

Expert Supplemental
Report of
Jennifer King, Ph.D.

Public Version

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF MARICOPA

STATE OF ARIZONA, *ex rel.* MARK) No. CV2020-006219
BRNOVICH, Attorney General,)
Plaintiff,)
v.) Assigned to the Hon. Timothy Thomason
GOOGLE LLC, A Delaware Limited Liability) (COMPLEX CALENDAR)
Company,)
Defendant.)
_____)

Supplemental Report of Jennifer King, Ph.D.

July 16, 2022

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY
PURSUANT TO PROTECTIVE ORDER

I. INTRODUCTION

I previously submitted my opening expert report in this matter on May 4 (“Opening Expert Report”) and my rebuttal expert report June 22, 2022 (“Rebuttal Expert Report”). I have become aware of new information relevant to the opinions I expressed in my prior reports, and I provide this report to supplement my opinions.

II. The European Consumer Organization’s Report on Google’s Account Setup

I have recently learned of report dated June 30, 2022, from the European Consumer Organization (“BEUC”) (the “BEUC Report”), and a related report from the Trans Atlantic Consumer Dialogue (“TACD”) about Google’s deceptive practices during the account sign-up process.¹ At a high level, this report explains that Google uses hidden default settings and confusing language so that it is “much more cumbersome to say ‘No’” to Google’s data collection.² Google’s account set-up process “deliberately steer[s] consumers to allow an extensive and invasive processing of their data” by setting its defaults—including Web & App Activity and Ads Personalization—to the most invasive configuration.³

According to a press release from the same day, various consumer agencies in Europe also filed complaints against Google concerning the issues raised in the BEUC Report.⁴ The BEUC press release also includes a link to a model complaint.⁵ In Annex 3 to this model complaint, the BEUC references documents produced by Google in another litigation, *Calhoun et al. v. Google LLC*.⁶ According to the model complaint, these documents were attached to the Cruz Declaration in the *Calhoun* litigation. I had not previously seen those documents from the Cruz Declaration, but I have recently reviewed them. These new materials provide further support for my findings, as set forth below.

¹ BEUC, *Fast track to surveillance: How Google makes privacy the hard choice* (June 2022), https://www.beuc.eu/publications/beuc-x-2022-073_fast_track_to_surveillance_how_google_makes_privacy_the_hard_choice.pdf; TACD, *Google puts its users on a ‘fast track to surveillance’: EU and U.S. groups urge authorities to take action* (June 30, 2022), <https://tacd.org/google-puts-its-users-on-a-fast-track-to-surveillance-eu-and-u-s-groups-urge-authorities-to-take-action/>

² Ibid.

³ Ibid.

⁴ BEUC, *European consumer groups take action against Google for pushing users towards its surveillance system*, (June 30, 2022), <https://www.beuc.eu/publications/european-consumer-groups-take-action-against-google-pushing-users-towards-its/html>.

⁵ Ibid.

⁶ BEUC, *COMPLAINT TO THE [DATA PROTECTION AUTHORITY] UNDER ARTICLE 77(1) OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION*, (June 2022), https://www.beuc.eu/publications/beuc-x-2022-072_model_complaint_google.pdf, at 76.

1. Google gives consumers the illusion of choice through settings and disclosures that are difficult to navigate and do not match their expectations.

Exhibits 6, 7, and 10 to the Cruz Declaration all seem to contain internal company discussions that pinpoint that Google users found the company’s account permissions, data collection and use, and user controls overly broad and confusing. I only have the versions that I can see that were attached to the Cruz Declaration, so I reserve the right to supplement my opinion if a more complete version becomes available. However, from what I can see, these internal documents call out Google’s data collection practices (and specifically highlight Web & App Activity) as being overly broad and enabling mass data collection to support Google interests at the expense of their individual users.

