

Expert Supplemental
Report of
Colin M. Gray, Ph.D.

Public Version

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

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

Supplemental Report of Colin M. Gray, Ph.D.

July 11, 2022

I, Colin M. Gray, previously submitted two reports in this action—my “Opening Report” on May 4, 2022, and my “Rebuttal Report” on June 22, 2022. I provide this Supplemental Report to address new information that has come to light since I provided my Rebuttal Report.

After I provided my Rebuttal Report, the European Consumer Organization (“BEUC”)¹ published a report entitled “Fast track to surveillance – How Google makes privacy the hard choice” relating to dark patterns in Google’s Account Setup process.² The BEUC report also links to a “model complaint” for various consumer groups and agencies to bring legal action against Google. The model complaint includes additional information, including an Annex that excerpts various documents from another United States litigation against Google, which are discussed below.

The BEUC also issued a press release on June 30, 2022 concerning its report, where it announced that various consumer groups and agencies have filed complaints against Google in Europe.³ These groups are listed in footnote 1 of the press release. One of these is “Forbrukerrådet (Norway),” which I discuss in my Opening Report at p. 7. I explained that this is the Norwegian Consumer Council, which I understand is a Norwegian government agency. The BEUC also sent letters to various regulators in Europe on the same day discussing its report and urging action by data protection agencies.⁴

Footnote 1 to the BEUC press release also says that “US consumer groups from the Transatlantic Consumer Dialogue (TACD) network are also sending a letter today to the Federal Trade Commission (FTC) denouncing Google’s practices.” From this footnote, I was able to locate a parallel June 30, 2022 announcement and report from the TACD,⁵ as well as the June 30,

¹ The BEUC describes itself as “the umbrella group for 46 independent consumer organisations from 32 countries. Our main role is to represent them to the EU institutions and defend the interests of European consumers.” Founded in 1962, its members are now “from all 27 EU Member States as well as Iceland, North Macedonia, Norway, Switzerland and the United Kingdom. BEUC is acknowledged as a trustworthy representative by decision-makers, thanks in particular to the collective skills, knowledge and expertise of our member organisations.” <https://www.beuc.eu/about-beuc/who-we-are>. (last visited July 8, 2022).

² https://www.beuc.eu/publications/beuc-x-2022-073_fast_track_to_surveillance_how_google_makes_privacy_the_hard_choice.pdf

³ <https://www.beuc.eu/publications/european-consumer-groups-take-action-against-google-pushing-users-towards-its/html>; <https://techcrunch.com/2022/06/29/google-account-gdpr-complaint/>

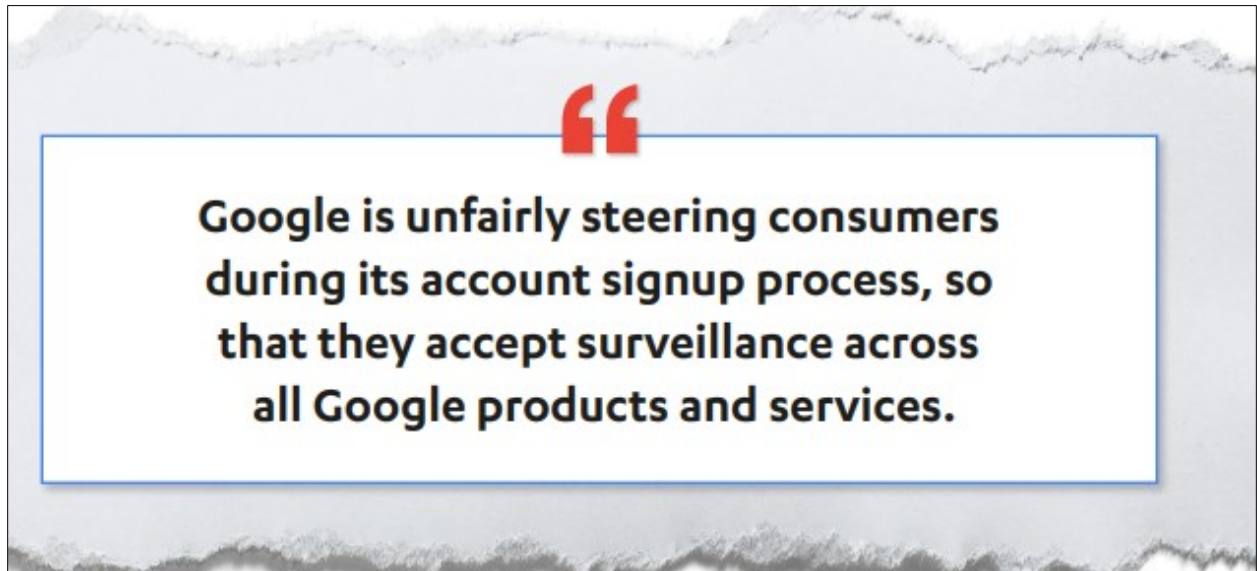
⁴ https://www.beuc.eu/publications/beuc-x-2022-074_letter_to_commissioner_reynders_-_google_gdpr_action.pdf; https://www.beuc.eu/publications/beuc-x-2022-075_letter_to_andrea_jelinek_-_google_gdpr_action.pdf; https://www.beuc.eu/publications/beuc-x-2022-076_letter_to_mr_wojciech_wiewiorowski_-_google_gdpr_action.pdf

