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

Public Redacted Version

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

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

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

June 22, 2022

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY

PURSUANT TO PROTECTIVE ORDER

Table of Contents

I. Introduction

I, Colin M. Gray, previously submitted a report in this action on May 4, 2022 (my "Opening Report"). I have received and reviewed the Expert Reports of Drs. Ghose, Steckel, Hoffman, and Arnold, and submit this report to respond to certain of the opinions and conclusions in those reports. In addition to the materials that I considered in preparing my Opening Report, I have attached as Appendix 1 a list of additional materials I considered in preparing this Rebuttal Report.

II. Google Is Presenting the Wrong Experts

Google has engaged three (or four, counting Dr. Arnold) experts to rebut my Opening Report. None of these individuals purport to have expertise in relevant fields for adequately understanding or responding to my opinions. As far as I can tell, none of these Google experts have expertise in the fields or disciplines of user experience (UX) or human-computer interaction (HCI)—fields which have been central to the study of dark patterns—much less in assessing the presence or impact of dark patterns in user interfaces. From the materials they submitted, Drs. Steckel, Ghose, Hoffman, and Arnold are all business, marketing, and economics scholars, lacking the experience and professional qualifications in UX and HCI research necessary to render valid and reliable conclusions on those subjects.

Dr. Ghose, for example, is an economics scholar and Professor of Business, but does not suggest that he has any practical or research experience in designing or understanding user experiences. (Ghose Report Appx. A). Dr. Ghose acknowledges that he is "not opining on whether Google's UI and location collection practices evidence 'dark patterns' . . . ." (*Id.* ¶ 13(c)). It seems Dr. Ghose only offers a string of criticisms that my Report is not somehow "scientific" enough—presumably based in his own quantitatively-focused economics perspective. With all respect to his field of study, economics is not the only field that engages in scientific inquiry, and this framing improperly ignores other legitimate and foundational forms of inquiry common elsewhere in the social sciences. Also, as explained below, his criticisms are incorrect.

Dr. Steckel is a Professor of Marketing, who claims experience in the fields of corporate branding, accounting, and statistics. (Steckel Report Appx. A). Aside from preparing consumer surveys, it appears that Dr. Steckel has no experience researching, analyzing, or creating user interfaces. (*Id.*). He claims no expertise in those areas. Like Dr. Ghose, Dr. Steckel does not appear to offer any opinions concerning whether Google's design decisions are misleading, deceptive, or confusing, and his report provides no response to my key claims of dark patterns in Google's interface relating to location settings.

Dr. Hoffman is another Professor of Marketing. From what I can tell from her vita, she does not have (and does not claim to have) any practical or research-based experience dealing

with UX design or HCI. (Hoffman Report Appx. A).[1] She also does not claim to have any experience or expertise in identifying, assessing, or analyzing dark patterns, from what I can tell. As I discuss below, her "UI Analysis" is also contrary to typical forms of analysis common in the practice of UX design.

Dr. Arnold is another economist. He says that his assignment was to "respond to the calculations of disgorgement damages and opinions relating to civil penalties in the Levy Report, including assessing alternative remedies, assuming liability and causation are established in some fashion," but he also seems to offer opinions regarding what Google did or did not disclose to its users and other issues outside of his claimed area of expertise. (*E.g.,* Arnold Report ¶¶ 45, 59, 60, 76, p. 35 n. 73). To my knowledge, Dr. Arnold is not, and does not hold himself as, an expert in disclosures, user experience, or human-computer interaction. It is not clear to me whether Dr. Arnold purports to render opinions on these points or if, instead, he is relying on others. If it's the former, I do not see how he has the expertise to render these opinions. If it's the latter, he does not explain who or what he is relying on, which makes it very difficult to address.

In contrast, I was involved in commercial design work from the late 1990s until the mid-2010s, and during that time worked for Fortune 500 clients and small businesses alike in building brand strategy, producing print materials, and developing websites and other digital products. Starting in 2015, I led the creation of one of the first undergraduate UX Design programs in the United States at Purdue University. As part of this program, I have contributed to the training of hundreds of UX design students that have gone on to roles in industry that include UX Researcher, UX Engineer, Product Manager, and UX Designer, among others. Through my professional work as a designer, art director, web developer, and now program lead for undergraduate and graduate programs at Purdue, I have worked extensively with colleagues and students to address issues related to privacy from a usability and UX perspective. These experiences—as a designer, a mentor, critic, and educator—supplement my experiences as a researcher in the domains of technology practice and dark patterns, enabling my analysis and supporting my theoretical contributions in my home disciplines of human-computer interaction and design.

One point that illustrates Google's expert's collective lack of experience and expertise is Drs. Hoffman and Ghose's discussion of a paper by Mathur et al. (2021) entitled *What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods*. Both Drs. Hoffman and Ghose seem to hone in on the same words in that study to argue that Mathur et al. purportedly shows that Dark Patterns research is "highly fragmented" (Hoffman Report ¶ 28) and "riddled" with "contradictions" (Ghose Report ¶ 77(b)). The

[1] Dr. Hoffman also appears to offer an opinion that I have not offered "scientific testimony," and that "to offer an expert opinion admissible at trial an expert must offer scientific testimony based upon scientifically valid reasoning." (Hoffman Report ¶ 33). As far as I am aware, Dr. Hoffman is not an expert in the standards for admissibility of expert testimony, nor is she an expert in what constitutes "scientific testimony" or what can be presented at trial.

conclusions that Drs. Hoffman and Ghose draw from that paper are simply incorrect. They seem to misread the paper. To my knowledge, the subject matter of the paper is not in their area of research—it's in my area. In fact, the Mathur paper quotes and cites my own studies extensively, and both my papers and Mathur's relating to dark patterns have formed a highly-cited core of scholarship that guides both contemporary academic research and regulatory action relating to dark patterns.[2]

The study and existence of dark patterns is well recognized in the literature and in the "real world." As I explained in my Opening Report, the terminology for dark patterns has been in the process of converging for the last decade, which is something recognized by Mathur and was foreshadowed in my initial 2018 paper. The "shaky foundation" quote is in reference to the terminology used for describing dark patterns in more precise ways, not the field's validity in evaluating instances where "dark patterns modify the underlying choice architecture for users." (Mathur et al. 2021). In building their argument, Mathur et al. cite my work sixteen times, and incorporate the taxonomy constructed in my 2018 paper (and applied in my Opening Report) as part of its effort to "synthesiz[e] dark patterns definitions, types, and taxonomies from recent scholarship into a pair of themes." (*Id.*). Mathur recognizes that the terminology itself is now converging—bringing with it shared language from design, behavioral economics, web measurement, and law.[3] Either way, Mathur also believes that "the dark pattern definitions and taxonomies in prior work [such as my 2018 paper] have been exceedingly valuable for surfacing descriptive insights and calling attention to problematic practices." (*Id.*).

I know Dr. Mathur, so I called him up to get his reaction to these characterizations of his paper.[4] Dr. Mathur confirmed my belief that Google's experts are misinterpreting his paper.[5] He explained that the intent of the paper was to highlight and further contribute to the building of

---

[2] As of June 2022, the Mathur et al. 2021 paper has received 42 citations and a previous Mathur et al. 2019 paper on the presence of dark patterns in e-commerce settings has received 196 citations. Both papers were cited in a recent EU Commission report that guides ongoing regulatory action in the EU relating to dark patterns. *Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation*. (2022). Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418

[3] See an expanded account of this disciplinary convergence in Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021, May). Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411764.3445779

[4] I kept my discussion high-level and focused on his article, without disclosing the parties. I wanted to share the expert reports (mine and Google's), but I understand Google has designated those as "Highly Confidential," including the discussion of Dr. Mathur's work. I understand that the State has asked Google to de-designate these reports (as well as my report), but so far that has not happened.

[5] Conversation with Dr. Arunesh Mathur, June 20, 2022.

consensus in the literature. His primary claimed contribution for this paper included providing a shared vocabulary regarding the various attributes of dark patterns, which he created by distilling those attributes from a range of papers—including my own—into *themes* and a common taxonomy concerning manipulation of the choice architecture.[6] He underscored that he and his co-authors did not use this paper to argue that the field is fragmented, contradictory, or incapable of rigorous analysis. Dr. Mathur further clarified the "conceptual inconsistency" and "shaky foundation" quotes that Google's experts hone in on, and confirmed (as I suspected) that there is consensus on the objective criteria that determine whether UI elements exhibit attributes of dark patterns. The goal of this paper, as Dr. Mathur stated, was to rally the academic community to cohere the various taxonomies in the literature and extract themes to succinctly describe dark design elements. He noted that my 2018 paper is a foundational work in the field, and the taxonomy I provided is highly accepted by researchers and scholars. Dr. Mathur also noted that the significant regulatory efforts targeting dark patterns (including those I discuss) are a testament to the validity and usefulness of dark patterns in consumer protection. Dr. Mathur currently works for the Competition & Markets Authority (CMA) in the United Kingdom, where he uses his expertise in dark patterns to enforce UK consumer protection laws. We also talked about some of the different types of dark patterns discussed in our work, including the notion that some dark patterns include false statements whereas other can be deceptive without affirmative misstatements. He pointed me back to page 8 of his paper, where he points out that dark patterns can be deceptive by inducing "false beliefs in users through affirmative misstatements, misleading statements, or omissions."[7] On the call, Dr. Mathur invited me to come give a talk at the CMA on my next visit to the United Kingdom.

As another example of misunderstanding the literature, Dr. Hoffman asserts that dark patterns are a "nebulous construct." She also accuses me of "not rigorously defining" what I mean by dark patterns. Again, most of Dr. Hoffman's discussions appear to reflect the fact that she is not in this field of study and has not previously published on the topic. She does not suggest that she has ever researched or evaluated dark patterns at any time before her current report. She cites two posts from Dr. Brignull at a time when he was still developing his terminology by compiling and evaluating examples of dark patterns, which he then used to form a typology that categorized these instances on his website darkpatterns.org.[8] Again, researchers

[6] Namely, the themes of "modifying the set of choices available to users" and "manipulating the information that is available to users," (Mathur 2021) which I use as part of my analysis framework in my Opening Report.

[7] That discussion in his paper also includes other attributes of dark patterns like "Assymetric dark patterns" that "impose unequal burdens on the choices available to the user", "covert dark patterns" "that push a user toward selecting certain decisions or outcomes, but hide the influence mechanism from the user," "Information hiding dark patterns," that "obscure or delay the presentation of necessary information to users," "Restrictive dark patterns" that "reduce or eliminate the choices presented to users," and "Disparate treatment."

[8] Harry Brignull, "Darkpatterns.org: naming and shaming sites that use black hat, anti-usability design patterns," August 16, 2010, https://90percentofeverything.com/2010/08/16/darkpatterns-org-naming-and-shaming-sites-that-use-black-hat-anti-usability-design-patterns/index.html;

in my field (including myself, Dr. Brignull and others like Dr. Mathur) have sought to create a convergence of terminology, so that practitioners, researchers, and regulators alike can apply taxonomies derived from rigorous studies of exemplar material.

Setting aside issues of taxonomy, the existence of dark patterns is widely accepted in both technology disciplines at large, and as a phenomenon that can be scientifically assessed by experienced researchers. As evidence of this, my work (and that of others, like Drs. Brignull and Mathur) has been supported by rigorous methods of analysis, evaluated and peer reviewed, and published in high quality venues within the UX and HCI space. These studies have gone on to be cited dozens or hundreds of times, and my (and my co-authors) claims (including as described in my Opening Report) are well-accepted in these relevant scientific communities. Dr. Hoffman is potentially unfamiliar with that research because she is not in a relevant field. She has not studied the dark patterns literature or otherwise contributed to this scientific discourse, and I have not seen her contributions at any of the key academic conferences that have produced critical scholarship on this topic.

Dr. Hoffman's attempted rebuttal of my opinions concerning Google's Search Results Footer is yet another example. (Hoffman Report ¶¶ 173–74). Not only does she cite articles inapplicable to the specific search results page context (*i.e.* the sources cited discuss footers for general purpose websites, not search results pages),[9] but she also uses these practitioner self-published web posts to purport that all "UX experts" believe these specific aspects of footers are design best practices in all contexts. The authors of these two posts (the "marketing guy" and the "technical researchers and writer") did not say anything that responds to my opinions. The marketing post describes elements that the authors feel should be at the bottom of a company's website (which is not necessarily going to be reviewed on a smartphone), such as a link to a contact page, privacy policy and similar things one might expect to find at the bottom of a company's website. Similarly, the post from the technical researcher describes a range of generic types of content that might be present on many company websites, but nothing specific to the design context I evaluated. This guidance—whether correct or not—has nothing to do with whether readers are likely to scroll all the way down to the bottom of a list of search results (often on their smart phone) to find a footer that tells them how their location was calculated. Further, recent scholarship has shown that a more frequent use of "infinite scroll" on web sites—common on many types of sites, even if this functionality is not currently used on Google's Search Results page—negates even the presence of footers since content continues to load in

Harry Brignull, "Dark Patterns: dirty tricks designers use to make people do stuff," July 8, 2010, https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/index.html.

[9] McGowan, Sean, "UX Design Tips To Put Your Best Footer Forward," UsabilityGeek, https://usabilitygeek.com/ux-design-tips-best-footer/. Crestodina, Andy, "Website Footer Design Best Practices: 27 Things to Put at the Bottom," Orbit Media Studios, available at https://www.orbitmedia.com/blog/website-footer-design-best-practices/.

dynamically as users scroll.[10] I explained the concerns with the footers in my Opening Report, citing my analysis and expertise as well as peer reviewed studies. Dr. Hoffman's response using cherry-picked advice from practitioner blogs does not represent a rigorous or adequate rebuttal of my concerns.

Drs. Hoffman and Ghose also ignore (or are unaware of) the significant attention that regulators and lawmakers around the country (and around the world) are devoting to combatting dark patterns. For example, some states like California have expressly passed laws (like the Consumer Privacy Act) that "agreement obtained through use of dark patterns does not constitute consent" and mandating that opt-in notifications must "not make use of any dark patterns."[11] As another example, I attended the Dark Patterns Workshop put on by the Federal Trade Commission ("FTC"), where the FTC's Acting Director for the Bureau of Consumer Protection explained that dark patterns "already are illegal under Section 5 of the FTC Act and state laws prohibiting deceptive and unfair practices."[12] Congress is also presently considering something called the DETOUR Act, which would more expressly make it illegal to "design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data."[13] Similarly, the European Data Protection Board (EDPB) put out "Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them"[14] (Mar. 14, 2022)) and the recently passed Digital Services Act which explicitly bans dark patterns that are used to "manipulate users' choices."[15] I have been personally involved in some of these efforts. I was invited by members of Congress to offer feedback on the pending DETOUR legislation. I have been consulted by state enforcers (other than Arizona) to consult in assessing and enforcing anti-dark patterns actions. I was asked to comment and provide expert review on a report from the Competition & Markets Authority in the United Kingdom entitled "*Online Choice*

[10] Sharma, S., & Murano, P. (2020). A usability evaluation of Web user interface scrolling types. *First Monday*, *25*(3). https://doi.org/10.5210/fm.v25i3.10309

[11] Importantly, California's CPRA guidance describes that "A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business's intent." §7004.(c). https://cppa.ca.gov/meetings/materials/20220608_item3.pdf

[12] https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf

[13] https://www.congress.gov/bill/117th-congress/senate-bill/3330

[14] https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

[15] "online platforms and marketplaces should not nudge people into using their services, for example by giving more prominence to a particular choice or urging the recipient to change their choice via interfering pop-ups. Moreover, cancelling a subscription for a service should become as easy as subscribing to it" https://www.europarl.europa.eu/news/de/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment

Architecture: How digital design can harm competition and consumers"[16] that addressed and built upon my typology of dark patterns strategies. I have also worked with other scholars to provide feedback on pending regulation by the EDPB and am currently working on formal comments in response to the FTC call "on preventing digital deception"[17] with fellow dark patterns researchers. The suggestion from Dr. Hoffman that "dark patterns" are just some nebulous construct is not in accord with a history of work in the HCI field or the uptake of this term in a wide range of technology, design, legal, and regulatory contexts.