For example, Exhibit 6 (GOOG-CABR-04754292) explains as follows:

When we ask people to turn on a setting like Web & App Activity or Ads Personalization, we highlight *enhanced functionality* and *personalization*. The reality, though, is we’re relying on that data for many purposes, including improving our products and fueling our ads-based revenue – neither of which benefit individual users directly, yet both of which fall under this **broad and contradictory consent**.⁷

In my Opening Report, I explained how Google uses WAA to collect and store far more data than it needs to provide users with its services. In my Rebuttal Report, I also responded to Dr. Ghose’s opinion that location-based services provide users numerous benefits. As I have explained, Google benefits significantly from financial exploitation of user location data, yet in many ways users do not. Exhibit 6 further supports this finding. It states that “[w]hile we [Google] believe personalized ads provide value to our users, our ads *measurement* practices (necessary to deliver value to our partners, and therefore core to our business) do not.”⁸ Thus, contrary to Dr. Ghose’s generalized assertions about users’ expectations from location-based services, Google itself recognizes that “[t]he fact remains that we do a bunch of stuff that doesn’t benefit any given user.”⁹ This is also a form of *contextually inappropriate* data usage, because users are forced (or defaulted) into a settings configuration that allows Google to store and exploit their location data to power services that are unconnected to the users’ individual search queries.

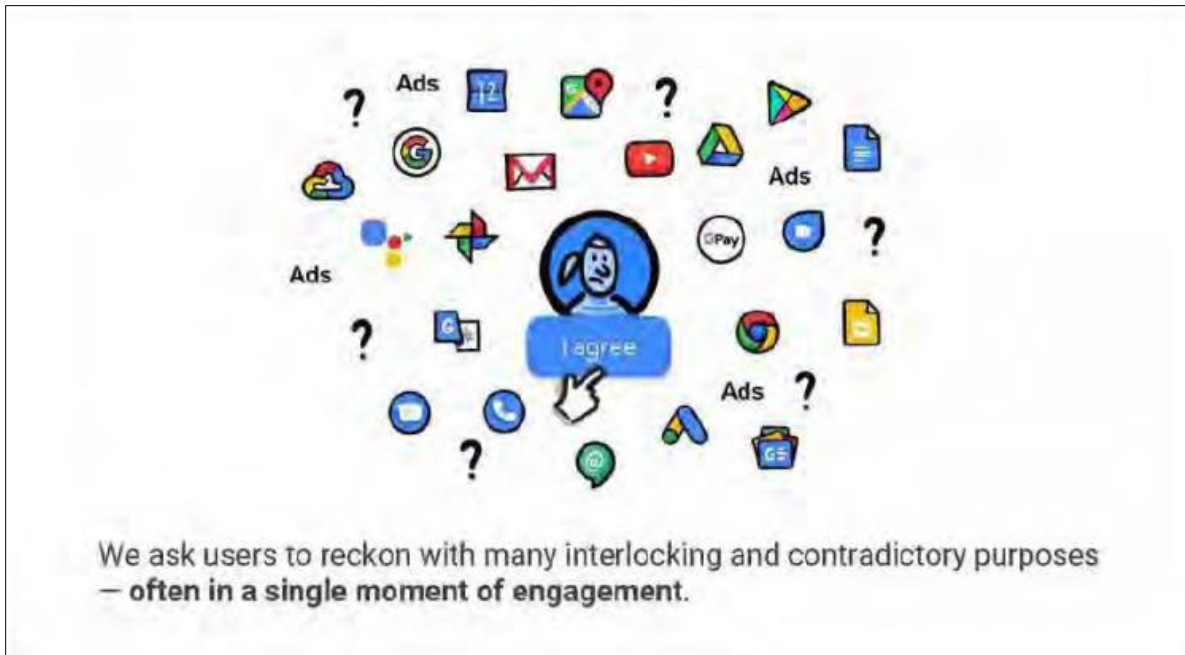
Exhibit 10 to the Cruz Declaration (GOOG-CABR-04754257) similarly criticizes Google’s reliance on “a single moment of engagement,” such as consent to WAA, to “reckon” with Google’s data collection and exploitation, and includes a graphic that helps illustrate this concept¹⁰:

⁷ GOOG-CABR-04754292 at 293 (emphasis in original).