⁵ <https://tacd.org/google-puts-its-users-on-a-fast-track-to-surveillance-eu-and-u-s-groups-urge-authorities-to-take-action/>.

2022 letter from the TACD to the United States Federal Trade Commission,⁶ both of which I discuss below.

BEUC Report

The BEUC Report analyzes Google’s Account Setup process and argues that Google makes it “much more cumbersome to say ‘No’ than to say ‘Yes’ to all Google’s data processing.” (BEUC Report at 8–9). The Report explains that Google engages in “[s]urveillance by design and by default” through its default enabling of the Web & App Activity and Ad personalization settings during Account Creation, and notes that even if users go through the lengthy process of manually disabling Google’s tracking, they are faced with “unclear, incomplete, and misleading” information “at every step of the registration process.” (*Id.*). The report concludes that Google “is deliberately steering consumers to allow an extensive and invasive processing of their personal data,” “a practice [that is] considered a ‘dark pattern’ by the European Data Protection Board and which runs counter to the principle of data protection by design.” (*Id.*).



(*Id.* at 3).

While some of the BEUC Report is focused on Google’s practices in Europe, the principle—that Google employs “a combination of deceptive design, unclear language, misleading choices and missing information”—is consistent with the opinions and analysis in my Opening and Rebuttal Reports. (*Id.* 8–9). In fact, as discussed below, the TACD explains that these concerns apply in the U.S. and, in some instances, are even more problematic.⁷ I addressed

⁶ <https://tacd.org/wp-content/uploads/2022/06/20220630-TACD-FTC-Google-Account-Letter.pdf>.

⁷ The TACD press release from footnote 5 (in this supplemental report) on 30 June 2022 notes “the key concerns [relating to the Google sign-up process] shared on the other side of the Atlantic remain and, in some cases, are even more hidden from consumers.”

many of these points in my prior reports. Further, the BEUC argues that “much against Google’s claim that users are in control of the data that the company collects and how it is used, the signup process is engineered to serve the company’s interests,” not the interests of users. (*Id.* at 4). This supports my overarching opinion that Google manipulates the choice architecture in order to prioritize stakeholder value at the expense of end users.

For example, in Appendix 4 to my Opening Report, I provided screenshots of a Google Account Setup flow in which users must tap a small “MORE OPTIONS” button at the bottom of Google’s Privacy and Terms in order to even have the option to review the Web & App Activity and Ads Personalization settings. If they don’t tap “MORE OPTIONS,” and instead tap “I agree,” their account will be created with WAA and Ads Personalization enabled, without ever having the option to disable either setting or learn about their functions. Moreover, even after tapping the “MORE OPTIONS” button, users are still not presented clear information about what these settings do—they have to tap a further “Learn more” tooltip button under each setting to get a fuller picture. As I have explained, burying these defaulted-on settings multiple clicks behind the privacy policy exhibits the dark patterns *sneaking* and *obstruction* by hiding or delaying the discovery of information necessary for users to make informed decisions. In line with this analysis, the BEUC concludes that “Google’s processing of personal data is not fair, because the design elements during and after signup seek to influence and/or cause the data subject to agree to more processing of personal data than he otherwise would have.” (*Id.* at 12).