Further, I understand that regulators all over the country (and outside of the United States) are investigating Google over many of the same allegations raised by Arizona in this case, including dark patterns. (Google's 11/22/2021 Responses to State's Interrogatories, Set Six, at 3-4). Earlier this year, the State of Washington brought a lawsuit against Google, which expressly calls out Google's deceptive conduct through dark patterns on pages 22-29 as shown in Appendix 2. At least three other lawsuits brought by regulators in Indiana, Texas, and the District of Columbia have also brought the same dark-pattern allegations against Google. (Appendices 3-5). Each of them has an extensive discussion of "dark patterns," including the same ones I call out in my report, and I incorporate those discussions here.

In fact, Google's own engineers use the concept of dark patterns as an analytic tool when discussing product design decisions. (*E.g.,* GOOG-GLAZ-00073836.C at 36–38 (email chain discussing "Dark patterns in [Google] Assistant" because Assistant "is requesting Location History tracking, Web / Search / App activity, Device information (contacts / calendar), Voice & Audio Activity even for queries that don't need them."); GOOG-GLAZ-00086385 at 88 (noting that "many clicks in deletion flow" could "be a 'dark pattern' with so many steps until deletion?"). Google's engineers also recognize some of the core insights from dark patterns research coupled with user-centered design practices when designing products. (*E.g.*, GOOG-GLAZ-00046988.R at 88 (noting that "[g]ray text is often not noticed in flows and notices" and [d]ialog boxes with a lot of text do not get read.")).

In short, the existence of dark patterns and the ability of qualified scholars to assess their presence is well accepted. Not only is the evaluation of dark patterns well accepted in the literature, but it seems that regulators are converging on the non-controversial conclusion that Google's specific interfaces constitute particular problematic and deceptive dark patterns. There are many experts in dark patterns across a range of fields, including visual design, HCI, UX, web measurement, and law. Google disclosed no less than four experts to address my opinions, but none of them have experience in one or more of the relevant fields. I can only assume Google was unable to find anyone in the relevant fields who disagrees with my analysis and conclusions.

[16] https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers/evidence-review-of-online-choice-architecture-and-consumer-and-competition-harm
[17] https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-looks-modernize-its-guidance-preventing-digital-deception

Assuming one has the right expertise, I am not aware of anything that would be controversial in the opinions I have rendered.

III. Google's Experts Make Unsupported Assumptions, Which They Try to Pass Off as Facts

Google's experts make a variety of statements that undermine the independence and reliability of their opinions. They assume Google's good intentions in designing its user interfaces and disclosures. Essentially, their opinion appears to be that "Google is good" or that "Google follows user-centered design practices" and therefore its conduct cannot be deceptive. These responses are not based in prior literature and do not address the key issues I raised in my Opening Report that go well beyond positive intentions or a user-centered design approach.

For example, Dr. Ghose asserts that Google's "motivation to improve user experience" and its "intent to provide a good user experience with their products while being minimally intrusive on user's devices." (Ghose Report ¶¶ 60(b), 73, 87, 91 100). These statements appear to frame Google's motivation "to improve user experience" as evidence that aspects of that user experience were being adversely impacted by product decisions. Even a cursory read of key studies relating to users' experiences with various aspects of the locations settings that I cited in my Opening Report reveals substantial user confusion. In my analysis, Google's "apparent motivation to improve user experience" (Ghose Report ¶ 91) is immaterial, since the user interface itself—validated through user studies—shows that the user experience was poor in critical areas. Additionally, Dr. Ghose cites instances where I supposedly "ignore[d] statements that show Google's continued efforts related to improving user experience" (Ghose Report ¶ 100(c)), yet he dismisses as anecdotal Google's statements concerning its awareness of user confusion and ads-driven motivations for making changes to its interfaces. The focus of my analysis was to identify instances where Google's interface could be expected to deceive or mislead users, not to identify the positive motivations or aspirations of the design teams. Further, it is not clear on what basis Dr. Ghose is offering these statements or opinions. The lack foundation is particularly revealing because Dr. Ghose admits he is "not opining on whether Google's UI and location collection practices evidence 'dark patterns' . . . ." (*Id.* ¶ 13(c)).

In the same fashion, Dr. Steckel assumes—despite not opining on any Google interfaces and technologies—that Google has a "commitment to improve transparency and avoid confusion . . . ." (Steckel Report ¶ 34). While a commitment to key user-centered design practices is admirable, it does not rebut the clear instances identified in my Opening Report where users could be expected to be deceived or misled.

Dr. Hoffman's report also offers similar unsupported opinions regarding the supposed goodwill of Google. Dr. Hoffman asserts that Google "is a customer-centric company," (Hoffman Report ¶ 42), that it "is well aware that privacy concerns are highly contextual and individualized, and designs its UI accordingly," (*id.* ¶ 59), and that Google is the "paramount example" of a "[c]ustomer-oriented provider[]" that "do[es] [its] best to apply principles of good UI design," (id. ¶ 37). She does not cite any sources (much less analysis) to support these assertions. Elsewhere, she claims that Google "rigorously designs its interfaces with the consumer in mind" (Hoffman Report ¶ 30) and describes "Google's goal [] to provide a 'well lit

path'" (Hoffman Report ¶ 62), citing only her conversations with Dr. Gelke and David Warren. She further claims that Google has a philosophy "not to hide things from users" and "flags [important information] concisely to avoid overwhelming users," and has a "customer-centric culture of innovation and constructive use of feedback," again citing only conversations with Google-designated representatives (Dr. Gelke, David Monsees, and Marlo McGriff). (*Id.* ¶¶ 102, 111). I obviously do not know what these individuals told Dr. Hoffman, since she has only provided heavily redacted notes from two interviews. However, it is not reliable to conclude there was a lack of deceptive intent or potentially deceptive outcomes simply because a Google employee framed their company's potential intent in a positive manner.

Most importantly, from a UX evaluation perspective, this approach fails to look at the actual evidence itself. Rather than analyzing Google's designs and using that analysis to come to a reasoned conclusion about Google's actions, Drs. Steckel, Hoffman, and Ghose instead assume what Google set out to do and shoehorned their analysis to fit that assumption.

IV. Google's Experts Fail to Undermine My Methodology and Conclusions

As noted in my Opening Report, I was asked to analyze whether and to what extent Google employs Dark Patterns in its disclosures and user interfaces as they relate to the collection, use, and exploitation of consumers' location data. Accordingly, I collected and analyzed numerous Google interfaces, disclosures, and internal documents, categorizing the design techniques I observed and applying the typology created in my foundational paper, *The Dark (Patterns) Side of UX Design*. (Gray et al. 2018). This approach is typical in the field—generating a corpus of exemplary texts and interfaces, and analyzing and categorizing them according to the design techniques they employ.

Far from being a matter of my "say so," the identification of dark patterns in design exemplars has become common and rigorous in the HCI literature, with numerous analyses of digital products in a range of domains conducted over the past five years by researchers familiar with both conventional UI design practices and dark patterns. Assessing the presence of dark patterns is based on a professional evaluation of UI characteristics which include, but are not limited to: readable text; layout; relative size and positioning of UI elements; use of color, typography, or text decoration; feedforward or other forms of feedback to the user; task flows or other relations between UI elements and screens; and the context or medium of use. My own experience in training researchers to evaluate the presence of dark patterns has demonstrated that a basic knowledge of UI design principles and elements of user psychology[18] and familiarization with examples of each dark pattern type or strategy previously identified is important. Further, an evaluation that determines the presence of a dark pattern should be able to identify with a reasonable level of precision the type or combination of types of dark patterns being used, the ways in which the choice architecture is being modified, and how the combination of the dark

[18] The most comprehensive collection of perceptual and behavioral psychology principles relating to UX and HCI work is Johnson, J. (2020). *Designing with the Mind in Mind: Simple Guide to Understanding User Interface Design Guidelines*. Morgan Kaufmann.

pattern and modified choice architecture may contribute to user confusion, steering, manipulation, deception, or coercion. One does not need to rely on my "say-so," nor is that how I presented my opinions. Instead, my report engages in a ***content analysis***[19] of Google's user interfaces and disclosures, analyzing the way they limit the choices available to users and convey misleading or untrue information or impressions. Others can evaluate the specific flows and interfaces to assess potential dark patterns, including by evaluating aspects such as the underlying modification of the decision space, or manipulation of the information flow, as well as evidence from the user interface, designer's decisions, and/or the user's experience of the interface.[20] These various aspects can be assessed against some of the objective criteria using the taxonomy in the field, including from the works of Dr. Brignull, Dr. Mathur, and my own work.

My Opening Report follows this rigorous approach. For example, I analyzed Google's removal of the location toggle from Quick Settings in Android. I first pointed to documents evidencing Google's design intentions—the toggle was causing a decline in "location attach rate[s]" (and a substantial impact on Google's revenue), so Google wanted to discourage the use of that toggle. (Opening Report pp. 29-30, 36-37). I evaluated that stated design motivation in relation to the actual design change—"moving [the location toggle] below the fold, behind a dark-grey-on-black *Edit* button"—*i.e.*, removing or moving the toggle. I explained that this made toggling location off more difficult; by removing the control from the easily-accessible and highly-used quick-settings pane, users were required to either re-add it to their QS panel or to navigate to their device's settings if they wanted to manage their device location setting. In other words, it was an ***obstructive*** design choice—it "[m]ad[e] a process more difficult than it need[ed] to be, with the intent of dissuading certain action(s)." I also assessed some of the stated motivations for the design change relating to increased "location attach rates" and increasing Google's advertising revenue, which may be inconsistent with the privacy and other objectives of the user. I also evaluated contemporaneous concerns raised by Google's Privacy Working Group concerning removal of the toggle from Quick Settings, and I noted that those concerns were inexplicably ignored or overruled. I used this approach for all other interfaces, task flows, and disclosures that I analyzed in my Opening Report. I also note that Google's four experts do not purport to disagree with me as to my assessment and evaluation of design criteria.

Dr. Ghose also argues that I "fail[ed] to establish[] that . . . the alleged deception occurred in connection with a sale or advertisement." (Ghose Report ¶ 13(c)(ii)). I understand that the State alleges Google's deceptive acts and practices are accomplishing "in connection with" the sale and advertising of (i) Android devices (that are pre-installed with Google's operating

[19] Content analysis is a common methodology used in the social sciences, and is defined as "the systematic, objective, quantitative analysis of message characteristics." Neuendorf, K. A. (2017). *The Content Analysis Guidebook* (2nd Ed.). Sage. Content analysis has also been used to support primarily qualitative investigations of message characteristics as well; for instance, Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687.

[20] See a detailed treatment of this argumentation process in Gray et al. 2021 *Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective.*

system, as well as the Google Play Store, apps and services), and (ii) other Google services. I understand that this exchange of non-monetary compensation can be a "sale" under the relevant statute, and that the sale need not be from Google directly.

I also understand that another expert (Dr. Seth Nielson) has already explained how the accused conduct is "in connection with" the State's theories. For example, Dr. Nielson previously explained that "when a consumer purchases an Android device, he or she receives a device that has been configured to provide Google with ability to collect, store, and exploit a user's location information through the software on the device." (11/16/2021 Nielson Decl. ¶ 29). Similarly, Dr. Nielson also explained that various locations services "are pre-installed on a vast majority of all Android phones sold in the U.S." (11/16/2021 Nielson Decl. ¶ 51). "When purchasing an Android phone, a consumer in Arizona gets a device that Google can use to track his or her location. Google obtains that information through various settings, such as WAA, WiFi scanning, and others, which are built into Google's Android operating system that is pre-installed on Android phones." (11/16/2021 Nielson Decl. ¶ 84). Dr. Nielson explained that device-level settings (like the device location setting that Google moved from its QS menu) "are specific to a given hardware device." (11/16/2021 Nielson Decl. ¶ 57). Dr. Nielson further explained how account-level settings like LH and WAA are set for a device when purchasing it—either by signing into an existing account or creating a new one. (11/16/2021 Nielson Decl. ¶ 66). "When purchasing an Android phone, a consumer in Arizona gets a device that Google can use to track his or her location. Google obtains that information through various settings, such as WAA, WiFi scanning, and others, which are built into Google's Android operating system that is pre-installed on Android phones." (11/16/2021 Nielson Decl. ¶ 66). Further, whether on Android or other operating systems, Dr. Nielson explained that through Google's IPGeo and [redacted] services, "nearly all transactions with Google products or services become an opportunity for Google to collect and exploit the user's location information—even if the user has disabled the location related settings." (11/16/2021 Nielson Decl. ¶ 34). "Despite the various settings, there is nothing a user can do to prevent Google from using location information collected from IP address location for purposes of serving ads." (11/16/2021 Nielson Decl. ¶ 66).

The dark patterns I have analyzed are part of the user experience that Google has designed and pre-installed into the products and services it provides, including the Android operating system, the pre-installed and downloaded apps, the settings that are on the device itself or the account, the centralized processors that collect information from the settings, as well as the IP-address related information that Google collects through all of its transactions.

A. User Heterogeneity is Not Responsive to My Report

Drs. Hoffman and Ghose both assert that my methodology ignores heterogeneity in user privacy expectations and preferences. (*E.g.,* Ghose Report ¶¶ 14, 22; Hoffman Report ¶¶ 56, 58, 70). They are incorrect. My opinions are agnostic to the particular type of user that is doing the interfacing. All users must access the same limited choice architecture to make decisions about their personal data. To put it in Dr. Ghose's terms, Google's user interface stays the same regardless of whether a user is a "privacy fundamentalist" or a "privacy pragmatist." (Ghose

Report ¶ 14). Google's incorporation of dark patterns into a wide range of settings relating to location impacts all of those use cases, even if the way it affects a "fundamentalist" user might be distinct from how it affects a "pragmatist" user.

I also understand that the jury must assess unfairness and deceptiveness from the perspective of "the least sophisticated consumer," although I am advised Google argues that a "reasonable consumer" perspective should apply. I understand from counsel the Arizona Consumer Fraud Act declares that deceptive or unfair practices are "unlawful practices," that they expressly provide that the practice is unlawful "whether or not any person has in fact been misled, deceived or damaged thereby." A.R.S. § 44-1522(A). I did not (need not) assume a "monolithic" user, and the practices Google has engaged in do not become legitimate even if (as Google suggests) there may be subgroups of consumers who care less about these issues.

These arguments also show that Drs. Hoffman and Ghose are unfamiliar with the fields of both dark patterns and UX design more broadly. In work guided by user-centered design principles, it is important to identify relevant user goals, contexts of use, and user mental models that relate to goals and outcomes—recognizing that these elements are all plural and appear in complex combinations.[21] My analysis makes no assumption that users are homogenous or monolithic. My focus is on the choice architecture with which the user can interface, and how the stakeholder/designer (here, Google and its engineers) controls those settings to manipulate users.

B. There is a Strong "Causal Link" Between Dark Patterns and User Behavior

Next, Drs. Ghose and Steckel assert that there is no "causal link between Google's user interface (UI) and consumers' resulting behavior." (Steckel Report ¶ 18; *see also* Ghose Report ¶ 72).

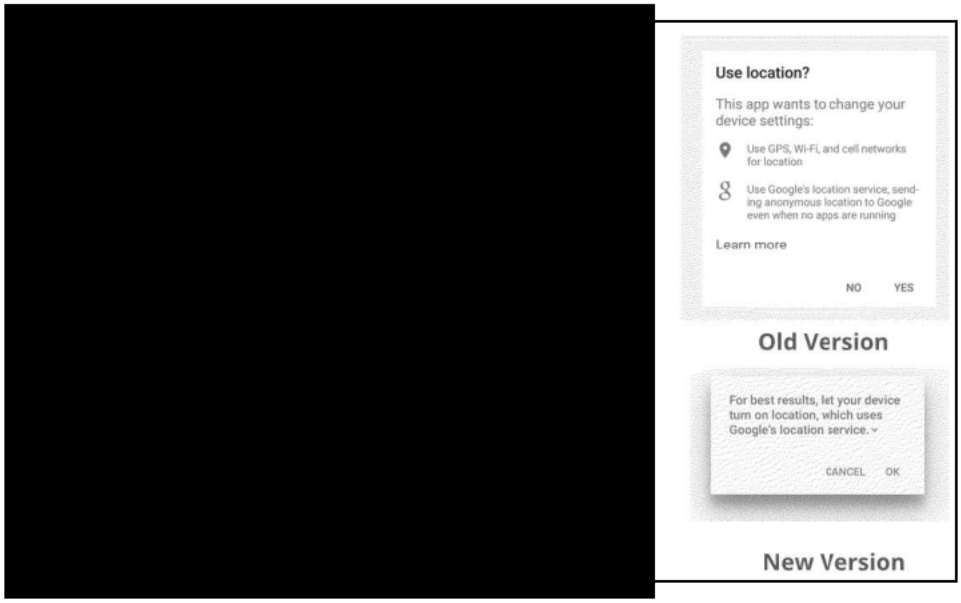
First, as I noted above, the Arizona Consumer Fraud Act does not require evidence that any consumer has been misled or deceived.