⁸ Id. at 301.

⁹ Id. at 304.

¹⁰ GOOG-CABR-04754257 at 70.



The document explains that “[t]he lack of clarity around what specific role people’s data plays in their experience of our services — means many struggle to understand, the value their collected data enables how their data will be used (and by extension, whether it could make them vulnerable to privacy issues) [and] the service implications of denying Google access to their data.”¹¹ The document further notes that “[i]t’s unclear to people what information about them is shared with our advertising partners & websites (3P) and what role our users play in our revenue model.”¹²

Exhibit 10 also supports my findings in my prior reports that Google’s data collection practices violate *contextual integrity* and create *information asymmetry* between users and Google. I have previously explained how the cumulative effects of data collection, targeted advertising, and interest predictions, as well as the imbalance between individuals and data collection companies, “upends our autonomy and creates a situation of unfairness.”¹³ In line with this analysis, this internal Google document explains that “[i]f consent is given despite an inaccurate or incomplete understanding of [Google’s data collection and exploitation], people can experience negative surprises (encountering unexpected personalization) eroding their trust in Google” and that “the extent to which people feel seen (and often followed) by advertisers triggers concerns about being profiled, surveilled, and even manipulated.”¹⁴

GOOG-CABR-04754160 (Exhibit 7 to the Cruz Decl.) expands on the issues of *information asymmetry*, *contextual integrity*, and disparity in user value. The document states

¹¹ GOOG-CABR-04754257 at 89.

¹² Ibid.

¹³ Opening Report p. 42.

¹⁴ GOOG-CABR-04754257 at 89.

that Google’s “[b]road permissions” system makes it “difficult for people to fully / meaningfully give permission” to Google’s data collection, and explains the problem as follows¹⁵:

- We have a few permissions covering a broad scope of activity, info & data collection and use
 - The lack of clarity around what specific role people’s data plays in their experience of our services — and the fact that everyone uses a different constellation of services — means many struggle to grasp.
 - the value their collected data enables
 - how their data will be used (and by extension, whether it could make them vulnerable to privacy issues)
 - the service implications of denying Google access to their data
 - what will happen with data after it’s collected; it’s very difficult for users (and us) to assess long-term risk
 - This can result in people feeling unequipped to make informed decisions, or even questioning whether they have a genuine choice if they want to enjoy Google services.
 - When consent is given despite an inaccurate or incomplete understanding of the above, people experience negative surprises / trigger moments (encountering unexpected personalization) eroding their trust in Google.
- ...so people struggle to know what exactly they’re sharing, and to see what’s “in it” for them.

“[T]he fact that everyone uses a different constellation of services” is another way of saying that users engage Google services in a variety of *contexts*.¹⁶ As explained above, however, Google’s permissions system is broad and all-encompassing, meaning that it doesn’t respect the specific contexts in which users agree to share their personal data with Google. The result according to this document (and as I have explained in my prior reports) is a significant disparity between what Google knows about users and what users know about Google, creating user anxiety and undermining autonomy. For example, Exhibit 7 notes that “[i]t’s unclear to people what information about them is shared with our advertising partners & websites (3P), and what role our users play in our revenue model,” and explains that this “triggers concerns about being profiled, surveilled, and even manipulated.”¹⁷

Exhibit 7 to the Cruz Declaration also undermines Dr. Ghose’s opinions concerning user value. In a section titled “Lack of benefits,” the document explains that “[w]hen permission is given, most people don’t experience enough (or *any*) of the value that their own data purportedly adds to the products they use,” but “[m]eanwhile, we [Google] espouse (and internally ascribe to) the idea that our users *primarily* benefit from giving access to their data – and Google’s revenue is a happy side-effect.”¹⁸ So while it may be true, as Dr. Ghose argues, that users value

¹⁵ GOOG-CABR-04754160 at 61

¹⁶ *Ibid.*

¹⁷ *Id.* at 63.