I have also explained how Google utilizes dark patterns in its settings, services, and policies to maximize the location data it collects from its users, which ultimately powers its advertising services. The BEUC agrees, and also notes that Account Setup is “one of the main entrances to the Google data mining universe and the red thread that connects everything Google users do,” and thus has “important repercussions” for both consumers’ data and Google’s advertising revenue. (*Id.* at 5–7). The BEUC report also explains that certain “Google services – such as Gmail and the Play Store – require a Google account before they can be accessed.” (*Id.* at 3). The BEUC report also explains that “Google provides a myriad of products and services, including the Android mobile operating system, Chrome browser, YouTube, Google Search, Gmail, Google Maps and the Google Play Store,” and the report explains how Google uses such an account to “unify” a user’s experience across all of Google’s services. (*Id.* at 3). As the BEUC notes in its Frequently Asked Questions document published along with the press release, Google’s “extensive and invasive tracking, profiling and ad-targeting practices . . . fuel its advertising revenue” and have made Google “one of the undisputed heavyweights of ‘surveillance capitalism,’ with 81% of its revenue coming from ads.”⁸

BEUC Model Complaint

As I noted above, the BEUC also prepared a “model complaint” for regulators to bring legal actions against Google. The Complaint includes detailed allegations that Google unfairly steers and manipulates users towards invasive data collection.⁹ The model complaint alleges that

⁸ https://www.beuc.eu/publications/beuc-x-2022-070_fast_track_to_surveillance_faq.pdf

⁹ <https://www.beuc.eu/publications/model-complaint-google-2022/html>

Google designs its sign-up process in a way that leads users “‘into making unintended, unwilling and potentially harmful decisions regarding the processing of [their] personal data,’ to the extent that they constitute ‘dark patterns.’” (Model Complaint ¶ 60). For example, it alleges that Google hides important information “‘behind extra clicks within the ‘Learn More’ section,” including information concerning WAA’s collection of personal data. (*Id.* ¶ 70.1).

The BEUC’s attention to Google’s use of dark patterns further supports my opinion that the significant regulatory efforts combatting dark patterns prove the legitimacy of the field. Google’s experts go to great lengths to undermine the field, but BEUC report and the related GDPR lawsuits are another example among the extensive regulatory and legislative efforts cited in my prior reports.

The model complaint also references discovery documents from a litigation called *Calhoun et al. v. Google LLC*, which I understand to be a case in United States Federal Court in the Northern District of California. Some documents from the *Calhoun* case are excerpted in Annex 3 to the model complaint. Specifically, Annex 3 indicates that these documents were exhibits to a “Cruz Decl.” from the *Calhoun* litigation. After I raised the BEUC report with the State’s counsel, I understand they were able to obtain some of those documents from the *Calhoun* litigation. Some of those documents have now been provided to me in the form that they were attached in the Cruz Declaration.

For example, the model complaint quotes an April 9, 2018 “internal email” (that was attached as Exhibit 5 to the Cruz Decl.) in which Google acknowledges that “we know that terms like ‘web & app activity’ mean zero¹⁰ to a user” and that the term “activity” “confuses users.” I understand that the BEUC is referencing a document produced in the *Calhoun* litigation as GOOG-CABR-04994797. After reviewing the document, I note that David Monsees—the product manager for WAA—was the one who said that “terms like ‘web & app activity’ mean zero to a user” The document includes further discussions involving Mr. Monsees and his colleagues at Google, where they acknowledge that Google has long believed that the nomenclature for WAA is misleading. Another email (dated March 12, 2018) from Mr. Monsees in that same chain explains “we still believe it confuses users,” acknowledging that “UXW/UXR could use a decision.” (GOOG-CABR-04994797 at 99).

The Monsees “WAA-means-zero” email is yet another example of the “naming deception” discussed in my prior reports. It further shows that Google knew that the name of WAA was highly misleading to users. As discussed in my prior reports, the nomenclature fails to convey any relationship between the WAA setting and the location tracking that it is used for, much less the extent or exploitation of the data collected by that setting. In my prior reports, I explained that this amounts to a “sneaking” dark pattern because Google attempts to misdirect or delay user acquisition of information. I further note that the WAA-means-zero email confirms that not only has Google long known that the WAA name is itself misleading, but more than four

¹⁰ I underline this key language because I subsequently refer to the document as the “WAA-means-zero” email. I use the same practice for the new documents below.

years after the “WAA-means-zero” email—and indeed, four years after Monsees said that “UXW/UXR could use a decision,” the setting is still called WAA.