Second, as I highlighted in my Opening Report, extensive evidence shows the importance of these dark patterns, how they are deceptive, and even how they deceived user**s** and affected their behavior.

For example, Google's own engineers and designers acknowledged that their design decisions affect user behavior, including by misleading, confusing, and deceiving users. Following the AP Article, Googlers expressed their confusion internally: "Although I know it works and what the difference between 'Location' and 'Location History' is, I did not know that Web and App activity had anything to do with location" and "Add me to the list of Googlers who didn't understand how this worked an [sic] was surprised when I read the article." (GOOG-GLAZ-00001288 at 289, 290). In other contexts, Googlers have acknowledged that Android settings can create [redacted] (GOOG-GLAZ-

[21] The foundational text in the HCI and UX space that addresses these issues is Norman, D. (2013). *The Design of Everyday Things: Revised and Expanded Edition*. Basic Books.

00057339 at 340) and [redacted]
[redacted]
(GOOG-GLAZ-00117506 at 506). And Google engineers expressly credited their changes to Google's location prompting as the cause of [redacted] as shown below:



(GOOG-GLAZ-00029585 at 595). I cited significant internal evidence at length in my Opening Report, but it seems that Google's experts simply dismiss it as "anecdotal."

As another example, my Opening Report discussed the statistically significant effect of [redacted] (Opening Report pp. 29–31). Contemporaneous documents show that Google itself observed [redacted] (GOOG-GLAZ-00032447 at 450; *see also* GOOG-GLAZ-00028327 [redacted] Drs. Steckel and Ghose are silent on this point.

As yet another example, following the AP Article's revelation that WAA also controlled the collection of user location data, Google observed a massive increase in the number of users changing their location-related settings. Specifically, [redacted] (GOOG-GLAZ-00001458 at 464-66).[22] Following the AP Article, Google recorded a near cacophony of

[22] Dr. Hoffman attempts to dismiss these figures, arguing that only "approximately 0.06 percent or less of Google accounts turned LH off" and "approximately 0.14 percent or less Google accounts turned WAA off in each of the three days following the AP Article." (Hoffman Report ¶ 113). As Dr. Hoffman notes, these percentages relate to *all* Google accounts, irrespective of whether or not the owners of those accounts even saw the AP Article. Further, many of those

negative reaction, with users, designers, and commentators alike stating expressly that they had been misled. (*E.g.,* GOOG-GLAZ-00001253 at 54-57; GOOG-GLAZ-00001458.R at 70.R-71.R). Senator Blumenthal tweeted that "[i]t should be simple—'off' means 'off,'"[23] and Alan Butler from the Electronic Privacy Information Center noted that the statement "seem[ed] like textbook deception to [him]."[24] Again, Drs. Steckel and Ghose have no response.

C. Google's User Studies and Engineers' Statements are Reliable

Ironically, Google's expert Dr. Steckel spends a significant portion of his report attacking Google's own user studies, arguing that they "provide very little, if any, information on the methodology used, sample recruitment, and generalizability." (Steckel Report ¶ 27). For example, Google's expert castigates Google's "think aloud" studies, asserting that they do not use "a scientifically rigorous method of drawing valid conclusions about consumer perceptions or behaviors across a population." (*Id.* ¶ 28).

Despite the supposed flaws that Dr. Steckel highlights, Google itself thinks that these studies are sufficient to inform its design decisions and future research.[25] For example, Google's Privacy Working Group [redacted] (GOOG-GLAZ-00026360 at 361). Similarly, Google considered merging its device-level Location Reporting and account-level Location History settings [redacted] like the ones cited in my Opening Report. (*E.g.*, GOOG-GLAZ-00032376.R at 77 [redacted] Importantly, neither Dr. Steckel nor any of Google's other experts attempt to controvert the results of the Google studies I cited, nor do they point to studies that suggest differing conclusions.

Dr. Steckel also criticizes Google and its studies due to their low sample size. However, as Google's UX designers and researchers clearly understand based on their pattern of planning, conducting, and reporting on research studies, it is well known that small scale studies, including studies in which N < 10, have significant value for informing product design decisions. A reliance on small, largely qualitative, studies is at the root of usability evaluation best practices, with qualitative work framed as essential for providing a conceptually-appropriate foundation for

---

accounts could be inactive, belong to non-English speakers, or belong to the same user. Put another way, she's not measuring the number of people who were deceived but rather the number of people who received some of the truth via the AP Article, which she shows is very small. Regardless, Google itself noted that the increases were "[redacted] GOOG-GLAZ-00001458.R at 65.R.

[23] https://twitter.com/SenBlumenthal/status/1029407493544390656

[24] https://www.wired.com/story/google-location-tracking-turn-off/

[25] Dr. Steckel acknowledges that these studies were "aimed at improving Google's offerings," contradicting his other statements that such studies are unreliable. (Steckel Report ¶ 32); *see also* September 3, 2021 Deposition of Gretchen Gelke, at 73:2-75:3, 103:1-105:17.

larger-scale quantitative inquiry.[26] These smaller studies facilitate more in-depth qualitative investigation as compared to generic non-contextual survey studies such as the one that Dr. Steckel employed. For instance, Jakob Nielsen, a leading expert on web usability and co-founder of the Nielsen Norman Group, advocates for testing a product with no more than five users at a time, since those five users will aid in identifying 85% of the usability problems.[27] I assume Dr. Steckel is unfamiliar with this research on appropriate uses of qualitative and mixed methods to support UX and UI design, as he is not in the relevant field.

Similarly, Drs. Steckel, Ghose, and Hoffmann disregard extensive *qualitative* statements from Google's own engineers and product designers, arguing merely those statements are "anecdotal" and cannot be generalized. (*E.g.,* Ghose Report ¶ 80). Google's experts do not engage with the substance of its engineers' opinions or attempt to controvert them.

V. Google's Experts' Opinions About "User Value" Are Misleading and Rely on Unfounded Assumptions

Both Dr. Ghose and Dr. Hoffman essentially opine that Google's dark patterns and related practices should be tolerated because they offer users purported value from location-related services and personalization. (*e.g.,* Ghose Report ¶¶ 34-42; Hoffman Report ¶ 57). They unfortunately apply the wrong framework and thereby offer a false choice. Google's experts do not offer any analysis as to why the dark patterns I have highlighted are necessary for users to realize these supposed benefits. For example, Dr. Ghose offers no opinion that forced action or obstruction are necessary to deliver "tailored customer experiences." (Ghose Report ¶ 35).

When discussing the purported benefits, Drs. Ghose and Hoffman focus on the wrong conduct. The question is not simply whether "targeted advertisements and personalization" benefit users in an abstract sense, apart from specific designed interfaces and disclosures. Rather, Google should not use dark patterns or deceptive conduct in order to obtain non-meaningful consent from users or in their everyday use of systems that include personalization or targeted advertisements. Drs. Ghose and Hoffman do not articulate any benefits emanating from the dark patterns or deceptive conduct employed by Google. Nor do they suggest that there is any user value provided via the illusion of choice, obstruction, or forced action that Google applies in many of their interfaces. Similarly, hiding settings or burying disclosures or the other

[26] Numerous methods texts directed towards designers advocate for the value of qualitative methods and small-scale studies to identify the complexity of user needs, goals, mental models, and motivations. *E.g.,* Nunnally, B., & Farkas, D. (2016). *UX Research: Practical Techniques for Designing Better Products*. "O'Reilly Media, Inc." Ladner, S. (2019). *Mixed Methods: A Short Guide to Applied Mixed Methods Research*. Muratovski, G. (2015). *Research for Designers: A Guide to Methods and Practice*. SAGE. Young, I. (2008). *Mental Models: Aligning Design Strategy with Human Behavior*. Rosenfeld Media.

[27] https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/, guidance based on the following research article: Nielsen, J., & Landauer, T. K. (1993). A mathematical model of the finding of usability problems. *Proceedings of the INTERACT '93 and CHI '93 Conference on Human Factors in Computing Systems*, 206–213. https://doi.org/10.1145/169059.169166

behavior discussed in my report is not associated with any "value" identified by Google's expert. If Google's services are as valuable and desired by users as it says, then users would be willing to share their data even if they are given a real choice over how and when their data is shared, tracked, stored, or exploited.

For example, a user can get "value" out of a free trial for a service, but be surprised once the service starts automatically charging her credit card at the end of the trial. If that user valued the service enough to continue paying for it, it is reasonable to expect that she would be willing to pay if given an explicit and transparent opt-in after her free trial.

I discussed some of the other harms caused by Google's conduct in my Opening Report. I understand Dr. Jen King has also offered her opinions concerning some of these harms. I would add that deception is intrinsically harmful. Deceptive design practices can have aggregate and long-term impacts on users due to the eroding of user autonomy and undermining of freedom of choice that is often felt by users over a long period of time. For instance, a disclosure that is hidden or obscured or a user interface that employs dark patterns to prevent users from making a transparent choice regarding their location settings impacts not only their interactions and capture of location data in that discrete moment; by contrast, once these settings are in place, location data may be captured for months or years without the user's full knowledge, and the settings may only be sought out explicitly when media coverage like the AP Article brings specific tracking issues to their attention.

Ultimately, much of Google's experts' analysis of "user value" from location data is inapplicable. For example, Dr. Ghose variously states that "if the anticipated benefits of data sharing exceed the costs, a user is expected to willingly give his/her data away," (Ghose Report ¶ 24), "users are more willing to trade-off their privacy, including location data, for improved service quality or scope," (*id.* ¶ 27), and that "users are comfortable with the use of location data to generate more relevant ads and recognize the benefits associated with targeted and personalized content," (*id.* ¶ 43). Each of these statements presuppose that the user had the freedom to agree to such services in an informed manner, unencumbered by deceptive practices from the stakeholder. The insight that dark patterns offers is that such agreement is often obtained due to design practices that mislead and deceive users. To be sure, Dr. Ghose agrees that such transactions should be subject to informed decision-making by users, noting that "people are beginning to demand a fair exchange for their data and want to negotiate the terms with brands to mutual advantage," and that users' data should be subject to a "give-and-take between customers and businesses."[28]

[28] Anindya Ghose (2017) "When push comes to shove, how quickly will you give up your data for convenience?" *Quartz*, https://qz.com/973578/data-privacy-doesnt-seem-to-be-a-concern-for-mobile-users-willing-to-swap-it-forconvenience/.

VI. Dr. Steckel's "WAA Study" Is Methodologically Flawed and Does Not Rebut My Opening Report

Dr. Steckel's survey is limited in scope and lacks ecological validity with relevance to the specific user interfaces at issue in this case. As explained below, Dr. Steckel essentially ran the same study with two groups and announces that he received the same results in both groups.

As an initial matter, Dr. Steckel does not test what is at issue in this case, nor the theories presented in my report. His study merely asked people if they would change particular settings given access to the contents of a help page, not if they ***understood*** or ***comprehended*** what those settings did or whether those settings mapped to their desired level of location tracking. Further, the help pages displayed to survey participants presumed that a user would typically view a corresponding help page (for a full 30 seconds) when making their decision to set or change their WAA settings—an action which would be difficult for a majority of users given that the help page would need to be searched for and accessed separately by the user (clicking a related "Learn more" link in the WAA settings panel or account setup flow appears to only produce a pop-up with more information and not the entire help page).

Second, Dr. Steckel used the wrong independent variable when constructing the survey study. He only made one change between the two flows that he presented in the survey—a change to the contents of the Location History help page, deleting the statement that "[w]ith Location History off, the places you go are no longer stored." (Steckel Report at D-13). Dr. Steckel did not correct the omission of a disclosure that WAA collects location data—in fact, no participants were presented with a disclosure informing them that WAA saved location data.

Put another way, the AP Article did not simply point out that Google stated "[w]ith Location History off, the places you go are no longer stored." Instead, it revealed that the statement ***was false*** because WAA also collected location data. Here, by contrast, users would have no reason to be skeptical of the statement that "with Location History off, the places you go are no longer stored" because there is no way for them to know that it is false. Accordingly, this study is simply inapplicable to the theories that I have presented.

Third, Dr. Steckel did not present any context to survey participants. For example, when presented with the help center pages, users were not provided with any information as to *why* they were reviewing these pages or what they were looking for. Dr. Steckel also did not inform survey participants that the goal of the study was to assess their preferences for location data collection based on Google's disclosures, and he did not inform them that the study was supposed to determine whether they were confused about the functions of Google's products based on their disclosures. This seems to run counter to the criticisms from Drs. Hoffman and Ghose that my methodology ignores user heterogeneity relating to users' expectations of privacy as it relates to location tracking. In contrast, Dr. Steckel's survey study—while creating a sample balanced to the US Census by age, sex, and region—does not address the diversity of user types and motivations as raised by other expert reports.

This point is particularly salient as it relates to the factually false statement on the Location History page. Users who would have seen that false disclosure are those users who

would have specifically searched for it and would have had a context as to what information they were seeking. The users in Dr. Steckel's study are not provided that sort of motivation or context. Of course, the claims here are also not limited only to the false Location History disclosure or those users who reached it.

Fourth, it appears that Dr. Steckel failed to provide important data that his survey would (or should) have generated. For example, he presents statistics regarding user engagement with the WAA and LH toggles, but does not present any results concerning user engagement with all ***other*** toggles. If the engagement rate as to those toggles was the same as the rate for the other toggles, it would further undermine his conclusions because it would suggest that the results are all noise. As another example, Dr. Steckel provided thumbnails on the last page of the survey, but failed to provide any numbers concerning how many users actually opened those thumbnails when deciding which settings to toggle.

Fifth, the key disclosures that Dr. Steckel purports to be testing are entirely illegible. I understand that both experimental groups received the stimuli at pages G-3 through G-5, and these stimuli appear perfectly legible. In contrast, the print is very difficult to read in the stimuli that were provided to the different groups (G-1 versus G-2). Even though I know what to look for, since I have reviewed other versions of these materials as part of my analysis work, I find it difficult to locate the relevant language. I understand Dr. Steckel has refused to provide a link to the study itself as the users saw it, so it's impossible for me to assess exactly what the users saw themselves. It is also impossible to know what additional questions Dr. Steckel asked that may not have been reported.

Sixth, this study is a hypothetical. Real-world data suggest the opposite conclusion—as noted, when users were informed in a way they understood that WAA surreptitiously collects location data despite statements that LH is the only relevant toggle, they tended to turn it off.

The lack of control over potential confounds in the sample, alongside other issues of ecological validity raised above, constitutes a series of major methodological flaws and leads any study conclusions to be unreliable. Further, it fails to consider (much less provide meaningful experimental evidence regarding) the various allegations in the case. Even as it relates to the LH and WAA settings relevant to this case, Dr. Steckel's survey does not afford any avenue for the two groups to express whether they have been misled or whether the deception has been corrected. For example, apart from an illegible, cryptic, and buried statement in the middle of G-2, neither group was informed that Google tracks their location through WAA.

Dr. Steckel's survey is not the type of research design that would be used to describe how users understand or are misled by Google's maze of settings and disclosures that are impacted by the use of dark patterns. Google's real-world studies that I cite in my analysis are much more helpful in that regard—which is why a company with Google's resources uses those studies.

VII. Dr. Hoffmann's Criticisms Are Unfounded and her "UI Analysis" Is Invalid

Painting in broad strokes, Dr. Hoffman asserts that my analysis is "contrived and not representative of actual user behavior," and that "[r]eal users would not be likely to interact with

the UI in the artificial manner Dr. Gray presents." (Hoffman Report ¶ 90). She cites nothing for these propositions, and, as noted, does not claim the necessary expertise in UX design to make these claims.[29]

Dr. Hoffman does not engage in a "UI Analysis," as that phrase would be understood by an HCI researcher or UX practitioner. A UI-focused analysis would typically be grounded in the user interface itself, using evaluation methods such as a heuristic analysis,[30] task flow analysis,[31] or cognitive walkthrough.[32] Instead, Dr. Hoffman simply marches through various Google pages—many disconnected from screens that contain dark patterns identified in my Opening Report—pointing out that users can get to those pages if they click on the right things and that the pages contain certain disclosures. She does not engage in a content or artifact analysis of the user interface, which involves deconstructing the relevant UI components, identifying their potential interactive relationships with each other, and how these elements contribute to a user's perception of the choice architecture. She rarely addresses any specific UI elements that I raised in my Opening Report which I have shown to contribute to a problematic choice architecture. She also disregards real-world evidence (including from Google employees and studies) emphasizing that Google's design interfaces are misleading and deceptive. As set forth below, her analysis does not rebut my conclusions in my Opening Report.