¹⁸ *Id.* at 62 (emphasis in original).

the ability to get directions from Google Maps, Google itself agrees that when the company uses location data out of context to turn a profit, it “trigger[s] mistrust, reinforcing misconceptions and feelings of exploitation.”¹⁹ In fact, Exhibit 7 addresses precisely this scenario:

- When people see their data at work in the products they use (*I allowed my location to be collected so now Maps can give me driving directions*) a key purpose of collecting their data is seen as obvious, justified; user data in, functionality/value out.
- People who don't directly experience their data at work in the products they use (*I allowed my location to be collected so now Gmail can... and YouTube can... um*) are likely to suspect the sole purpose of collecting their data to be ads p13n — user data in, money for Google out — for lack of any other demonstrable purpose.

In terms of the analysis I have provided in my prior reports, users “see[ing] their data at work in the products they use” is a form of *contextually appropriate* data use.²⁰ For example, if a user wants to find “pizza near me,” it might make sense that a Google search for “pizza near me” could make use of user location data to provide the service. It would be *contextually inappropriate*, however, to store the user’s location data (whether or not the data come from the search query or from some other setting) to use the location data from that search for other purposes, such as to power ads personalization later on, in different and unrelated contexts.

In my Opening Report, I used the analogy of sharing personal health information with my doctor. I would expect my doctor to have that information when I go to my annual check-up, but I would not expect the restaurant next-door to have that information. Exhibit 7 specifically notes that users get confused about why they are being asked to grant access to their location data. It seems that Google is aware of this concept, but unfortunately has not effectively implemented it.

One of Google’s key privacy themes has been that it does not “sell” its users’ personal data. Another document attached to the Cruz Declaration shows how simplistic and inaccurate this statement is. GOOG-CABR-0011180 (Exhibit 17), titled “Chrome + Privacy Marketing strategy,” includes a “Product assessment” for Google’s Chrome browser, analyzing how the browser “lives up to Google’s privacy principles.”²¹ For the first principle—“Only collect info we absolutely need”—the document states “Status today: Red. We do not yet minimize the amount of info Google collects for personalized advertising, or with other Google services.”²² For the second principle—“Never sell your data to anyone else”—the document states “Status today: Red. While Chrome . . . doesn’t actively share your info with 3Ps directly, we allow 3Ps to collect your data very actively through Chrome through cookies, and extensions, and we make lots of money from ads – that sounds like selling data to many people. It is hard to reconcile this with a commitment not to share user-data.”²³ As I have explained, this stark disparity between the financial benefit of user location data to Google versus to consumers is highly unfair. Aside from the “free” services that users get to use, users have no opportunity to benefit from the

¹⁹ Id. at 63.

²⁰ Ibid.

²¹ GOOG-CABR-00111820 at 22.

²² Ibid.

²³ Ibid.

immense fortune that Google has accumulated by monetizing their location data despite its claims that it does not sell that data.

2. Harms of location data collection are not reasonably avoided by consumers.

The Calhoun exhibits also note that Google’s permission system and data collection (including as enabled by WAA) does not allow Google users true control over their data; in fact, the internal PDPO²⁴ organization that apparently produced several of these documents argues that the company fails to practice privacy by design and calls for a “180 degree change in approach” to how the company manages the user data relationship, moving to a more context specific, real time permissions system rather than a ‘set it and forget it’ or default opt-ins.²⁵

GOOG-CABR-03683283 (Exhibit 13 to the Cruz Decl.) further develops the issue of user harm. The document appears to be a slideshow presented on October 13, 2020, titled “A new approach to building trust.”²⁶ The slideshow references research that Google conducted concerning user sentiment, and states that this “research has indicated that our [Google’s] users have growing concerns about the amount of data that is out there about them, and what little control they have over it... what’s being done with that data, who has access to it, and how it is being used.”²⁷ The slideshow also states that “users are increasingly concerned that they are becoming ‘the product’” and “do not want to feel like the product or that they are the currency being used to facilitate business transactions.”²⁸ In what appear to be speaker notes for one slide discussing a “summary” of Google’s privacy challenges, the slideshow concludes that “a lack of tangible benefits from the data we collect, fuels the feeling that people are the product and that we are using their data mostly for our own gains. We see that the root cause for all of this is in our monolithic consent and data model.”²⁹ As I have explained, this feeling of powerlessness, objectification, and loss of autonomy on the part of users is one of the aggregate, long-term, and indirect harms caused by Google’s conduct.