The BEUC also quotes another internal document (that was attached as Exhibit 6 to the Cruz Decl.), and was produced in the *Calhoun* litigation as GOOG-CABR-04754292. I understand this document has not been produced in the current litigation, and the version available from the Cruz Decl. is redacted, undated and without any metadata that would identify authors, custodians of the document or other information that may be relevant. Even without these details, the document appears to be an internal policy document prepared by Google’s Privacy and Data Protection Office (PDPO).¹¹ In it, Google acknowledges that its “current approach to data collection is fundamentally problematic and at the core of the privacy challenges we face today.” (*Id.* at 93). The document goes on to state:

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**.

What’s more, our *one vast interconnected ecosystem* premise doesn’t align with how people actually engage with Google; **most use fewer than 6 services, and the connections between them range from subtle to non-existent**. So while we communicate that *data in = value out*, depending on the configuration of someone’s individual Google ecosystem, they might not experience any benefit at all as a result of turning on WAA.

[. . .]

When people consent without knowing *what* exactly they’re agreeing to share with Google – and what’s “in it” for them – they “set and forget” the toggle – then are often negatively surprised by unexpected personalisation down the line. After all, the things Google knows about them are like dark matter in the universe. People may understand that *something* is there, but don’t really know what, or why, or how that might impact their lives.

(*Id.* at 93–94) (emphasis in original).

¹¹ The document explains that it “details the foundation upon which we will craft the **PDPO’s 5-year user privacy experience** vision” and claims that “**PDPO’s role at Google** needs to evolve.” GOOG-CABR-04754292 at 92. PDPO at Google refers to the Privacy and Data Protection Office, which is an “umbrella group” that contains Google’s Privacy Working Groups. (2/27/2020 Berlin EUO Tr. at 97:2-19). As I discussed in my Opening Report, Google’s Privacy Working Group recommended against moving the location master setting from the Android Quick Settings Panel, but Google proceeded to do so anyway. (Opening Report at 30).

The “fundamentally problematic” document further supports my opinion that Google’s settings and user interface mislead and deceive users into what they are consenting to and hides relevant information from them, as explained in my prior reports. The “fundamentally problematic” document also shows Google’s knowledge that users not only lack awareness that data is being collected, but also how that data is being exploited when collected. As I explained in my opening report, both of these practices are forms of *sneaking* and *forced action* that prevent users from acquiring information important to their decisions to use Google products and services, which has the material impact of forcing users to agree to broad and invasive data collection in order to use those services.

Like the WAA-means-zero email, the “fundamentally problematic” document also reinforces that Google has long been aware of the problems associated with WAA (and other settings). In the “fundamentally problematic” document, the PDPO explains that it must become “a **necessity** to unlock a model for permission that makes sense for users and for our business.” (*Id.* at 97), noting that “[a]chieving these goals will require fundamental rewiring of our cross-Google infrastructure, with a renewed focus on coherent, auditable systems that enable us to trace personal data from collection to use—and map that data to the experience it powers.” (*Id.* at 96). It seems like Google understands that the permissions do not currently “make sense for users.” (*Id.*).

The “fundamentally problematic” document also has a section called “Previous version below.” Under the heading “contradictory consents,” Google acknowledges that at least its “ads *measurement* practices,” which are “necessary to deliver value to our partners, and therefore core to our business,” do not “provide value to our users.” (*Id.* at 301). Google also acknowledges, “The fact remains that we do a bunch of stuff that doesn’t benefit any given user.” (*Id.* at 304). This section acknowledges that Google needs a complete “fundamental” “180° turnaround” in its “relationship with our users,” complete with a proposed “Google 180” logo. (*Id.* at 302-303).



The draft document also proposed that Google “should give users a feeling or safety” (which I suspect means a “feeling of safety”) “and be proof points of Google actively protecting the user’s privacy.” (*Id.* at 309). In this new world, “we [Google] need to tangibly deliver on the premise that data is only being collected, user and shared for explicit value.” (*Id.*). On the same page, Google acknowledges that WAA and other overarching data models and their respective controls will not exist in the proposed system” and that the “current data review and control products ... and surfaces ... need to be rethought.” (*Id.*). Additionally, labeled as part of an “ongoing conversation,” this document notes that “[t]oday, Google’s privacy experience is defined by a pattern of set-and-forget”—a characteristic of at least some of the dark patterns employed that I note in my Rebuttal Report which tend to be felt over a long period of time by users (Rebuttal Report at 16).