A. Task Flows

Building on her point regarding the heterogeneity of user types and motivations, Dr. Hoffman states that "users vary in terms of their . . . particular navigational goals at any one point in time," and that I assume "that there is a single task flow . . . that can be applied to all users." (Hoffman Report ¶ 116). For example, she claims that my analysis of the task flow to access WAA (Appx. 3 to my Opening Report) "ignores the multitude of other situations that could lead a user to that screen," and claims that there are "many entry points and paths by which any given user can access information to make informed decisions regarding how much information they are willing to share with Google for what purposes." (*Id.* ¶ 117).

While Dr. Hoffman purports to characterize these other unspecified "entry points and paths," she does not actually identify any or specifically highlight how they disprove my analysis—she just says they exist. Her only support for the supposed differences in these unspecified task flows and entry points is her conversations with Mr. David Monsees and a current (*i.e.*, not representative of the entire relevant time period) website, safety.google.com, and even then she does not isolate any specific task flows that materially differ from my analysis. (*Id.* ¶ 117 n.153, n.154). Instead, she points to snapshots of single pages in relevant task flows, such as an undated WAA settings page (*id.* ¶ 122), a My Activity page from June 2022 (*id.* ¶ 124), and an undated popup screen that appears when a user toggles WAA off, then on again (*id.*

[29] Such statements also contradict Dr. Hoffman's earlier statements that user behavior is not "monolithic." (*E.g.,* Hoffman Report ¶ 115).
[30] https://methods.18f.gov/discover/heuristic-evaluation/
[31] https://methods.18f.gov/decide/task-flow-analysis/
[32] https://methods.18f.gov/discover/cognitive-walkthrough/

¶ 128). She fails to analyze ***how*** and ***in what interactive contexts*** users would get to these screens or settings in the user experience, and assumes that because some information is available is upon tapping "Learn more" or "MANAGE ACTIVITY," the interface cannot deceive or mislead. Even during the time period when these disclosures were posted—and even for those users who would have reached these disclosures—Dr. Hoffman ignores that disclosures and interfaces can be technically truthful but still have the capacity to mislead and deceive. Further, Dr. Hoffman only "analyzes" ***two*** specific task flows—Google's Android Account Setup flow and a flow from Android Settings to Google's Help Center content—and even then, Dr. Hoffman simply states that they are "good" examples of progressive disclosure. Each of these flows are discussed in detail in Section VII(B) below.

Though Dr. Hoffman questions their applicability, the task flows that I identified in my Opening Report are highly relevant. Appendix 3 to my Opening Report, for example, depicts the flow from the "Personal info & privacy" Android settings page, to activity controls, to Web & App Activity, and finally to the disclosures users would see when toggling WAA on and off.[33] This is a key pathway and set of clicks that would be needed for a user to enable or disable WAA, and Dr. Hoffman does not provide any reason to think otherwise. Where Dr. Hoffman identifies specific flows or pathways that she believes are materially different from those that I analyzed in my Opening Report, I address them here.[34]

Similarly, Appendix 4 to my Opening Report depicts the Google Account setup flow that a user would experience when setting up a new Android device, including Google's Privacy & Terms page and its disclosures concerning Location History and Web & App Activity.[35] Dr. Hoffman does not seriously contest that this is a representative task flow, nor does she identify important task flows that she believes are materially different as it relates to my analysis.

B. Progressive Disclosure

While Dr. Hoffman spends a significant amount of time engaging in her "UI Analysis," her basic point is straightforward—Google incorporates "progressive disclosure," providing a purportedly "well lit path." (Hoffman Report ¶ 62). Even if correct, the use of progressive disclosure does not mean that the disclosure is intrinsically honest or sincere. Nor does it rebut the existence of dark patterns used in elements that are part of the progressive disclosure design strategy. For example, in my scholarly work I have described how stakeholders can "us[e] progressive disclosure to hide aspects of the service and its monetary impact," including by

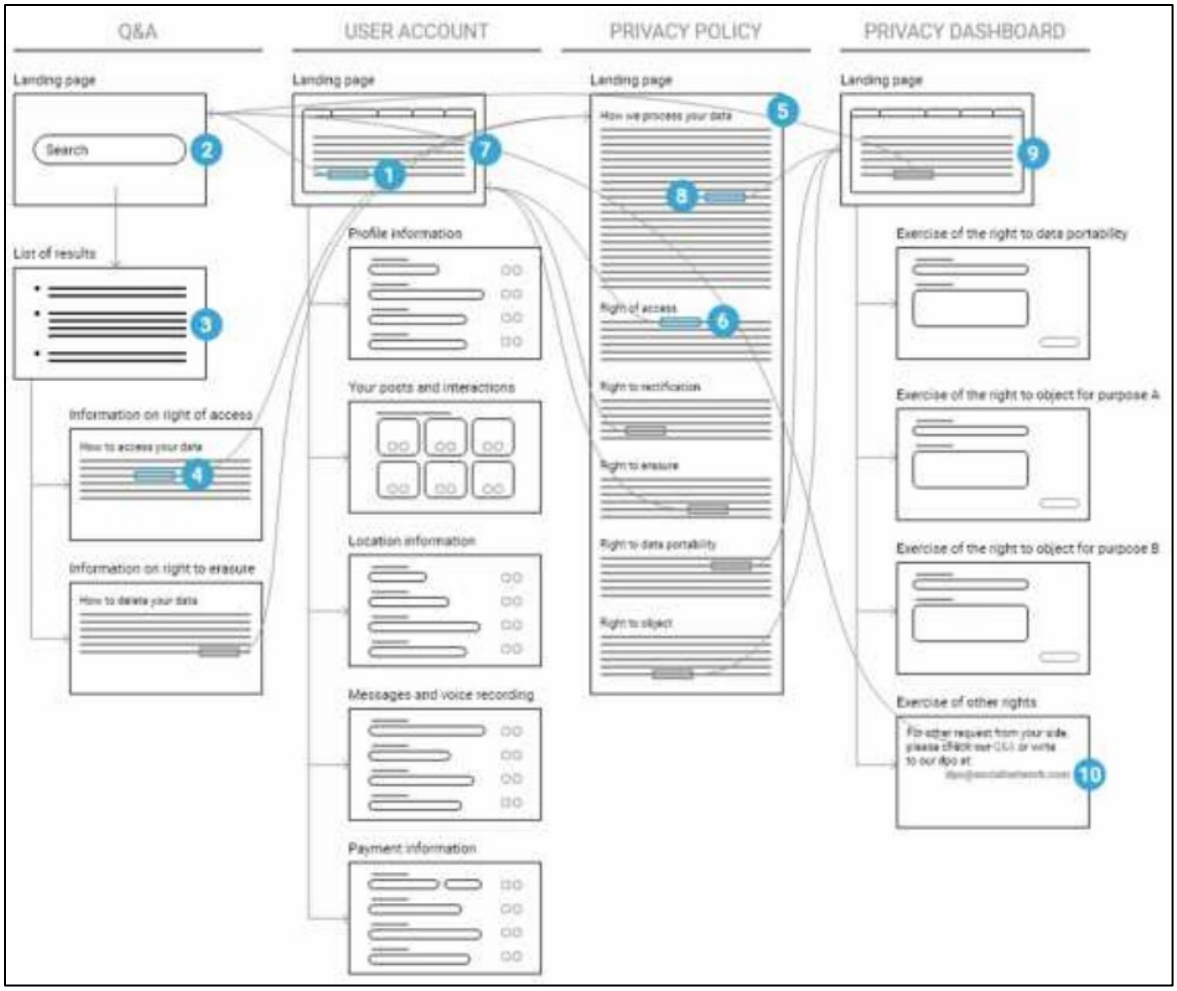
[33] Based on the Australian court documents (GOOG-GLAZ-00299199), these screens were visible to users between 2017 and 2018.
[34] I focused my analysis on the versions and pathways produced by Google, which I understood were intended to be representative. Obviously, I understand that Google can make changes to various interfaces and introduce new ones, but I would expect Google and its experts to identify ones they believe to be materially different from the representative ones Google produced.
[35] Based on the Australian court documents (GOOG-GLAZ-00299199), these screens were current between 2018 and 2019.

burying the true cost of a service behind multiple pages that the user would have to "progress" through to find out.[36]

As an example of Google's use of "progressive disclosure," Dr. Hoffman walks through a Google "Privacy and Terms" flow that a user would see "when setting up their devices" in around 2017. (Hoffman Report pp. 32–34). Instead of engaging in an analysis of how a user would interface with such a flow, Dr. Hoffman summarily concludes (or perhaps, assumes) that because some information is available behind hyperlinks, users will be able to clearly proceed through such a flow, understand the relevant information, and then get to the relevant page to modify their settings. By contrast, as I have shown in the task flows in my opening report, the sheer number of screens and settings make it unlikely that a user would click on these hyperlinked disclosures unless they already suspected that their choice architecture was being actively modified by Google.

From the perspective of an analysis of dark patterns, however, this flow presents serious problems. For example, the EDPB identifies a dark pattern it calls the "privacy maze," in which users "have to navigate through many pages without having a comprehensive and exhaustive overview available." (EDPB, "Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them," 26 ¶ 73 (Mar. 14, 2022)).[37] The Board provides a graphical illustration, as set forth below:

[36] Gray, Colin M., Shruthi Sai Chivukula, and Ahreum Lee. 2020. "What Kind of Work Do 'Asshole Designers' Create? Describing Properties of Ethical Concern on Reddit." In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, 61–73. DIS '20. New York, NY, USA: Association for Computing Machinery.
[37] https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf



Id. at 50. In terms of the typology identified in my Opening Report, this strategy is a form of ***obstruction***, in that it makes the process of navigating and controlling settings more difficult and overwhelming, and ***interface interference***, in that it manipulates the user interface by presenting too many options to the user, overloading them with options and places to go. As with other dark patterns that I have identified, here the stakeholder can provide information that is technically correct, but presented to the user in such a manner as to mislead or significantly undermine comprehension.

The specific task flow presented by Dr. Hoffman at pp. 32–34 presents users with such a privacy maze. The first page (on p. 32) mentions that "[w]hen you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including . . . location." A user seeking to learn more must then tap the hyperlink for "Privacy Policy," which takes them to a page containing yet more hyperlinks (p. 33). A user must then tap the "key terms" hyperlink to determine how Google gets location info—but there is nothing around that hyperlink that indicates it would provide any information about location data. If the user does tap "key terms," the user is taken to another page that discusses, among other things, location information (p. 34). The statement about location information on that page has three further hyperlinks contained within it.

Importantly, it appears that nothing in this flow includes (or at the very least clearly indicates) a link to a page where users could ***actually control*** some of Google's data collection, such as Activity Controls. To do so, they would have to navigate elsewhere, and it is unclear where they should go based on this flow. Instead, "users are buried under a mass of information, spread across several places" and under various hyperlinks. (EDPB, "Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them," at 55 ¶ 162 (Mar. 14, 2022); *see also* Fed. Trade Comm'n, "FTC Looks to Modernize Its Guidance on Preventing Digital Deception,"[38] Jun. 6, 2022 (rejecting the claim that firms "can avoid liability under the FTC Act by burying disclosures behind hyperlinks . . . ."). Instead of a "well lit path," Google users must navigate a labyrinth of pages and hyperlinks, with relevant information either buried in the mess or not provided at all.

The inapplicability of Dr. Hoffman's opinions is evident in the context of the particular dark patterns I identified in my Opening Report. As just one example, Dr. Hoffman offers no real analysis concerning the importance of setting defaults, such as Google's use of the Web & Activity to collect location by default. She likewise does not dispute that, in many instances described in my Opening Report, Google did not provide disclosures, progressive or otherwise.[39] Progressive disclosures are also inapplicable to the forced actions I describe, such as the lack of opt-outs for IPGeo and [redacted]. Progressive disclosures are also of no consequence when it comes to Google deliberately hiding or de-emphasizing settings using interface interference-related dark patterns (like the removal of the location master in Quick Settings). Nor is it relevant to my discussion of dark patterns that manipulate users into enabling settings (such LH) when prompted by Google for use of a particular service that does not actually require that setting. In short, her "progressive disclosure" discussion finds little application as it relates to the opinions I have offered and the deceptive conduct I identified.

Dr. Hoffman also points to an updated version of the "Location information" page within Google's privacy policy (p. 36). The same problems are evident—after getting to this portion of the policy, users are presented with five more hyperlinks to navigate through. Further, though the updated version appears to give users links to places to control their location information, the disclosure is *misleading*—it omits any reference to Web and App Activity. Thus, what Dr. Hoffman describes as the "numerous branching points" offered by Google's design, (Hoffman Report ¶ 119) results in users being "likely to give up or miss the relevant information or

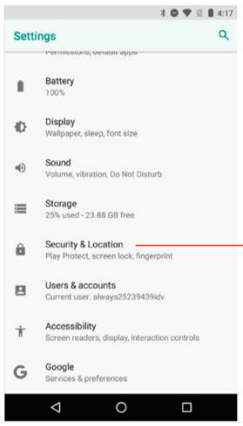
[38] https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-looks-modernize-its-guidance-preventing-digital-deception

[39] For example, until mid-2018, Google did not disclose any relationship between WAA and location, such that "progressive disclosure" would be irrelevant. (Monsees 7/12/2019 EUO Tr. at 175:7-15, 373:18-374:13). She does not dispute that, until Android Q, an Android user could not directly access the WAA setting on their phone—disclosures or not. (*Id.* at 164:16-166:19). Dr. Hoffman likewise does not dispute that, even after that changed in mid-2018, users would have had to click on "Learn More" to view such a disclosure until at least 2018 (*id*. at 373:18-374:13, 376:15-377:3), or that users who had set up an account before 2018 would never receive such a disclosure even as they continued to use new devices (*id.* at 381:1-23).

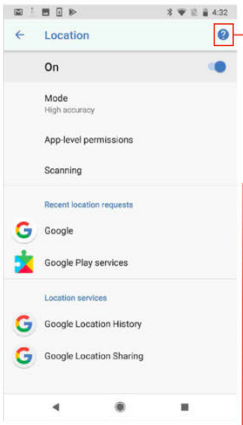
control." (EDPB, "Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them," at 60 (Mar. 14, 2022).

As another example, Dr. Hoffman presents a task flow beginning with Android Settings and terminating in the location master toggle or Google's Help Center content (Hoffman Report ¶¶ 160–64). I have attempted to recreate this flow below—the screenshots appear in the documents from the Australian lawsuit, and it appears that Dr. Hoffman may have omitted some of the relevant points in the task flow.

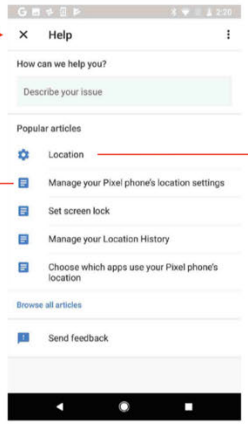
As an initial matter, this flow does not contain any point at which a user would be able to manage WAA, or even learn that WAA relates to location tracking. Instead, the flow suggests that *the opposite* is true—by purporting to provide all location related toggles and settings, Google implies that other settings have nothing to do with location data collection at all. More fundamentally, however, this again presents the problem of the "privacy maze"—the user must navigate through a set of extended interfaces with numerous toggles and other exit points (including seemingly recursive pathways), ultimately landing on a wall of text that itself includes hyperlinks to other locations. (*See also* Hoffman Report ¶ 164 (including image of updated "Turn location on or off for your device" with numerous hyperlinks to various locations)).



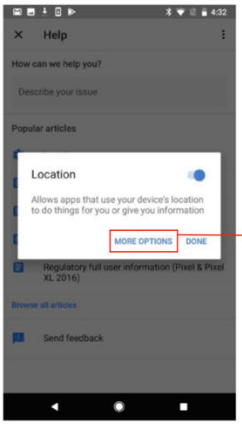
GOOG-GLAZ-00299282



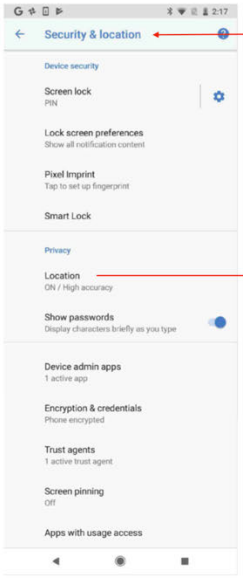
GOOG-GLAZ-00299292



GOOG-GLAZ-00299293



GOOG-GLAZ-00299294



GOOG-GLAZ-00299290-291

Turn location on or off for your device

You can turn location mode on or off completely for your device. You can also change only your device's location accuracy mode. Each mode uses different sources to estimate your device's location.

