Privacy Policy Lessons After Google App Data Verdict

By **Beth Waller** (September 23, 2025)

Beth Waller

After a three-week trial, on Sept. 3, a California federal jury found Google liable for two California law-based claims in invasion of privacy and common-law inclusion upon seclusion.

The class action, Rodriguez v. Google LLC, in the U.S. District Court for the Northern District of California, centered on the plaintiffs' claims that Google collected users' data after they switched off the "Web App and Activity" tracking feature in their Google privacy settings.

Google had countered that the data was nonpersonal, pseudonymous and not associated with any individual user's identity. The plaintiffs sought $31 billion in damages and received $425 million after the jury deliberated for 10 hours. The jury did not find that Google acted with malice and declined to award punitive damages.

Google has vowed an appeal, stating that the "decision misunderstands how our products work."

This privacy class action brings to the forefront the complex interplay between pseudonymization and customer understanding of privacy choices in privacy policies. The jury found that Google invaded the privacy of its users through continuing to collect, use and disclose pseudonymized data.

Ultimately, this decision should cause every business to examine its privacy policy and customer choices around pseudonymized tracking.

The Tracking at Issue

The case centered on Google settings related to activity tracking that allowed users to toggle a privacy feature on or off.

The plaintiffs claimed that after toggling off a web app and activity feature that tracked their Chrome history and activity from sites, apps and devices that use Google services, Google continued to use their activity with its advertisers.

The class action complaint claimed Google had falsely "promised that by turning off this feature, users would stop Google from saving their web and app activity data, including their app-browsing histories."[1] The plaintiffs claimed that Google built comprehensive accounts of users after toggling the web app and activity feature off, and that this information was used for Google application developers and advertising.

Google Analytics for Software Development

This high-tech privacy class action focused on several of Google's software development kits, which are used by third-party app developers, and several tools that aid developers with user engagement and app usage.

The Northern District of California, in denying summary judgment earlier in the case, noted

that Google utilized this web app and activity data, even after the plaintiffs switched the setting to off, to provide analytic services to aid developers. Google argued that when the switch was turned to off, the information was nonpersonally indentifiable.

Google's Privacy Policy

Google had argued that it collected pseudonymous data lawfully and that users knew and understood what was meant by turning the web app and activity feature off. Once a user toggled the feature off, the user's data was "logged with random number identifiers that cannot be joined with any person."[2] This pseudonymized information was shared with advertisers.

Google stated that "whenever these concepts are discussed in the privacy policy, Google's distinction between "your Google Account" and "non-personal information" is clear and unambiguous, and the privacy policy also makes clear that "Privacy Controls ... can toggle whether Google collects personal information, but that it will continue to keep basic records with non-personal information and report that basic record information to advertisers."[3]

What the Jury Found

The court certified a class of 98 million cellphone users who had opted to not have their app activity tracked between the years of July 2016 and September 2024.

The jury heard three California law-based claims: (1) invasion of privacy under the California Constitution, (2) common-law intrusion upon seclusion, and (3) a violation of the Comprehensive Computer Data Access and Fraud Act.

The jury found for the plaintiffs on two of the claims: invasion of privacy and intrusion upon seclusion. Under the invasion of privacy claims, the law centered on two similar elements: a reasonable expectation of privacy and whether the intrusion was highly offensive.

Google had argued that there was no reasonable expectation of privacy in pseudonymized data. The jury disagreed and awarded $425 million in damages. The jury did not find that Google acted with malicious intent, sparing Google from punitive damages. Google has stated it plans to appeal.

The Takeaway: Advertising Technology is Complex and Privacy Policies Should be Explicit

As a privacy law specialist watching this lawsuit from the sidelines, it is clear that the case centered on the interplay between consumer understanding and privacy policy descriptions. In the wake of this lawsuit, businesses using complex advertising technology or tracking should be reviewing their privacy policies and choices to make sure they are clear and unambiguous to a consumer.

What does this mean in practice? Below are three practical steps legal teams should take in wake of this decision.

1. Understand how the data is anonymized, and whether it is truly untraceable.

Legal departments should work to have an in-depth understanding of how their business units and technical teams are applying pseudonymization. There are multiple ways to implement pseudonymization, including replacing identifiable information with random

codes or tokens. This is the way that Google's team pseudonymized information once a user opted out of the web app and activity-f tracking.

There are other ways to also hash data, i.e., taking cryptographic functions, or to manipulate data, such as using data masking, which is replacing information with dummy or random characters.

Some of these methods can be undone, meaning they can be reversed with the right set of tools. Legal departments should have a working understanding of how their teams use and manipulate data, including whether it is later sold to a third party or combined with other data, so that this information can be properly disclosed in privacy policies.

2. Privacy policies should be readable to the average consumer.

Google was left at trial with attempting to argue that its privacy policy was explicit enough for the average consumer to understand its data practices. Google used terms such as "your Google account" and "non-personal information" to try to draw a distinction for the average consumer that it was, indeed, still collecting data that it pseudonymized.

Legal departments should read their consumer-facing privacy policies with an eye toward whether they would want the language blown up on a big screen in front of a jury box.

In order to test privacy policies, it's important to make sure that those beyond the legal department are given an opportunity to read and weigh in on readability, especially when considering complex advertising technology choices.

3. Toggle features are excellent, but can they send the wrong message?

Here, too, Google used a slide button to allow a user to opt out of tracking. This slide feature was not alongside the language in the privacy policy. Thus, it may have been possible for a consumer to misunderstand what truly was happening when the toggle was switched on and off.

One way to fight back against misunderstanding is to embed a link to the privacy policy alongside a toggle button with a note that says "to learn more about what occurs when you slide this button off, click here." Adding context can work to prevent misunderstandings.

Ultimately, it appears that Google lost this trial in part because a group of average consumers — in this case, the jury — believed that Google did not properly disclose how it was using data it collected. Businesses should pay close attention to this verdict and put in place countermeasures to ensure that consumers truly understand their privacy choices.

Beth Burgin Waller is a principal and chair of the cybersecurity and data privacy practice at Woods Rogers.

[1] Fourth Amend. Compl. P1.

[2] SJ brief at page 20.

[3] Id.