Exhibit 13 also advocates a concept that I have applied in my previous reports. Specifically, it endorses data minimization, noting that Google “can address this by asking only for the data needed, when needed (not more).”³⁰ At present, however, every interaction between a user and Google is an opportunity for it to store, collect, and exploit user location data.³¹

3. Privacy is a multifaceted, contextual concept.

Echoing the evidence I present in my own reports, Exhibit 6 describes privacy as multifaceted, incorporating: “human nature (privacy is personal and subjective), varying contexts

²⁴ I am advised by counsel that “PDPO” refers to Google’s Privacy and Data Protection Office.

²⁵ GOOG-CABR-04754292 at 302, 303

²⁶ GOOG-CABR-03683283 at 284.

²⁷ Id. at 315.

²⁸ Id. at 316.

²⁹ Id. at 319.

³⁰ Id. at 340.

³¹ Nielson 11/16/2021 Decl. ¶¶ 119-121.

(cultural, personal, situational, etc.), and the overall complexity and intangibility of technology.”³² The authors acknowledge that Google is far more than an internet company: people “entrust us with their precious family photos, passwords, information about the places they go and the things they buy.”³³ Further, Exhibit 10 cites the work of technology philosopher Helen Nissenbaum, as I do in my reports, summarizing a key message from *Privacy In Context* as: “This book claims that what people really care about when they complain and protest that privacy has been violated is not the act of sharing information itself — most people understand that this is crucial to social life — but the inappropriate, improper sharing of information.”³⁴ It appears that Google’s PDPO is familiar with this understanding of privacy and has argued to embrace these precepts into the company’s strategic rethinking of their approach to privacy, but I have seen nothing to suggest that those recommendations have been implemented. This stands in stark contrast to the arguments presented in Dr. Ghose’s rebuttal report, which suggested that the majority of consumers were “privacy unconcerned” or “privacy pragmatists” and were comfortable with the trade-offs of their data for the use of Google services, a premise that Google’s own documents clearly call into question.

III. GOOGLE’S RECENT ACTIONS AND RECENT FTC GUIDANCE CONFIRM THAT GOOGLE IS TRACKING AND STORING HIGHLY SENSITIVE LOCATION DATA

Following the Supreme Court’s decision in *Dobbs v. Jackson Women’s Health Organization*, numerous federal lawmakers reached out to regulators to address the relationship between location data collection and personal health decisions. For example, a group of lawmakers including Sens. Ron Wyden, Elizabeth Warren, Cory Booker, and Rep. Sara Jacobs penned a letter to FTC Chair Lina Khan explaining that “[p]rosecutors in states where abortion becomes illegal will soon be able to obtain warrants for location information about anyone who has visited an abortion provider.”³⁵ Some Google employees expressed similar concerns. For example, Googler Parul Koun explained that “users are concerned about, in light of this ruling, is that Google will pass information on their searches, communications, and location history to law enforcement and that this data will be used to criminalize those seeking abortions,” and noted that “Google has completely failed to address this concern.”³⁶

In the wake of this pressure, Google released a blog post (by Ms. Jen Fitzpatrick) explaining that Google will update its Location History product such that “if [its] systems identify that someone has visited [abortion clinics, fertility centers, addiction treatment facilities, weight loss clinics, cosmetic surgery clinics, and others], [it] will delete these entries from

³² GOOG-CABR-04754292 at 301

³³ Id at 2.

³⁴ GOOG-CABR-04754257.