When location is turned on for your device, Google can use your Location History to get useful information – like automatic commute predictions or better search results – based on the places that you've been with your Android device.

Change your location mode

Choose your location mode based on:

- How accurate you want the location estimate to be
- How long it takes to determine your location
- How much battery power location services uses

If you turn off location completely for your device, then no apps (neither Google nor non-Google apps) can use your device location. Many useful features will be turned off.

Turn location on or off for your device

1. Open your phone's Settings app.
2. Under "Personal", tap **Location**.
3. At the top, tap the **On/Off** switch.
   - **Off**
     Your device location isn't shared with any apps.
   - **On**
     Choose your mode:
     - **High accuracy**
       High accuracy mode uses GPS, Wi-Fi, cellular networks, and other sensors to get the highest-accuracy location for your device. It uses Google's location service to help estimate your location faster and more accurately.
     - **Battery saving**
       Battery saving mode estimates your location using low battery-intensive location sources, like Wi-Fi and cellular networks. It uses Google's location service to help estimate your location faster and more accurately.
     - **Device only**

Device only mode estimates your location using GPS only. It doesn't use Google's location service to provide location information. This mode may use more battery power and take longer to determine your location.

When an app is using your device's precise location, the top of your screen shows Location. This icon doesn't necessarily mean that there's GPS activity. Rather, it means that a mode using more power to determine your location is turned on.

Tip: Location is a Quick Setting.

Related links

- Manage location settings for apps
- Manage & delete your Location History
- Find & improve your location's accuracy in Google Maps

GOOG-GLAZ-00299455-56

C. AP Article

Dr. Hoffman next asserts that the AP Article "[o]versimplifies" Google's disclosures and "fails to appreciate" the complexity of Google's location technologies. (Hoffman Report p. 40, ¶ 97). In truth, the issues that the AP investigated are not complicated—Google told users that turning off Location History prevented their locations from being stored, and that statement was false. (7/11/2019 McGriff EUO Tr. at 139:13–17). Importantly, Dr. Hoffman does not suggest that the statement "[w]ith Location History off, the places you go are no longer stored" is true. Even setting aside the expressly false disclosure, the AP article explains the inherent deceptiveness of offering users an opt-in setting called "Location History" while having a separate setting called "Web & App Activity" that is both on by default and collects users' location history. In fact, Dr. Hoffman fails to address the numerous statements even from Googlers themselves acknowledging they did not know WAA collected location data or that they were otherwise surprised by the AP's findings. (*See generally* Opening Report p. 18). If Google's own engineers and researchers were misled, it is hard to see how the least sophisticated reader wasn't.

Quoting Mr. Monsees, Dr. Hoffman asserts that the AP Article was incorrect "because the Web & App Activity setting does not collect any location information in the 'background.'" Dr. Hoffman and Mr. Monsees both neglect to mention that WAA tracks location data while users interact with Google products and services. To a user, this is easily interpreted as location collection in the "background," in the sense that they would not realize that whenever they interact with a Google service, their location information is stored.[40]

In a similarly narrow view, Dr. Hoffman claims that the specific page containing the statement "[w]ith Location History off, the places you go are no longer stored" "was intended to apply specifically to the Location History feature itself rather than be interpreted more broadly with respect to user location entirely." (Hoffman Report ¶ 107). But as Google employee Martin Callegaro notes, this is "[d]efinitely confusing from a user point of view if we need googlers [to] explain it to us." (GOOG-GLAZ-00001288 at 289; *see also* GOOG-GLAZ-00313060 at 63 ("the LH controls do not manage *all* location storage and a user might assume they do.")).

Dr. Hoffman also identifies a version of the "Privacy and Terms" interface that a user may see during Google Account Creation. (Hoffman Report pp. 57–62). Importantly, she does not identify ***when*** any of these disclosures were presented to users.[41] Further, the WAA disclosure that she identifies (on p. 61) omits any reference that WAA collects location data. She points to the "broad disclosure" that Google collects "location data" in the top-level Privacy and

[40] In fact, "Google started storing precise device-based location as part of Web & App Activity from users' interactions on Google Search and Google Maps in September of 2015." (Google's 9/4/2019 Response to DFI No. 25). I understand that Google continued storing precise location for WAA until 2019, when it reverted to coarsened location. (Monsees 7/12/2019 EUO Tr. at 186:7-13).

[41] For example, until as late as November 30, 2018, Google's Privacy & Terms webpage for location data page made no mention of WAA. (Ex. 297 at Ex. A 11-12).

Terms interface, but ignores the fact that this disclosure is unconnected to any particular setting (*e.g.,* LH, WAA, etc.), giving users no way of knowing how to control their location data.

Dr. Hoffman further opines that WAA's connection to location information collection should have been obvious to users, even though it was rarely (if at all) referenced in user-facing disclosures, because if users tap "MANAGE ACTIVITY," they will be able to view the location information that has been saved. (Hoffman Report ¶ 124). Dr. Hoffman ignores the fact that a user wishing to disable Google's location tracking would have no reason to get to "MANAGE ACTIVITY" because they would have no reason to know that WAA was connected to location data collection. For example, even as late as May 30, 2019, Google's WAA Help Center page simply failed to disclose that WAA recorded user location data even though it purports to explain "[w]hat these settings do." (GOOG-GLAZ-00000885 at 85–88; *see also* Google's 2/21/2020 CID Responses at 34–35 (explaining that GOOG-GLAZ-00000885 was part of a document production containing "new responsive Help Center materials currently available online" as of May 30, 2019)). Requiring that users go this deep into the interface to even find out that WAA saves their location data is a prime example of ***sneaking***, in that it buries information so deep that users are unlikely to discover it.

It bears noting that the AP Article only covers the limited subset of issues that were apparent to the journalists who authored it. For example, it seems that the AP reporters were unaware of Google's IPGeo and [redacted], whereby Google collects and stores user location even if both LH and WAA are disabled. The AP reporters were also not fully aware of how extensively Google uses location information collected from WAA and IPGeo. Apart from the dark patterns identified in my report, I understand Dr. Nielson identifies further ways in which Google collects location information, much of which Google has designated as confidential and was not available to the AP reporters. If anything, the AP story vastly underestimates the scope of the problem.

D. Google's Other Location Settings and Disclosures

After her discussion of the AP Article and WAA and LH, Dr. Hoffman proceeds to discuss the other location-related services, settings, and disclosures mentioned in my opening report, such as the QS Toggle, IPGeo, the Google Search Footer, and WiFi settings. However, most of Dr. Hoffman's analyses are not responsive to my opinions, merely stating Google's various forms of location collection were disclosed in general or through progressive disclosure, or are "consistent with good UI design principles." (*E.g.,* Hoffman Report ¶¶ 159, 175).

VIII. Dr. Arnold's Cursory Opinions Are Unsupported

As noted, Dr. Arnold seems to offer opinions concerning what Google *disclosed* to its users. (Arnold Report ¶¶ 45 (noting that Google's Privacy Policy discloses "that Google Display Network includes ads on third party sites or apps based on location data"), 59-60 (asserting that Google's Privacy Policy and search results page "disclose[] to users that IP address is a signal to obtain location information."). As far as I can tell, Dr. Arnold does not purport to have any background or expertise that would qualify him to make these assessments. Thus, is unsurprising that his assertions are devoid of any consideration of user task flows or

manipulation of information flow. For that matter, his assertions do not employ (and do not purport to employ) any methodology at all for evaluating these disclosures, except to say that he (a non-expert in the field) believes they are there. Further, Dr. Arnold exclusively cites to *current* versions of certain Google disclosures, while ignoring how those may have changed over time. (*See* Arnold Report ¶ 59 n.73).

Perhaps more importantly, Dr. Arnold's assertions do not contend with the opinions that I offer or the claims that the State has alleged here. For example, Google's location services go far beyond just using IP addresses for location. Google engineer Blake Lemoine (an engineer with responsibility for "user trust") explains that "the level of accuracy of our IPGeo system is far beyond anything achievable based solely on the location information inherent in IP addresses." (GOOG-GLAZ-00315032 at 34). He adds, [redacted] (GOOG-GLAZ-00234771 at 72). As just some examples of this, I understand [redacted] (Eriksson 9/13/2021 Tr. at 114:9-22, 79:4-24; Eriksson 10/5/2021 Tr. at 338:11-339:5). Dr. Nielson also explains that Google's [redacted] (Nielson Decl. ¶ 113).

Google has taken affirmative steps to *not* disclose how it uses IP addresses. As early as 2009, Google recognized that IPGeo was not merely part of the standard function of IP addresses, prefacing an internal presentation on the subject with:

> *You have no idea how incredibly confidential this one is. My my, is this confidential. I kid you not. Imagine an article titled "Google knows where you live, because it spies on you" in the NYT. You've been warned.*

(GOOG-GLAZ-00222226 at 28). Another Google engineer (Mr. Eriksson), when asked whether Google publicly discloses "the fact that it can use [redacted] to compute a user's location based on information reported by the reporters," responded "We say that we translate IP to location. We don't give the details." (Eriksson 10/5/2021 Tr. at 346:10-17). I also understand from counsel that Google has sought to keep all references to these services and their functionality in this litigation from the public, including just the high-level discussions quoted above.

Further, burying language (to the extent these are actually disclosed) in a privacy policy does not dispel either the existence of deception relating to the presence of dark patterns in Google's products. Not only does Google employ a maze of settings and disclosures (or a privacy maze), it also thereby creates the impression that a user could successfully prevent Google from tracking, storing, and exploiting their location data by clicking the right combination of settings. As it turns out, this is a false impression, given the *forced action* here that results in location data being tracked via IPGeo regardless of the settings they select. On

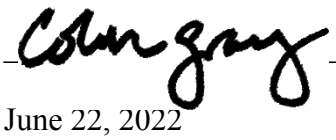
this issue, too, Google's own engineers confirm how this is deception. For example, Engineer Lemoine warns that Google is "deceiving users by telling them they can turn off location and then spending millions of dollars to infer their location through other means" and that "[t]he text of the 'device location' permission setting and other related permission settings can build an expectation in users' minds that if you turn those permissions off then Google will no longer know your location." (GOOG-GLAZ-00315032 at 34-35). Google's Chief Internet Evangelist, Vint Cerf, agrees that Mr. Lemoine made "a good point that we appear to be tracking even when users have turned off what they think and we imply are tracking mechanisms." (*Id.* at 33). Dr. Arnold does not refute these points and, as far as I can tell, neither do any of Google's other experts.

Google's current disclosure[42] concerning the use of location data on third party sites is similarly not a response to any of the State's claims or my opinions. The State alleges, and I have opined, that Google employs dark patterns and other deceptive and unfair practices to collect and store user location data, which is then exploited. Google's privacy-maze disclosures (even to the extent reached by users) does not remedy or eliminate any of those allegations. Put differently, Google's collection of location data is deceptive and unfair—and that remains true regardless of whether Google exploits that deceptively collected data on Google's own websites or on third party websites.

IX. Conclusion

I reserve the right to provide additional demonstratives (including those illustrating the account setup process, Help Center content, and other disclosures a user could navigate through) to be used at trial. I also reserve the right to supplement my opinions to the extent I am permitted to do so, including in response to any new information that I learn.

Colin M. Gray, PhD



June 22, 2022

[42] Dr. Arnold fails to acknowledge that there was no such disclosure in Google's Privacy Policy before May 2018. (*Compare* https://policies.google.com/privacy/archive/20171218 (December 2017 Privacy Policy) *with* https://policies.google.com/privacy/archive/20180525 (May 2018 Privacy Policy)).

Additional Production Documents Considered

GOOG-GLAZ-00032376.R
GOOG-GLAZ-00046988.R
GOOG-GLAZ-00073836.C
GOOG-GLAZ-00073891.R
GOOG-GLAZ-00086385
GOOG-GLAZ-00222226
GOOG-GLAZ-00101684
GOOG-GLAZ-00219004
GOOG-GLAZ-00217782
GOOG-GLAZ-00217783
GOOG-GLAZ-00217784
GOOG-GLAZ-00217785
GOOG-GLAZ-00217786
GOOG-GLAZ-00217787
GOOG-GLAZ-00217788
GOOG-GLAZ-00217789
GOOG-GLAZ-00217790
GOOG-GLAZ-00217791
GOOG-GLAZ-00217792
GOOG-GLAZ-00217793
GOOG-GLAZ-00217794
GOOG-GLAZ-00217795
GOOG-GLAZ-00217796
GOOG-GLAZ-00217797
GOOG-GLAZ-00217798
GOOG-GLAZ-00217799
GOOG-GLAZ-00217800
GOOG-GLAZ-00217801
GOOG-GLAZ-00217802
GOOG-GLAZ-00217803
GOOG-GLAZ-00217804
GOOG-GLAZ-00217805
GOOG-GLAZ-00217806
GOOG-GLAZ-00217807
GOOG-GLAZ-00217808
GOOG-GLAZ-00217809
GOOG-GLAZ-00217810
GOOG-GLAZ-00217811
GOOG-GLAZ-00217812
GOOG-GLAZ-00217813
GOOG-GLAZ-00217814
GOOG-GLAZ-00217815
GOOG-GLAZ-00218073
GOOG-GLAZ-00218074
GOOG-GLAZ-00218075
GOOG-GLAZ-00218076
GOOG-GLAZ-00218077
GOOG-GLAZ-00218078
GOOG-GLAZ-00218079
GOOG-GLAZ-00218080
GOOG-GLAZ-00218081
GOOG-GLAZ-00218082
GOOG-GLAZ-00218083
GOOG-GLAZ-00218084
GOOG-GLAZ-00218085
GOOG-GLAZ-00218086
GOOG-GLAZ-00218087
GOOG-GLAZ-00218088
GOOG-GLAZ-00218089
GOOG-GLAZ-00218090
GOOG-GLAZ-00218091
GOOG-GLAZ-00218092
GOOG-GLAZ-00218093
GOOG-GLAZ-00218094
GOOG-GLAZ-00218095
GOOG-GLAZ-00218096
GOOG-GLAZ-00218097
GOOG-GLAZ-00218098
GOOG-GLAZ-00218099
GOOG-GLAZ-00218100
GOOG-GLAZ-00218101
GOOG-GLAZ-00218102
GOOG-GLAZ-00218103
GOOG-GLAZ-00218104
GOOG-GLAZ-00218105
GOOG-GLAZ-00218106
GOOG-GLAZ-00218107
GOOG-GLAZ-00218108
GOOG-GLAZ-00218109
GOOG-GLAZ-00218110
GOOG-GLAZ-00218111
GOOG-GLAZ-00218112
GOOG-GLAZ-00218113
GOOG-GLAZ-00218114

GOOG-GLAZ-00217816
GOOG-GLAZ-00217817
GOOG-GLAZ-00217818
GOOG-GLAZ-00217819
GOOG-GLAZ-00217820
GOOG-GLAZ-00217821
GOOG-GLAZ-00217822
GOOG-GLAZ-00217823
GOOG-GLAZ-00217824
GOOG-GLAZ-00217825
GOOG-GLAZ-00217826
GOOG-GLAZ-00217827
GOOG-GLAZ-00217828
GOOG-GLAZ-00217829
GOOG-GLAZ-00217830
GOOG-GLAZ-00217831
GOOG-GLAZ-00217832
GOOG-GLAZ-00217833
GOOG-GLAZ-00217834
GOOG-GLAZ-00217835
GOOG-GLAZ-00217836
GOOG-GLAZ-00217837
GOOG-GLAZ-00217838
GOOG-GLAZ-00217839
GOOG-GLAZ-00217840
GOOG-GLAZ-00217841
GOOG-GLAZ-00217842
GOOG-GLAZ-00217843
GOOG-GLAZ-00217844
GOOG-GLAZ-00217845
GOOG-GLAZ-00217846
GOOG-GLAZ-00217847
GOOG-GLAZ-00217848
GOOG-GLAZ-00217849
GOOG-GLAZ-00217850
GOOG-GLAZ-00217851
GOOG-GLAZ-00217852
GOOG-GLAZ-00217853
GOOG-GLAZ-00217854
GOOG-GLAZ-00217855
GOOG-GLAZ-00217856
GOOG-GLAZ-00217857
GOOG-GLAZ-00217858

