charge of violating Article 5 stick. Originally, a fine of 500,000 euros was propounded — this was later dropped to 250,000 euros when League demonstrated a geolocation icon was visibly indicated on the devices used (League's turnover at the time was estimated at close to 2 million euros according to the AEDP) [2]. Given the scale and scope of the activities (affecting approximately 1 percent of its userbase at any given time [2]), the minimal risk of malicious usage post-processing, and the thoroughness of the AEDP's investigation, the final fine appears reasonably arrived at.

The ruling set a precedent for other companies on how background data procesing should function: namely, it held that it was insufficient for applications to collect data once consent is given without notifying the data subject at the time of collection [1]. In this case, League's big mistake was not investing in a microphone symbol or a notification indicating what it was doing when it tried to capture recordings.

3 Discussion

The League case highlights how companies can overemphasize their duties as processors, but eschew similiar focus on controllership. League's technical defenses held up on examination because it had done the necessary post-collection processing to preserve user's privacy, but not so in the court of public opinion: often, users were not aware their data was being anonymized, or that they were being recorded / geolocated at all [4]. This is because League focused all of its efforts on data protection by processing data carefully — but not in its responsibility, as a data controller, to disclose its activities. League may even have had incentives to prevent transparency, as users would be unlikely to consent if they *were* listening to a pirated broadcast.

What could have been done to prevent this GDPR breach? In terms of technology, the League case demonstrates the limitations of the mobile permissions model — permissions granted once could allow any use of data in the future, and so should be reviewed regularly. Firmware designers could switch to a permission expiry model, where permissions granted to an app once expire after a certain amount of configurable time, reminding users to review what their applications do. League should have been required to register a message whenever permissions are set again, explaining the specific use of any permission. Application usage of all peripheral components should be made visible from the firmware side, the way geolocation usage currently is, and it should be easy to identify which application is using the said peripheral device.

Above all, though, League's case emphasizes that features built with inherent conflict of interest with user's transparency should never have been greenlit. More review and accountability is needed internally, and hopefully that is the future we are all hurtling towards post-GDPR.

References

[1] dataguidance.com. Spain: Aepd fines laliga 250,000 for gdpr violations. https://www.dataguidance.com/opinion/spain-aepd-fines-laliga-%E2%82%AC250000-gdpr-violations, August 2019. (Accessed on 09/18/2020).

[2] Agencia Española de Protección de Datos. ps-00326-2018.pdf. https://www.aepd.es/es/documento/ps-00326-2018.pdf, June 2019. (Accessed on 09/18/2020, translated to English by Google Translate).

[3] Intelligencer.com Max Read. Your smartphone is spying (if you're a spanish soccer fan). https://nymag.com/intelligencer/2019/06/laliga-app-spied-on-users-earning-soccer-league-a-fine.html, June 2019. (Accessed on 09/18/2020).

[4] Techcrunch.com Natash Lomas. Laliga fined $280k for soccer app's privacy-violating spy mode. https://techcrunch.com/2019/06/12/laliga-fined-280k-for-soccer-apps-privacy-violating-sp June 2019. (Accessed on 09/18/2020).