The “fundamentally problematic” documents also include comments from Google employees, although no names are attached to those comments. In Comment [6], one Google employee notes as follows when discussing the proposed “user-defined ecosystem”: “anyone concerned that we lose the ‘break up waa’ gut-punch?” Another Google employee responds in Comment [7], “No – because WAA is only part of the problem and we don’t want to push a Google-wide approach into a smaller box.” Again, Google recognizes the problematic nature of WAA (in Comment [6]), and recognizes that it is part of a “Google-wide” problem (in Comment [7]). Despite the recommendation in this document, I am unaware of any “break up” that actually occurred with respect to WAA, and the name remains unchanged. I also haven’t seen anything suggesting that that “Google-wide” changes have been implemented.

Next, the BEUC quotes another internal PDPO document that highlights “[k]ey experience challenges,” which was attached as Exhibit 7 to the Cruz Decl. produced in the *Calhoun* litigation as GOOG-CABR-04754160. The document provides a “Mission” that states, “This workstream aims to define an overarching vision and strategy for PDPO to inform the Google privacy experience across products and services according to a 5-year time horizon.” (*Id.* at 60). The document notes that “[i]t’s difficult for people to fully / meaningfully give permission” to Google’s data collection. (*Id.* at 61). The document further notes that “[n]ot only are the implications of WAA extremely broad and varied, but people use Google in such diverse ways – much of the language intended to be comprehensive feels vague and hard-to-parse for non-engineers / lawyers, and our examples are not universally relevant.” (*Id.*). According to the document, this “lack of clarity” 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’s services,” and giving consent “despite an inaccurate or incomplete understanding of” Google’s data collection products. (*Id.*). Again, I understand this document has not been produced in the existing litigation, so I do not have access to the complete unredacted document or to any of the relevant metadata for it.

The “difficult-to-meaningfully-consent” document further includes a discussion called “Unclear role of personalized ads,” where Google acknowledges that “Personalized ads trigger mistrust, reinforcing misconceptions and feelings of exploitation.” (*Id.* at 63).

The “difficult-to-meaningfully-consent” document also explains and corroborates one of the primary concerns with dark patterns, which I discussed in my prior reports. In contrast to the assertions of Dr. Ghose (Ghose Report starting at 7) that users knowingly and willingly choose to give up their data to gain value, this document notes that even “[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 *Google still has an incentive to get them to accept!*” (GOOG-CABR-04754160 at 65) (emphasis in original). Google further acknowledges that **actually** “empower[ing] a given user to be *in control of their privacy ... would cripple [Google’s products.]*” (*Id.*). This is one of the hallmark of dark patterns—Google manipulates users to enable settings that are in Google’s interests, even when users would not otherwise do so. Of course, as discussed in my other reports, this manipulation is all the more relevant in contexts where Google employs defaults to opt-in users in the first place or—as with IPGeo and Realtime