GOOG-GLAZ-00218115
GOOG-GLAZ-00218116
GOOG-GLAZ-00218117
GOOG-GLAZ-00218118
GOOG-GLAZ-00218119
GOOG-GLAZ-00218120
GOOG-GLAZ-00218121
GOOG-GLAZ-00218122
GOOG-GLAZ-00218123
GOOG-GLAZ-00218124
GOOG-GLAZ-00218125
GOOG-GLAZ-00218126
GOOG-GLAZ-00218127
GOOG-GLAZ-00218128
GOOG-GLAZ-00218129
GOOG-GLAZ-00218130
GOOG-GLAZ-00218131
GOOG-GLAZ-00218132
GOOG-GLAZ-00218133
GOOG-GLAZ-00218134
GOOG-GLAZ-00218135
GOOG-GLAZ-00218136
GOOG-GLAZ-00218137
GOOG-GLAZ-00218138
GOOG-GLAZ-00218139
GOOG-GLAZ-00218140
GOOG-GLAZ-00218141
GOOG-GLAZ-00218142
GOOG-GLAZ-00218143
GOOG-GLAZ-00218144
GOOG-GLAZ-00218145
GOOG-GLAZ-00218146
GOOG-GLAZ-00218147
GOOG-GLAZ-00218148
GOOG-GLAZ-00218149
GOOG-GLAZ-00218150
GOOG-GLAZ-00218151
GOOG-GLAZ-00218152
GOOG-GLAZ-00218153
GOOG-GLAZ-00218154
GOOG-GLAZ-00218155
GOOG-GLAZ-00218156
GOOG-GLAZ-00218157

GOOG-GLAZ-00217859
GOOG-GLAZ-00217860
GOOG-GLAZ-00217861
GOOG-GLAZ-00217862
GOOG-GLAZ-00217863
GOOG-GLAZ-00217864
GOOG-GLAZ-00217865
GOOG-GLAZ-00217866
GOOG-GLAZ-00217867
GOOG-GLAZ-00217868
GOOG-GLAZ-00217869
GOOG-GLAZ-00217870
GOOG-GLAZ-00217871
GOOG-GLAZ-00217872
GOOG-GLAZ-00217873
GOOG-GLAZ-00217874
GOOG-GLAZ-00217875
GOOG-GLAZ-00217876
GOOG-GLAZ-00217877
GOOG-GLAZ-00217878
GOOG-GLAZ-00217879
GOOG-GLAZ-00217880
GOOG-GLAZ-00217881
GOOG-GLAZ-00217882
GOOG-GLAZ-00217883
GOOG-GLAZ-00217884
GOOG-GLAZ-00217885
GOOG-GLAZ-00217886
GOOG-GLAZ-00217887
GOOG-GLAZ-00217888
GOOG-GLAZ-00217889
GOOG-GLAZ-00217890
GOOG-GLAZ-00217891
GOOG-GLAZ-00217892
GOOG-GLAZ-00217893
GOOG-GLAZ-00217894
GOOG-GLAZ-00217895
GOOG-GLAZ-00217896
GOOG-GLAZ-00217897
GOOG-GLAZ-00217898
GOOG-GLAZ-00217899
GOOG-GLAZ-00217900
GOOG-GLAZ-00217901

GOOG-GLAZ-00218158
GOOG-GLAZ-00218159
GOOG-GLAZ-00218160
GOOG-GLAZ-00218161
GOOG-GLAZ-00218162
GOOG-GLAZ-00218163
GOOG-GLAZ-00218164
GOOG-GLAZ-00218165
GOOG-GLAZ-00218166
GOOG-GLAZ-00218167
GOOG-GLAZ-00218168
GOOG-GLAZ-00218169
GOOG-GLAZ-00218170
GOOG-GLAZ-00218171
GOOG-GLAZ-00218172
GOOG-GLAZ-00218173
GOOG-GLAZ-00218174
GOOG-GLAZ-00218175

Google's 11/22/2021 Responses to State's Interrogatories, Set Six

Complaint in State of Washington v. Google LLC

Complaint in District of Columbia v. Google LLC

Complaint in State of Texas v. Google LLC

Complaint in State of Indiana v. Google LLC

Conversation with Dr. Arunesh Mathur, June 20, 2022.

GOOG-GLAZ-00217902
GOOG-GLAZ-00217903
GOOG-GLAZ-00217904
GOOG-GLAZ-00217978
GOOG-GLAZ-00217979
GOOG-GLAZ-00217980
GOOG-GLAZ-00217981
GOOG-GLAZ-00217982
GOOG-GLAZ-00217983
GOOG-GLAZ-00217984
GOOG-GLAZ-00217985
GOOG-GLAZ-00217986
GOOG-GLAZ-00217987
GOOG-GLAZ-00217988
GOOG-GLAZ-00218060
GOOG-GLAZ-00218061
GOOG-GLAZ-00218062
GOOG-GLAZ-00218063
GOOG-GLAZ-00218064
GOOG-GLAZ-00218065
GOOG-GLAZ-00218066
GOOG-GLAZ-00218067
GOOG-GLAZ-00218068
GOOG-GLAZ-00218069
GOOG-GLAZ-00218070
GOOG-GLAZ-00218071
GOOG-GLAZ-00218072

STATE OF WASHINGTON
KING COUNTY SUPERIOR COURT

STATE OF WASHINGTON,

Plaintiff,

v.

GOOGLE LLC, a Delaware limited liability company,

Defendant.

Case No.

COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF UNDER THE CONSUMER PROTECTION ACT, RCW 19.86

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

[redacted] As one Google employee put it, "Real people just think in terms of 'location is on,' 'location is off' because that's exactly what you have on the front screen of your phone."

E. Google Deploys Deceptive Practices that Undermine Users' Ability to Make Informed Choices About Their Data

4.68 Google engages in unfair and deceptive practices that makes it difficult for users to decline location tracking or to evaluate the data collection and processing to which they are purportedly consenting. Such practices are known in academic literature as "dark patterns." Dark patterns are deceptive design choices that take advantage of behavioral tendencies to manipulate users to make choices for the designer's benefit and to the user's detriment. Examples of "dark patterns" include complicated navigation menus, visual misdirection, confusing wording (such as double negatives), and repeated nudging.

4.69 Google makes extensive use of dark patterns, including repeated nudging, misleading pressure tactics, and evasive and deceptive descriptions of location features and settings, to cause users to provide more and more location data (inadvertently or out of frustration).

1. Dark Patterns in Google Account Settings

4.70 Some of Google's deceptive practices with respect to Google Account settings alleged above reflect the use of dark patterns. For example, Google's decision to enable the Web & App Activity feature by default while failing to disclose the existence of the setting was a deceptive use of design. Through this dark pattern, Google not only misled users about the extent of its location tracking, but also made it difficult for users to opt-out of this tracking.

4.71 Google also uses dark patterns through its "in-product" prompts to encourage users to enable Google Account settings. For example, for at least part of the relevant time period, Google told users that certain Google products, such as Google Maps, Google Now, and Google Assistant "need[]" or "depend[] on," the Location History feature when setting up these products. *See:*

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

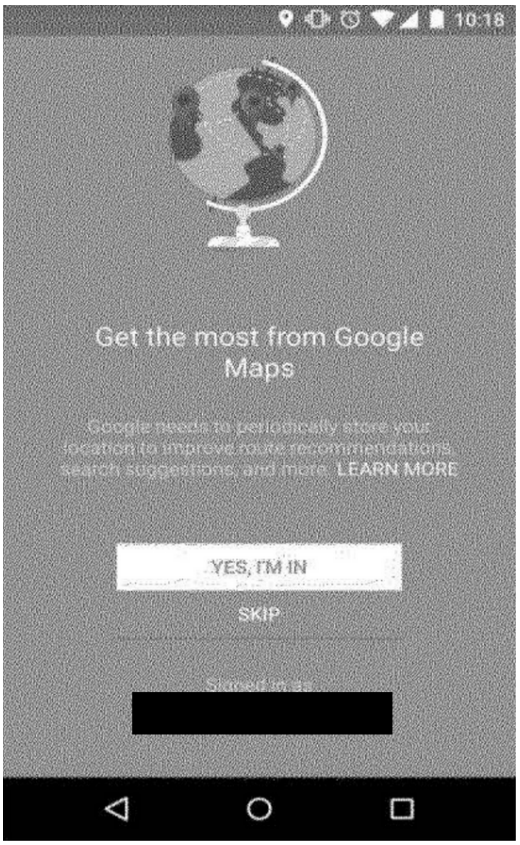


Fig 4 ("Get the most from Google Maps[:] Google needs to periodocally store your location to improve route recommendations, search suggestions, and more").

4.72 However, these products could properly function without users agreeing to constant tracking. For example, Maps and Google Now did not "need" Location History in order to perform its basic functions and, in fact, both products would continue to function if the user disabled Location History.

4.73 Google also used dark patterns in its design for the set-up process of certain Google products. For example, Google prompted users to enable Location History and Web & App Activity, along with multiple other settings, in order to use products like Google Assistant or Google Now. By presenting users with an "all or nothing" opt-in, Google similarly denied users the ability to choose which data-sharing features to enable, unless users took the additional and burdensome

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

action of trying to locate and disable these features after set-up. In other words, users could only opt in or out of these settings collectively at set-up of the Google product. *See:*

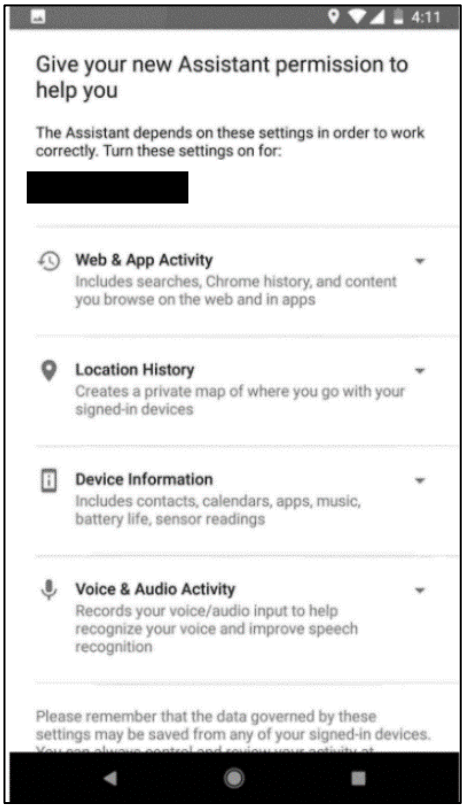


Fig. 5 ("Give your new Assistant permission to help you[.] The Assistant depends on these setting in order to work correctly. Turn these setting on for: . . . Web & App Activity[:] Includes searches, Chrome history, and content you browse on the web and in apps[;] Location History[:] Creates a private map of where you go with your signed-in devices").

4.74 Google also did not (and still does not) give users the choice to decline location tracking once and for all. For example, if users decline to enable Location History or Web & App Activity when first prompted while setting up their Android device, Google continues to repeatedly prompt users to enable these settings when using Google products.

4.75 [redacted] By repeatedly "nudging" users to enable Google Account settings, Google increases the chances that a user will enable the setting

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

inadvertently or out of frustration. Google does not and has never provided similarly frequent prompts to opt out of location sharing.

4.76 [redacted]

4.77 Until at least mid-2018, Google's prompts misleadingly emphasized a few benefits that Location History provided to users—such as commute notifications or more personalized search results—without providing a similar emphasis and disclosure about the advertising and monetary benefits to Google. Indeed, Google only revealed that it used this comprehensive data for advertising purposes in separate linked or drop-down disclosures that users would likely never see. *See*:

//

//

//

//

//

//

//

//

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

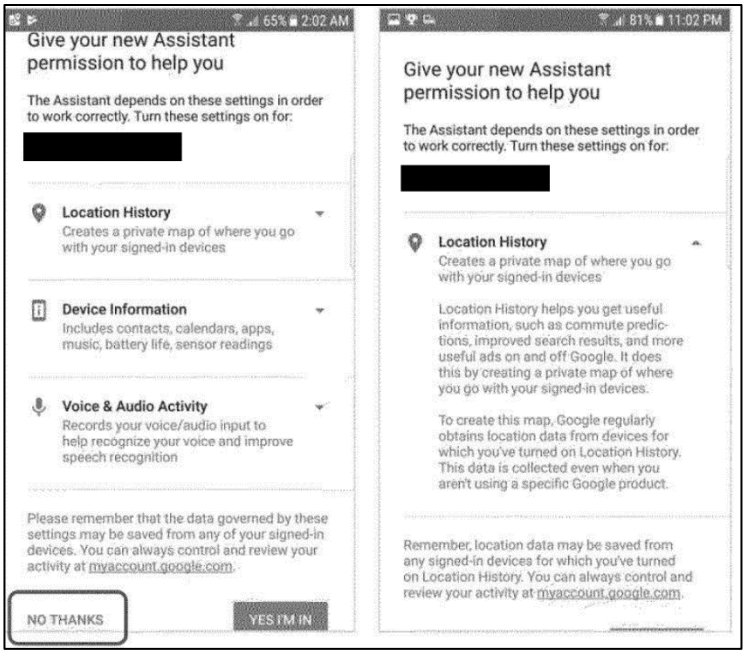


Fig. 6 ("Location History[:] Creates a private map of where you go with your sign-in devices[.] Location History helps you get useful information such as commute predictions, improved search results and more useful ads on and off Google.")

4.78 [redacted]

4.79 At relevant times, users who paused Location History or deleted Location History entries also received vague warnings implying that disabling or limiting Location History would hinder the performance of Google apps. For example, users were told that disabling Location History "limits functionality of some Google products over time, such as Google Maps and Google Now" and that "[n]one of your Google apps will be able to store location data in Location History." Users who deleted Location History entries were also warned that "Google Now and other apps that use your Location History may stop working properly." These failed to provide users with

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

sufficient information to understand what, if any, services would be limited, and deceptively implied that Google products would not function unless the user agreed to provide location data on a continuous basis.

2. Dark Patterns in Device Settings

4.80 Users who seek to limit Google's location data collection through device settings are also confronted with various dark patterns. For example, users may try to disable location settings on their devices, such as through the location "master switch" or the app-specific location permission settings. However, after disabling these settings, users are subject to repeated prompting to re-enable location when using a Google app. [redacted]

4.81 Once location is re-enabled on a user's device, other Google apps and services can access the user's location, including (in some versions of the Android OS) when the user is not interacting with the app. The only way to avoid such access is if the user remembers to disable location again, a process which the user is discouraged to undertake because it requires a number of steps and must be repeated every time a user wants to permit (and then deny) Google access to their location.

4.82 During the relevant time period, Google also actively sought to increase the percentage of users who enabled location settings on Android devices by providing vague disclosures and making it more difficult for users to disable these settings. For example, in one version of Android (called KitKat),[10] Google offered a toggle that allowed users to disable location from a pull-down menu at the top of their screen. This made the setting more easily accessible to users. However, Google removed this toggle from Android phones that Google manufactured,

[10] Android KitKat was publicly released on October 31, 2013.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

[redacted]

4.83 [redacted]

[redacted]

Around the same time, Google also changed the dialogue box that users would see when prompted by Google to enable location. Pursuant to this change, Google no longer advised users that they were agreeing to persistent tracking of their precise location by Google, as shown below:

//

//

//

//

//

//

//

//

//

//

//

//

//

//

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

Fig. 7 (Old Version – "Use location? This app wants to change your device setting: Use GPS, Wi-Fi, and cell networks for location. Use Google's location service, sending anonymous location to Google even when no apps are running." New Version – "For best results, let your device turn on location, which uses Google's location service.")

4.84 [redacted]

[redacted]

[redacted]

F. Google Engages in Deceptive and Unfair Acts and Practices in Trade or Commerce in Washington

4.85 Google's deceptive and unfair acts and practices alleged herein occurred in in trade or commerce in Washington. Google offers, sells, provides, and advertises its devices, software products, and services to Washington consumers. Consumers purchase Google's products with the deceptive settings in Washington. Through its ad business, Google receives advertising revenue

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

6.5 That the Court, as an equitable remedy, disgorge Defendant of money, property, or data (including any algorithms developed using such data) acquired by Defendant as a result of the conduct complained of herein.

