

Google Privacy Policy Litigation Illustrates Evolving Disclosure Standards

August 05, 2021

Even the giants of the information age are working to keep up with tightening standards for privacy policy disclosure. Tech giant Google is currently defending against a class action and under regulatory scrutiny for an alleged failure to properly disclose how it utilizes data from users browsing in “incognito” mode. In addition, Google is under fire for allegedly storing audio recordings for undisclosed purposes. These Google cases provide cautionary tales for every company of the risks of failing to properly disclose information to users and failing to update privacy policies when collection and use of data changes.

Before drafting a privacy policy or terms of use for a website or mobile application, companies of all sizes must assess and disclose in careful detail the following types of information:

- the types of data that is being collected and from whom data is collected;
- the purposes for the collection of data;
- the ways in which collected data is being used; and
- whether data is being shared with or sold to any third parties.

In addition, some state laws and regulations require explicit disclosures about the sale of data and require companies to afford consumers the ability to opt out of the sale of personal information. New York is likely to pass such a law within the next year.

Companies should undertake to regularly reassess their privacy policies. A policy adopted even one or two years ago may be fatally flawed if data collection and use practices or legal disclosure standards have changed. And, as the Google cases demonstrate, special care must be taken whenever a company makes a potentially inconsistent statement about the use of consumer data or the privacy of a service provided by the company separately from the company’s official privacy policy.

Cases Allege Undisclosed Data Collection and Use by Google Incognito Mode and Google Assistant.

A 2020 class-action lawsuit alleged that Google illegally collects information during private browsing sessions using its “incognito” mode, through which users believe they are keeping their search activity private. Despite displaying a message stating that “incognito” users can browse “privately” without their search history becoming visible to other users of the device, according to the complaint, Google tracks and collects consumer browsing history and other web activity while using incognito mode, thus unlawfully intercepting and collecting confidential communications without user consent.

While Google contends that the plaintiffs consented to have their data collected when they agreed to the terms of service, according to the complaint many users feel that they were given a false or misleading impression by Google about what was being done with their data.

The Google Privacy Policy states that it does not sell personal information. However, the complaint alleges that this statement is categorically false, citing a 2019 New York Times op-ed discussing how Google monitors and commoditizes its consumers' digital footprint by selling their personal information. Armed with the knowledge of how Google interacts with third-party advertisers, this wholesale qualification that Google does not sell any personal data struck many as a jarring misrepresentation.

On March 12, 2021, a California judge ruled that the action will proceed and denied Google's motion to dismiss, holding that plaintiffs could have reasonably believed, based on Google's representations, that Google would not have access to their browsing activity while they were in incognito mode. Google "did not notify users that [it] engages in the alleged data collection while the user is in private browsing mode." *Brown v. Google LLC*, 2021 WL 949372, at *10 (N.D. Cal. Mar. 12, 2021). This case underscores the importance of fair and accurate disclosures of data collection, retention, sharing and selling procedures in privacy policies for all companies, and highlights the value of including prominent links to a privacy policy whenever a customer is about to engage in activity the company has described as shielded from disclosure.

In another recently filed California action, a federal judge ordered Google to face class-action claims regarding privacy concerns with Google Assistant.

Google Assistant is voice-activated software that carries out users' commands by constantly listening and responding to users' voices when it picks up on hot words, such as "Okay Google." Typically, Google Assistant does not respond unless it hears one of the hot words. However, plaintiffs allege that Google Assistant does not overwrite locally stored random-access memory of audio recordings when Google Assistant makes a mistake and perceives an unrelated phrase as a hot word. The complaint states that Google Assistant allegedly uses stored audio recordings for purposes other than carrying out users' commands, including targeted personal advertising to users and improving the Google Assistant's voice recognition capabilities. This may mean that even when users do not believe that their Google Assistant has been activated and is recording and collecting users' data, Google Assistant is collecting user data and using it for unapproved purposes. *In re Google Assistant Privacy Litigation*, No. 5:19-cv-04286-BLF (N.D. Cal. Jul. 1, 2021).