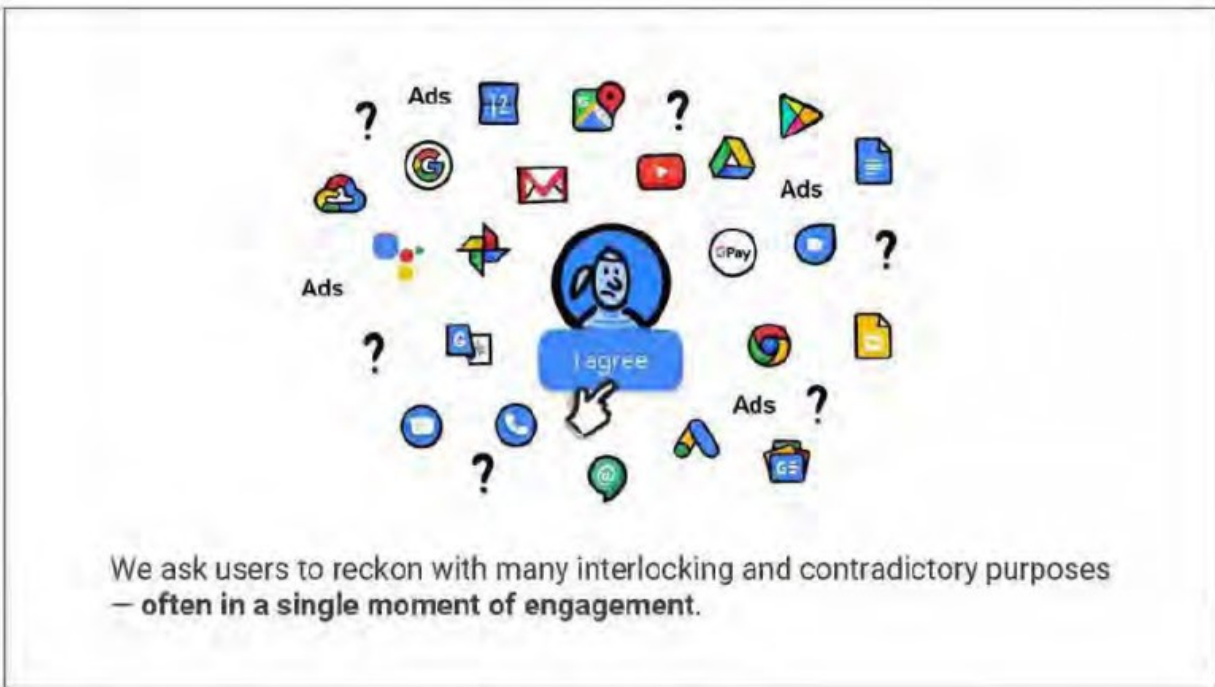
IPGeo—Google does not offer any opt-outs at all in ways that are almost completely obscured to end users.

I further point out that Google’s expert Dr. Ghose criticized me by suggesting that my report does not address whether any of these concerns are “in connection with” the sale of merchandise. (Ghose Report ¶ 101). I previously responded that Google’s dark patterns are in connection with its sale of Android devices, which are pre-installed with the software and user experience I have analyzed. I also note that the “difficult-to-meaningfully-consent” document (which I understand Google has still not produced to the State) actually addresses some of this. For example, the document includes a Comment [11] that users “acknowledge (and mostly) accept that the benefit to them is being able to use free products and services, and the ‘cost’ is ‘paying’ with their data.” (GOOG-CABR-04754160 at 62). The document also notes that many users “feel their data is the ‘price they pay’ to use Google.” (*Id.* at 63).¹²

The “difficult-to-meaningfully-consent” document also adds, “The extent to which people feel seen (and often followed) by advertisers triggers concerns about being profiled, surveilled, and even manipulated.” (*Id.*). In the document, Google also acknowledges that “It’s unclear to people what information is shared with our advertising partners & websites (3p), and what role our users play in our revenue model.” (*Id.*). Again, these statements confirm my opinions (discussed above as well) that Google forces action, controlling information flow in order to mislead and deceive users into providing location data.

¹² Even for users for whom this is true, they do not necessarily know how much or which data Google collects or what Google does with it. As the document explains. Google’s collection of “data for two core and contradictory reasons”—some of which might be immediately visible to the user in the form of “data at work in the products they use” and other uses for “users (plural)” perhaps somewhat or completely opaque to end users. (GOOG-CABR-04754160 at 63, 65). The document also describes lack of perceived or actual value experienced by users, as addressed elsewhere in this document. (*Id.* at 62).

The BEUC also includes an image from a Google slideshow that was attached as Exhibit 10 to the Cruz Declaration and produced in the *Calhoun* case as GOOG-CABR-04754257. Again, to my understanding, this document was not produced in the current litigation and only a redacted version is available with the Cruz Declaration. On its face, it appears to be dated September 2, 2020, and appears to be another document from the PDPO. In my opinion, this diagram also supports my opinions and depicts the mental overload that users can experience when faced with the dark patterns that I have highlighted. The image further supports my opinion in my prior reports that Google’s “Privacy Maze” approach to user interfaces and practice of hiding relevant information behind numerous “learn more” links mislead, deceive, and confuse users.