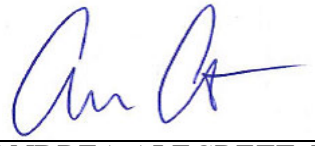
6.6 That the Court make such orders pursuant to RCW 19.86.080 as it deems appropriate to provide for restitution and prejudgment interest on restitution to consumers of money or property acquired by Defendant as a result of the conduct complained of herein.

6.7 That the Court make such orders pursuant to RCW 19.86.080 to provide that the Plaintiff, State of Washington, recover from Defendant the costs of this action, including reasonable attorneys' fees.

6.8 That the Court order such other relief as it may deem just and proper to fully and effectively dissipate the effects of the conduct complained of herein, or which may otherwise seem proper to the Court.

DATED this 24th day of January, 2022.

ROBERT W. FERGUSON
Attorney General



ANDREA ALEGRETT, WSBA #50236
DANIEL DAVIES, WSBA #41793
JOE KANADA, WSBA #55055
KATHLEEN BOX, WSBA #45254
BEN BRYSACZ, WSBA #54683
Assistant Attorneys General
For Plaintiff State of Washington
800 Fifth Avenue, Suite 2000
Seattle, WA 98104
(206) 389-3843

IN THE SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
Civil Division

DISTRICT OF COLUMBIA a municipal corporation 441 4th Street, N.W. Washington, D.C. 20001, Plaintiff, v. **GOOGLE LLC,** 1600 Amphitheatre Parkway, Mountain View, California, 94043, Defendant.	Case No.: **JURY TRIAL DEMANDED**

COMPLAINT FOR VIOLATIONS OF THE CONSUMER PROTECTION PROCEDURES ACT

[redacted] As one Google employee put it, "Real people just think in terms of 'location is on,' 'location is off' because that's exactly what you have on the front screen of your phone."

E. Google Uses Deceptive Practices that Undermine Users' Ability to Make Informed Choices About Their Data.

95. Google has relied on, and continues to rely on, deceptive and unfair practices that make it difficult for users to decline location tracking or to evaluate the data collection and processing to which they are purportedly consenting. Such practices are known in academic literature as "dark patterns." Dark patterns are deceptive design choices that alter the user's decision-making for the designer's benefit and to the user's detriment. Dark patterns take advantage of behavioral tendencies to manipulate users into actions that are harmful to users or contrary to their intent. Common examples of "dark patterns" include complicated navigation menus, visual misdirection, confusing wording (such as double negatives), and repeated nudging.

96. Because location data is immensely valuable to the Company, Google makes extensive use of dark patterns, including repeated nudging, misleading pressure tactics, and evasive and deceptive descriptions of location features and settings, to cause users to provide more and more location data (inadvertently or out of frustration).

1. Dark Patterns in Google Account Settings

97. Some of Google's deceptive practices with respect to Google Account settings already alleged above reflect the use of dark patterns. For example, Google's decision to enable the privacy-intrusive Web & App Activity feature by default, while failing to disclose this setting, was a deceptive use of design. Through this dark pattern, Google not only misled users about the extent of its location tracking, but also made it difficult for users to opt out of this tracking.

98. Google also uses dark patterns in "in-product" prompts to enable Google Account settings—i.e., prompts to enable these settings when a user begins to use Google apps and services

on a device. For example, for at least part of the relevant time period, Google told users that certain Google products, such as Google Maps, Google Now, and Google Assistant "need[]" or "depend[] on," the Location History feature when setting up these products. *See:*

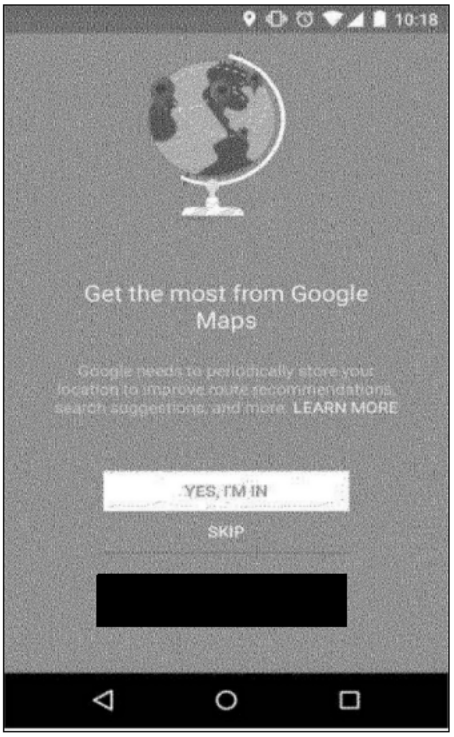


Fig 4 ("Get the most from Google Maps[:] Google needs to periodocally store your location to improve route recommendations, search suggestions, and more.")

99. However, these products could properly function without users agreeing to constant tracking. For example, Maps and Google Now did not "need" Location History in order to perform its basic functions and, in fact, both products would continue to function if the user later took a series of actions to disable Location History. Because Google's statements falsely implied that users were not free to decline Google Account settings if they wished to use certain (often pre-installed) Google products as they were intended, users were left with effectively no choice but to enable these settings.

100. Google also designed the set-up process for certain Google products in a manner that limited users' ability to decide whether to permit Google to track them. In particular, Google

prompted users to enable Location History and Web & App Activity, along with multiple other settings, in order to use products like Google Assistant or Google Now. In other words, users could only opt in or out of these settings collectively at set-up of the Google product. *See:*

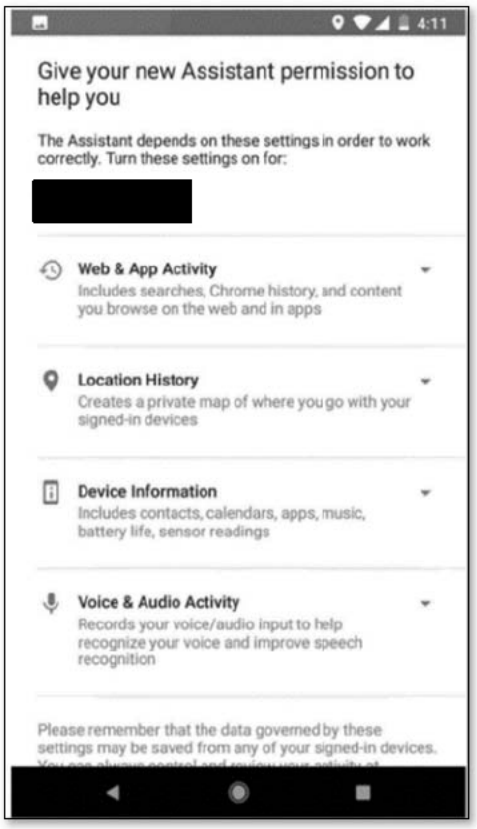


Fig. 5 ("Give your new Assistant permission to help you[.] The Assistant depends on these setting in order to work correctly. Turn these setting on for: . . . Web & App Activity[:] Includes searches, Chrome history, and content you browse on the web and in apps[;] Location History[:] Creates a private map of where you go with your signed-in devices.")

101. By presenting users with an "all or nothing" opt-in, Google similarly denied users the ability to choose which data-sharing features to enable, unless users took the additional and burdensome action of trying to locate and disable these features after set-up.

102. Google also did not (and still does not) give users the choice to decline location tracking once and for all. For example, if users decline to enable Location History or Web & App Activity when first prompted in the set-up process for an Android device, Google continues to

repeatedly prompt users to enable these settings when using Google products—despite already refusing consent.

103. [redacted] By repeatedly "nudging" users to enable Google Account settings, Google increases the chances that a user will enable the setting inadvertently or out of frustration. Google does not and has never provided similarly frequent prompts to opt out of location sharing.

104. [redacted]

105. Further, until at least mid-2018, users who read Google's prompts to enable Google Account settings were provided only vague and imbalanced information about the consequences of enabling Google Account settings, unless users clicked on links that led to further information. These prompts misleadingly emphasized a few benefits that Location History provided to users—such as commute notifications or more personalized search results—without providing a similar emphasis and disclosure about the advertising and monetary benefits to Google. Indeed, Google

only revealed that it used this comprehensive data for advertising purposes in separate linked or drop-down disclosures that users would likely never see. *See*:

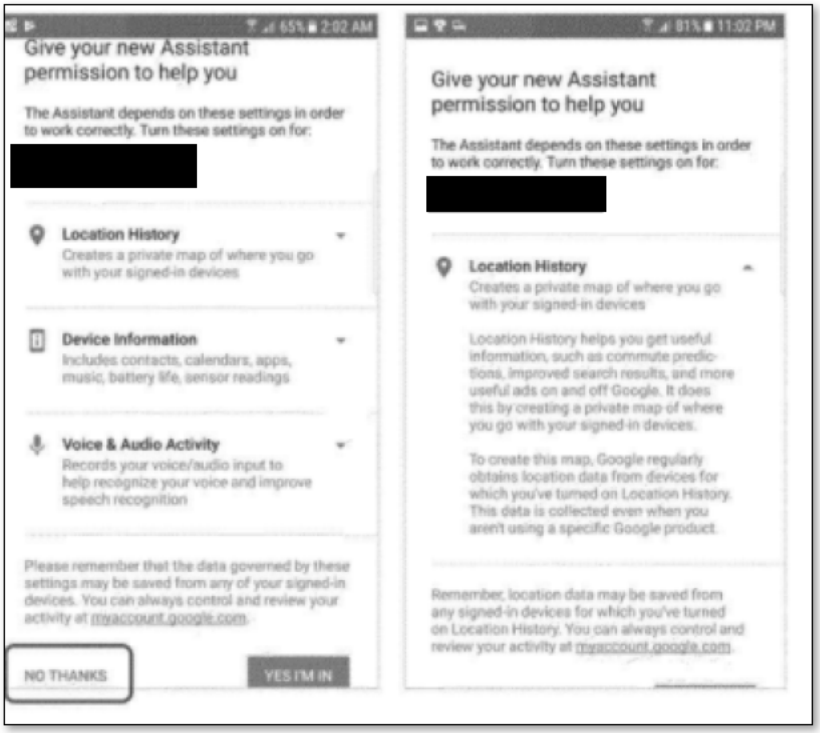


Fig. 6 ("Location History[:] Creates a private map of where you go with your sign-in devices[.] Location History helps you get useful information such as commute predictions, improved search results and more useful ads on and off Google.")

106. [redacted]

107. At relevant times, users who paused Location History or deleted Location History entries also received vague warnings implying that disabling or limiting Location History would hinder the performance of Google apps. For example, users who disabled Location History were

told that doing so "limits functionality of some Google products over time, such as Google Maps and Google Now" and that "[n]one of your Google apps will be able to store location data in Location History." Users who deleted Location History entries were also warned that "Google Now and other apps that use your Location History may stop working properly." These warnings were misleading because they failed to provide users with sufficient information to understand what, if any, services would be limited, and falsely implied that Google products would not function unless the user agreed to provide location data on a continuous basis.

2. Dark Patterns in Device Settings

108. Users who seek to limit Google's location data collection through Android device settings are also confronted with various dark patterns. For example, users may try to disable location settings on their Android devices, such as through the location "master switch" or the app-specific location permission settings. However, after disabling these settings, users are subject to repeated prompting to re-enable location when using a Google app. [redacted]

109. Once location is re-enabled on a user's device, other Google apps and services can access the user's location, including (in some versions of the Android OS) when the user is not interacting with the app. The only way to avoid such access is if the user remembers to disable location again, a process which the user is discouraged to undertake because it requires a number of steps and must be repeated every time a user wants to permit (and then deny) Google access to their location.

110. During the relevant time period, Google also actively sought to increase the percentage of users who enabled location settings on Android devices by providing vague disclosures and making it more difficult for users to disable these settings. For example, in one version of Android, Google offered a toggle that allowed users to disable location from a pull-

down menu at the top of their screen. This made the setting more easily accessible to users. However, Google removed this toggle from Android phones that Google manufactured, [redacted]

111. [redacted]

112. Around the same time, Google also changed the dialogue box that users would see when prompted by Google to enable location, so that more users would consent to report their locations to Google. Pursuant to this change, users were no longer advised that they were agreeing to persistent tracking of their precise location by Google, as shown below:

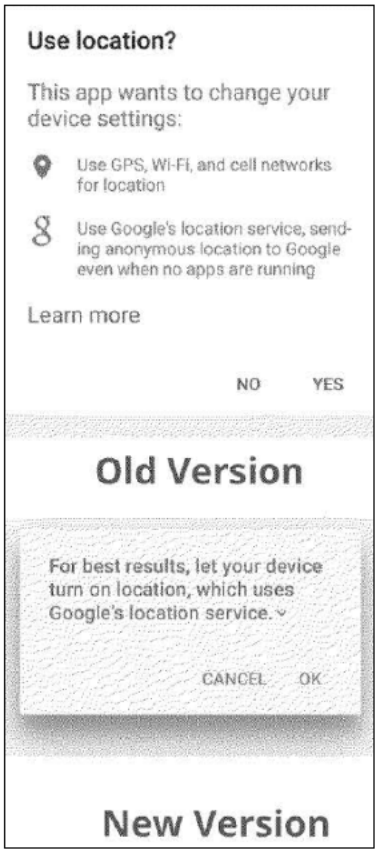


Fig. 7 (Old Version – "Use location? This app wants to change your device setting: Use GPS, Wi-Fi, and cell networks for location. Use Google's location service, sending anonymous location to Google even when no apps are running." New Version – "For best results, let your device turn on location, which uses Google's location service.")

113. [redacted]

114. Google took these actions because it has profound financial incentives to pressure users into enabling location services and other location settings on their devices. Without these settings enabled, Google has a substantially reduced ability to ascertain, extract, and monetize the locations of its users.

135. Google's violations present a continuing harm and the unlawful acts and practices complained of here affect the public interest.

136. Google's actions to date have failed to fully address the misleading and deceptive nature of its business activities and the Company continues to engage in acts prohibited by the CPPA.

PRAYER FOR RELIEF

WHEREFORE, the District respectfully requests that this Court enter judgment against Google and in favor of District as follows:

a. Permanently enjoining Google, pursuant to D.C. Code § 28-3909(a), from violating the CPPA;
b. Order the disgorgement of monies, property, or data (including any algorithms developed using such data) from Google based on its unlawful conduct and/or ordering Google to pay damages and restitution;
c. Award civil penalties in an amount to be proven at trial and as authorized per violation of the CPPA pursuant to D.C. Code § 28-3909(b);
d. Award the District the costs of this action and reasonable attorney's fees pursuant to D.C. Code § 28-3909(b); and
e. Granting such further relief as the Court deems just and proper.

JURY DEMAND

The District demands a trial by jury by the maximum number of jurors permitted by law.

Respectfully submitted,

Dated: January 24, 2022

KARL A. RACINE
Attorney General for the District of Columbia

/s/ Kathleen Konopka
KATHLEEN KONOPKA
Deputy Attorney General
Public Advocacy Division

/s/ Jimmy R. Rock
JIMMY R. ROCK [493521]
Acting Deputy Attorney General
Public Advocacy Division

/s/ Benjamin M. Wiseman
BENJAMIN M. WISEMAN [1005442]
Director, Office of Consumer Protection

/s/ Jennifer M. Rimm
JENNIFER M. RIMM [1019209]
Assistant Attorney General
441 4th Street, N.W.
Washington, D.C. 20001
(202) 741-5226 (Phone)
(202) 741-8949 (Fax)
benjamin.wiseman@dc.gov
jennifer.rimm@dc.gov

Attorneys for the District of Columbia

CAUSE NO._____

THE STATE OF TEXAS, Plaintiff,	§ § §	IN THE DISTRICT COURT OF
v.	§ §	VICTORIA COUNTY, TEXAS
GOOGLE LLC, Defendant	§ §	____ JUDICIAL DISTRICT

PLAINTIFF'S ORIGINAL PETITION

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff, STATE OF TEXAS, acting by and through the Attorney General of Texas, KEN PAXTON (the "State"), complains of Defendant GOOGLE LLC ("GOOGLE," the "Company," or the "Defendant"), and for causes of action would respectfully show as follows:

INTRODUCTION

Google has become one of the richest companies in the world, in part, by deceiving Texans and profiting off their confusion. Specifically, Google has systematically misled, deceived, and withheld material facts from users in Texas about how their location is tracked and used and how to stop Google from monetizing their movements. More to the point, while many Texans may reasonably believe they have disabled the tracking of their location, the reality is that Google has been hard at work behind the scenes logging their movements in a data store Google calls "Footprints." But while footprints generally fade, Google ensures that the location information it stores about Texans is not so easily erased.