Other Tech Giants Are Thinking Proactively About Privacy

These decisions come on the heels of Apple's announcement that its upcoming iOS 15 update will give iPhone users more insight into and control over their own data. Among other things, users will be able to see the entities or users with whom the mobile apps are sharing their personal data, will be able to stop trackers from detecting if and when an email is opened, and will allow users to keep internet activity and some phone app usage private. Consumers are choosing not to share data at a high rate, and this change in data sharing frequency will shake up the internet advertising economy. Apple's decision further highlights the increasing commoditization of data and represents one of the clearest examples of a major player in big tech attempting to proactively capitalize on the privacy concerns many consumers have. Apple will have to make sure it honors its privacy promises to consumers.

Now Is the Time To Reassess Privacy Policies and Disclosures

As data privacy lawsuits become more commonplace, businesses are reminded that they should take stock of their own data collection, use and disclosure policies. The obvious starting point in assessing privacy-related requirements are the state data privacy laws that have been enacted in the last few years, the most prominent of which is the California Consumer Privacy Act (the "CCPA," as amended by the California Privacy Rights Act, or the "CPRA"), which applies to California residents. At least eight other states have since passed similar privacy regulations mirroring certain provisions of the CPRA, indicating that the regulation of privacy rights and oversight of data collection and use are concepts that are here to stay. In order to assess organizational privacy readiness, the following are some initial steps and considerations:

- *Take stock of what data you collect.* Sensitive personal information like social security numbers, credit card or payment information, and biometric data have received increased scrutiny from regulators and may require more stringent protocols with

respect to data retention. Data collection processes can change in important ways every time a service is updated or a new version rolled out.

- *If you sell data, disclose it in your privacy policy.* Trying to conceal or disguise the fact that you sell data to third parties, including advertising partners, will cause issues down the road, particularly as newly promulgated regulations tend to have heightened focus around the sale of data and use of third-party advertisers. If the sale of data is part of your long-term business model, consider what changes will need to be made, even before you start selling data. Even if you don't sell information, sharing it with third parties is something that should be disclosed. The CPRA will expand the CCPA's opt-out right afforded to consumers whose information is being sold or shared.
- *Once you have a privacy policy, remember to update it.* If your company has multiple departments, keep the conversation fluid regarding what data is being collected, stored, shared or sold. Your privacy policy should be considered a living document subject to appropriate updates. By keeping your privacy policy up to date regarding your collection practices, you may be able to avoid potential lawsuits in the future.
- *Analyze your relationship with third-party advertisers.* Do you engage with third-party advertisers? Other states are beginning to follow California's lead by restricting the sharing of personal information for cross-context behavioral advertising (defined as the targeting of advertising to consumers based on the personal information obtained from their activity across businesses, distinctly branded websites, applications or services, other than which the consumer intentionally interacts). For example, Virginia recently passed the Consumer Data Protection Act, which allows consumers to opt out of targeted advertising and reflects legislation that appears to be modeled after California's CCPA, at least in part. The CPRA, voted into law in November, further restricts businesses from sharing personal information for cross-context behavioral advertising. Under the CPRA, the transfer of personal information to a vendor for cross-context behavioral advertising purposes is no longer considered a "business purpose" (for which user consent was not required) as it was under the CCPA.
- *Obtain meaningful consent.* Since changes in the law leave businesses with limited options to avoid being considered "sharers" of personal information under the CPRA, many will need to assess methods for obtaining consent from users in order to share personal information with other entities. Consent must be obtained affirmatively before the information is collected. Consumers must be able to easily locate privacy policies, and in some cases, be able to revoke or limit their consent.

Conclusion

If you have any questions about your company's privacy policies or terms of use, speak to a privacy law attorney who can help you ensure that you are making the proper and accurate disclosures reflecting your company's data collection practices. Doing so can save your organization a significant amount of time and money in the long term.

* * *

Carter Ledyard & Milburn LLP uses Client Advisories to inform clients and other interested parties of noteworthy issues, decisions and legislation which may affect them or their businesses. A Client Advisory does not constitute legal advice or an opinion. This document was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. © 2021 Carter Ledyard & Milburn LLP.

related professionals

John M. Griem, Jr. / Partner

D 212-238-8659

griem@clm.com

Matthew D. Dunn / Partner

D 212-238-8706

mdunn@clm.com

Jennifer "Jenny" Frank / Associate

D 212-238-8650

frank@clm.com