³⁵ Brian Fung, *Apple and Google should face FTC probe over ad practices that could end up harming abortion-seekers, US lawmakers say*, CNN BUSINESS (June 24, 2022), <https://www.cnn.com/2022/06/24/tech/apple-google-ftc-probe-abortion-ads/index.html>

³⁶ Gerrit De Vync et al., *Abortion is illegal for millions. Will Big Tech help prosecute it?*, WASH. POST (June 29, 2022), <https://www.washingtonpost.com/technology/2022/06/29/google-facebook-abortion-data/>

Location History soon after they visit.”³⁷ As Ms. Fitzpatrick explains, this information “can be particularly personal.”³⁸ To the extent that there was any doubt, Ms. Fitzpatrick’s blog post confirms that Google has been tracking and storing this information.

In my Opening Expert Report, I explained how location data can reveal highly sensitive details about a user’s personal life, including in the form of medical and health information. I also pointed to examples of how information asymmetries and contextual integrity can implicate highly sensitive personal or healthcare issues, such as pregnancy, including how Target was able to infer and reveal that certain consumers were pregnant before those consumers had announced that news to their families. One of Dr. Ghose’s responses to this privacy harm was to argue that my analysis was “not tied to Google or Google’s alleged conduct at issue in this case.”³⁹ On the contrary, location information is often tied and can be used as a proxy for highly sensitive issues such as healthcare and pregnancy. Google’s public statements even acknowledge now that Google has been collecting location data that can be translated into healthcare or pregnancy information. Google now outwardly agrees with its internal statement that “one of the most sensitive and vast personal signals that we collect from users is User Location.”⁴⁰ This also shows that Google recognizes location data can be tied to specific users and used to infer highly sensitive personal information, including medical and healthcare decisions. Ultimately, it is indisputable that the location data that Google has collected through deceptive and unfair practices can be used to reveal sensitive details about users’ personal details.

The Federal Trade Commission recently released a Business Guidance Blog titled *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, in which the Commission provides further support for findings I made in my prior reports.⁴¹ For example, the post notes that while the “conversation about technology tends to focus on benefits,” “location data can reveal a lot about people, including where we work, sleep, socialize, worship, and seek medical treatment.”⁴² According to the FTC, this “exposes consumers to significant harm,” such as profiling based on sensitive health and medical information.⁴³

As to Google’s proposition that aggregation or anonymization of user location data are sufficient to protect this sensitive data, the FTC responds:

³⁷ Jen Fitzpatrick, *Protecting people’s privacy on health topics*, THE KEYWORD (July 1, 2022), <https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/>.

³⁸ *Ibid.*

³⁹ Ghose Report ¶ 52(b).

⁴⁰ GOOG-GLAZ-00317865 at 68.

⁴¹ Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, FTC (July 11, 2022), <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use>.

⁴² *Ibid.*

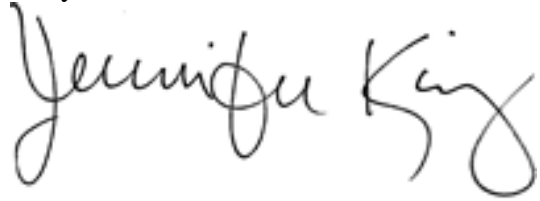
⁴³ *Ibid.*

Claims that data is “anonymous” or “has been anonymized” are often deceptive. Companies may try to placate consumers’ privacy concerns by claiming they anonymize or aggregate data. Firms making claims about anonymization should be on guard that these claims can be a deceptive trade practice and violate the FTC Act when untrue. Significant research has shown that “anonymized” data can often be re-identified, especially in the context of location data. One set of researchers demonstrated that, in some instances, it was possible to uniquely identify 95% of a dataset of 1.5 million individuals using four location points with timestamps. Companies that make false claims about anonymization can expect to hear from the FTC.⁴⁴

I cited similar research about “anonymized” or “de-identified” data in my Opening Report. The bottom line, as I have explained, is that user location data is a highly sensitive and personal form of information that is over-collected and over-exploited by Google.

July 16, 2022

Berkeley, CA

A handwritten signature in black ink that reads "Jennifer King". The signature is written in a cursive, flowing style.

Jennifer King, Ph.D.

⁴⁴ Ibid.