(GOOG-CABR-04754257 at 70). The document notes that Google needs to “**Align** on the key aspects of our perspective and the path forward,” but that there are “**no solutions yet.**” (*Id.* at 59). According to the PDPO, Google’s “permission structure . . . is based on the premise that our users understand – and are on board with – our ecosystem,” but “people DON’T understand the ecosystem and instead think of Google as the products they personally use,” which “calls our integrity / intentions into question” and “reinforces confusion/suspicion about creepy ads / tracking.” (*Id.* at 70). The “Graveyard” portion of the document also includes a slide stating that Google must “reckon with the fact that our mindset and underlying mechanisms must be **fundamentally rewired** in order to support **meaningful** transparency and control,” and points out that Google collects “data in a huge bucket and allow[s] it to flow wherever and whenever, noting that “Even **we** [Google] can’t trace it” and “People can’t follow how / whether sharing their data translates to value for them.” (*Id.* at 76, 88) (emphasis in original). Another slide states that Google’s “Broad permissions structure” “can feel incomprehensible & overwhelming” because just “a few permissions cover[] a broad scope of activity, info & data collection and use.” (*Id.* at 89). This document confirms and reinforces my opinion that Google presents the

appearance of user control, but ultimately uses forced action to ensure that users’ location data is collected and exploited.

Ultimately, each of these documents excerpted in the BEUC’s model complaint (Annex 3) provide further support for the opinions in my prior reports. They show that Google knew that its user interfaces were misleading, confusing, and deceptive to users.

TACD Materials

On June 30, 2022, the TACD published its own press release, “Google puts its users on a ‘fast track to surveillance’: EU and U.S. groups urge authorities to take action.”¹³ Citing the BEUC report, the TACD explains, “When testing the sign-up process in the U.S., our members found that while slightly different in structure, the key concerns shared on the other side of the Atlantic remain and, in some cases, are even more hidden from consumers. In the U.S. sign-up process, several design choices are made to highlight options that would enable the most possible information collection and use.” The TACD also explains that a “Google account is the red thread which connects how users’ data is used across all Google services,” and that consumers can either “create a Google account voluntarily”—meaning before purchasing an Android phone or using Google services—“or be obliged to create one when they user certain Google products and services.” (*Id.*). The TACD explains that users “must” create a Google account when they buy a smartphone that uses Google’s Android operating system if they want to use the Google Play store. (*Id.*)

Similarly, the TACD press release quotes Calli Schroeder, the digital co-chair for the U.S. at the TACD, that Google’s “practices likely violate the FTC Act, a law that empowers the agency to prevent deceptive practices that harm consumers.” (*Id.*). On that note, the TACD wrote a letter encouraging the FTC “to open an investigation into Google’s practices when a consumer creates a Google account.”¹⁴ (*Id.*). In the letter, the TACD contends that the practices identified by the BEUC “are also a violation of Google’s obligation to refrain from unfair practices within the U.S. and that these actions can and should be investigated by the Federal Trade Commission.” (*Id.*). The TACD explains that its members “signed up for a Google account from a U.S. location to investigate the process here,” and its letter details some of those findings starting at page 2 of the letter through the end. Rather than quote that discussion, I incorporate those findings by reference.

Again, as noted above, this confirms the opinions in my prior reports that Google manipulates the choice architecture and information flows available to users to obtain significant amounts of location data from them by sneaking them into preselected and invasive states during Account Creation and obstructing them from getting out of those states.


¹³ <https://tacd.org/google-puts-its-users-on-a-fast-track-to-surveillance-eu-and-u-s-groups-urge-authorities-to-take-action/>

¹⁴ <https://tacd.org/wp-content/uploads/2022/06/20220630-TACD-FTC-Google-Account-Letter.pdf>

Further Work

I have not yet located the complaints referenced in footnote 1 of the BEUC's press release. I understand these may not be in English, but I will attempt to learn more information about them. I also understand that the Cruz Decl. includes other documents that were not excerpted in the BEUC's model complaint. I have not had a chance to review those yet. I understand many of these documents were not produced by Google in the present litigation brought by the State of Arizona. My investigation is ongoing with respect to this new information, and I reserve the right to supplement further.

Colin M. Gray, PhD

A handwritten signature in black ink that reads "Colin Gray". The signature is written in a cursive style. To the right of the signature is a horizontal line that extends to the right edge of the page.

July 11, 2022