Google leads its users to believe that they can easily control what location information the Company retains about them and how it is used. For example, Google has touted a setting called "Location History" as allowing users to prevent Google from tracking their location. Given Google's representations, a reasonable user would expect that turning a setting called "Location

connectivity" setting along with Google Location Services, Google continues to access and use Wi-Fi scanning to locate the user, even if Wi-Fi scanning was disabled by the user.

88. Simply put, even when a user's mobile device is set to deny Google access to location data, the Company finds a way to continue to ascertain the user's location. Google's undisclosed practice of bypassing users' location-related device settings constitutes a deceptive act or practice.

89. Because these practices are not clearly disclosed to users and contradict user expectations, users cannot reasonably avoid Google's access to and use of their location data. [redacted] As one Google employee correctly summed up user beliefs, "Real people just think in terms of 'location is on,' 'location is off' because that's exactly what you have on the front screen of your phone."

E. Google Deploys Deceptive Practices that Undermine Users' Ability to Make Informed Choices About Their Data.

90. In addition to misrepresenting the extent of user control and choice over location-data collection, Google has relied on, and continues to rely on, deceptive practices that make it difficult for users to decline location tracking or to evaluate the data collection and processing to which they are purportedly consenting.

91. Such practices are known in academic literature as "dark patterns." Dark patterns are deceptive design choices that alter the user's decision-making for the designer's benefit

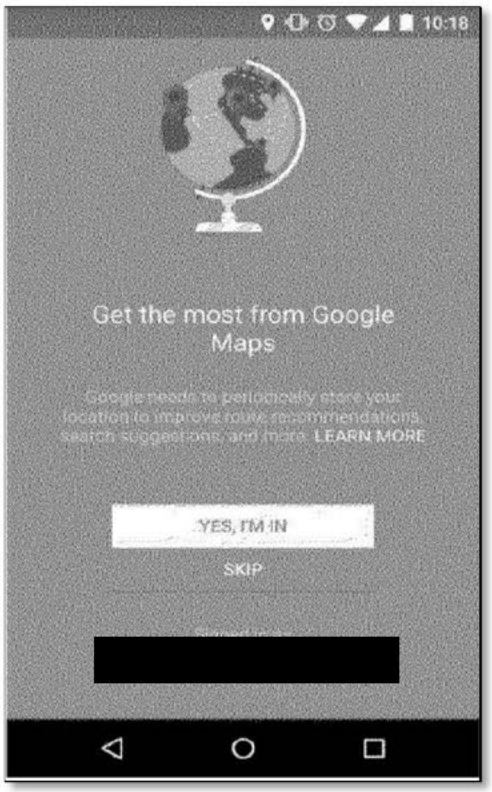
and to the user's detriment. Dark patterns take advantage of behavioral tendencies to manipulate users into actions that are harmful to users or contrary to their intent. Common examples of "dark patterns" include complicated navigation menus, visual misdirection, confusing wording (such as double negatives), and repeated nudging.

92. Because location data is immensely profitable to Google, the Company makes extensive use of dark patterns, including repeated nudging, misleading pressure tactics, and evasive and deceptive descriptions of features and settings, to cause users to provide more and more data (inadvertently or out of frustration), and to impede them from protecting their privacy.

1. Dark Patterns Exist in Google Account Settings.

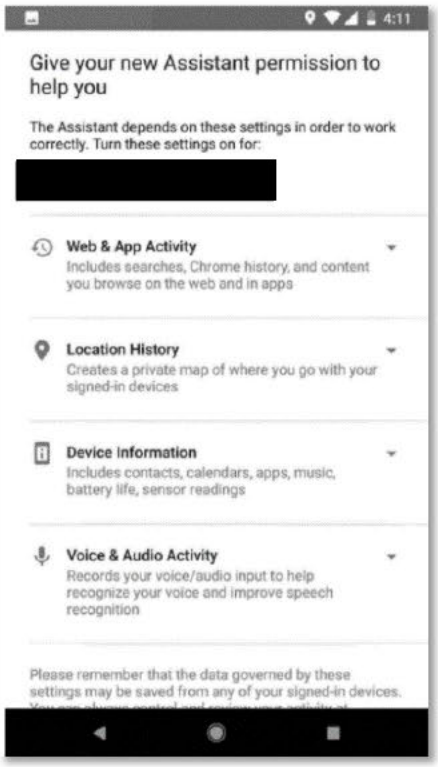
93. Some of Google's deceptive practices with respect to Google Account settings already alleged above reflect the use of dark patterns. For example, Google's decision to enable by default the privacy-intrusive Web & App Activity feature, while failing to disclose this setting, was a deceptive design. By enabling privacy intrusive settings and then hiding those settings, Google not only misled users about the extent of its location tracking, but also made it more difficult for users to refuse this tracking.

94. Dark patterns are also evidenced in Google's presentation of "in-product" prompts to enable Google Account settings—i.e., prompts to enable these settings when a user begins to use Google apps and services on a device. For example, for at least part of the relevant time period, Google told users during setup that certain Google products, such as Google Maps, Google Now, and Google Assistant "need[]"or "depend[] on," the Location History feature. *See:*



95. However, these products could properly function without users agreeing to constant tracking. For example, Maps and Google Now did not "need" Location History to perform their basic functions and, in fact, both products would continue to function if the user later took a series of actions to disable Location History. Because Google's statements falsely implied that users are not free to decline to enable Google Account settings if they wished to use a number of (often pre-installed) Google products as they were intended, users were left with effectively no choice but to enable these settings.

96. Google also designed the set-up process for certain Google products in a manner that limited users' ability to decide whether to permit Google to track them. In particular, Google prompted users to enable Location History and Web & App Activity, along with multiple other settings, in order to use products like Google Assistant or Google Now. *See:*



97. By presenting users with an "all or nothing" opt-in, Google similarly denied users the ability to choose which data-sharing features to enable, unless users took the additional and burdensome action of trying to locate and disable these features after set-up.

98. Google also did not (and still does not) give users the choice to decline location tracking once and for all. If users decline to enable Location History or Web & App Activity when first prompted in the set-up process for an Android device, for instance, they are later shown further prompts to enable these settings when using Google products—despite already refusing consent to these services.

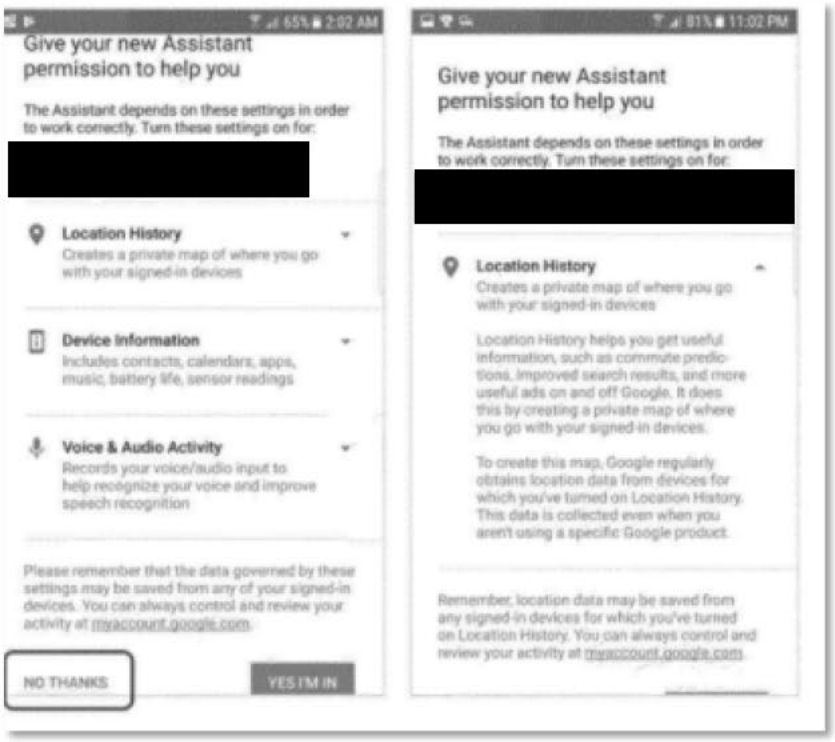
99. [redacted]. By repeatedly "nudging" users to enable Google Account settings, Google increases the chances that a

user will relent and enable the setting inadvertently or out of frustration. Google does not and has never provided similarly frequent prompts to opt *out* of location sharing.

100. [redacted]

101. Further, until at least mid-2018, users who read Google's prompts to enable Google Account settings regarding location issues were provided only vague and imbalanced information about the effects enabling Google Account settings, until users clicked on discrete links that led to further information.

102. These prompts misleadingly emphasized a few benefits that Location History provided to users—such as commute notifications or more personalized search results—without providing a similar emphasis and disclosure about the advertising and monetary benefits to Google. Indeed, Google only revealed that it used this comprehensive data for advertising purposes in separate linked or drop-down disclosures that were hard to find. *See*:



103. [redacted]

104. At relevant times, users who paused Location History or deleted Location History entries also received vague warnings implying that disabling or limiting Location History would hinder the performance of Google apps. For example, users who disabled Location History were told that doing so "limits functionality of some Google products over time, such as Google Maps and Google Now" and that "[n]one of your Google apps will be able to store location data in Location History." Users who deleted Location History entries were also

warned that "Google Now and other apps that use your Location History may stop working properly." These warnings were misleading because they failed to provide users with sufficient information to understand what, if any, services would be limited, and they falsely implied that Google products would not function unless the user agreed to provide location data on a continuous basis.

2. Dark Patterns Exist in Device Settings.

105. Users who seek to limit Google's location data collection through device settings also face an uphill battle to protect their privacy as a result of Google's deceptive design practices. For example, users may try to limit Google's surveillance of their location through the location "master switch" or the app-specific location permission settings. However, after disabling these settings, users are subject to repeated pressuring to re-enable location tracking when using various Google apps. One Google employee complained, [redacted]

106. Furthermore, once location is re-enabled on a user's device, other Google apps and services can access the user's location, including (in some versions of the Android OS) when the user is not interacting with the app. The only way to avoid such access is if the user remembers to disable location again, a process which the user is discouraged to undertake because it requires a number of steps and must be repeated every time a user wants to permit (and then deny) Google access to their location.

107. During the relevant time period, Google also actively sought to increase the percentage of users who enabled location settings on Android devices by providing vague disclosures

and making it more difficult for users to disable these settings. For example, in one version of Android (called KitKat),[12] Google offered a toggle that allowed users to disable location from a pull-down menu at the top of their screen. This made the setting more easily accessible to users. However, Google removed this toggle from Android phones that Google manufactured, [redacted]

108. [redacted].

[12] Android KitKat was publicly released on October 31, 2013.

109. Around the same time, Google also changed the dialogue box that users would see when prompted by Google to enable location, so that more users would consent to report their locations to Google. Pursuant to this change, users were no longer advised that they were agreeing to persistent tracking of their precise location by Google, as shown below:

110. [redacted].

111. Google took these actions because it has profound financial incentives to pressure users into enabling location services and other location settings on their devices. Without these settings enabled, Google had a substantially reduced ability to ascertain, extract, and monetize the locations of its users.

of restitution, damages or civil penalties, as provided by law.

116. Plaintiff further prays that this court grant all other relief to which Plaintiff may show itself entitled.

Respectfully submitted,

NORTON ROSE FULBRIGHT US LLP

/s/ Marc B. Collier
Marc B. Collier
Texas State Bar No: 00792418
Marc.collier@nortonrosefulbright.com
Julie Searle
Texas State Bar No: 24037162
Julie.Searle@nortonrosefulbright.com
Chris Cooke
(pro hac to be sought)
Christopher.cooke@nortonrosefulbright.com
Sean Patrick McGinley
Texas State Bar No: 24116740
Sean.patrick.mcginley@nortonrosefulbright.com
Chase Sippel
Texas State Bar No. 24126753
Chase.sippel@nortonrosefulbright.com
98 San Jacinto Blvd., Suite 1100
Austin, Texas 78701
(512) 474-5201 – Tel
(512) 536-4598 – Fax

Vic Domen
Vic.domen@nortonrosefulbright.com
(pro hac to be sought)
799 9th Street NW, Suite 1000
Washington, DC, 20001
(202) 662-0200 – Tel

NORTON ROSE FULBRIGHT US LLP

/s/ Joseph Graham
Joseph Graham
Texas State Bar No: 24044814
Joseph.graham@nortonrosefulbright.com
M. Miles Robinson
Texas State Bar No. 24110288
Miles.robinson@nortonrosefulbright.com
Fulbright Tower
1301 McKinney, Suite 5100
Houston, Texas 77010-3095
(713) 651-5151 – Tel
(713) 651-5246 – Fax

/s/Ronald B. Walker
Ronald B. Walker
State Bar No. 20728300
rwalker@walkerkeeling.com
WALKER KEELING LLP
101 W. Goodwin, Ste. 400
Post Office Box 108
Victoria, Texas 77902
Tel. (361) 576-6800
Fax (361) 576-6196

KEN PAXTON
Attorney General

/s/ Shawn E. Cowles

Brent Webster, First Assistant Attorney General of Texas
Brent.Webster@oag.texas.gov
Grant Dorfman, Deputy First Assistant Attorney General
Grant.Dorfman@oag.texas.gov
Murtaza Sutarwalla, Deputy Attorney General for Legal Counsel
Murtaza.Sutarwalla@oag.texas.gov
Aaron Reitz, Deputy Attorney General For Legal Strategy
Aaron.Reitz@oag.texas.gov
Shawn E. Cowles, Deputy Attorney General for Civil Litigation
Shawn.Cowles@oag.texas.gov
Nanette DiNunzio, Associate Deputy Attorney General for Civil Litigation
Nanette.Dinunzio@oag.texas.gov
Ralph Molina, Special Counsel to the First Assistant Attorney General
Ralph.Molina@oag.texas.gov

Steve Robinson, Chief,
Consumer Protection Division
Steven.Robinson@oag.texas.gov
Pedro Perez, Deputy Chief,
Consumer Protection Division
Pedro.Perez@oag.texas.gov
Jennifer Roscetti, Deputy Chief,
Consumer Protection Division
Jennifer.Roscetti@oag.texas.gov
Brad Schuelke, Assistant Attorney General,
Consumer Protection Division
Brad.Schuelke@oag.texas.gov
James Holian, Assistant Attorney General,
Consumer Protection Division
James.Holian@oag.texas.gov
Patrick Abernethy, Assistant Attorney General, Consumer Protection Division
Patrick.Abernethy@oag.texas.gov
Jacob Petry, Assistant Attorney General,
Consumer Protection Division
Jacob.Petry@oag.texas.gov
Jameson Joyce, Assistant Attorney General,
Consumer Protection Division
Jameson.Joyce@oag.texas.gov
Tamra Fisher, Assistant Attorney General,
Consumer Protection Division
Tamra.Fisher@oag.texas.gov

OFFICE OF THE ATTORNEY GENERAL OF TEXAS
P.O. Box 12548
Austin, TX 78711-2548
(512) 936-1674

Attorneys for Plaintiff State of Texas

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT
	)	
COUNTY OF MARION	)	CAUSE NO._____

STATE OF INDIANA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**JURY TRIAL DEMANDED**
	)	
GOOGLE LLC,	)	
	)	
Defendant.	)	

COMPLAINT FOR CIVIL PENALTIES, INJUNCTION, RESTITUTION, DISGORGEMENT, COSTS AND OTHER RELIEF

114. Simply put, even when a consumer's mobile device is set to deny Google access to location data, the Company finds a way to continue to ascertain the consumer's location. Google's undisclosed practice of bypassing consumers' location-related device settings constitutes a deceptive and unfair act or practice. Because these practices are not clearly disclosed to consumers and contradict consumer expectations, consumers cannot reasonably avoid Google's access to and use of their location data.

115. Google employees admit that the Company's practices contradict consumer expectations. [redacted] "Real people just think in terms of 'location is on,' 'location is off' because that's exactly what you have on the front screen of your phone."

E. Google Deploys Deceptive Practices that Undermine Consumers' Ability to Make Informed Choices About Their Data

116. Google has relied on, and continues to rely on, deceptive and unfair practices that makes it difficult for consumers to decline location tracking or to evaluate the data collection and processing to which they are purportedly consenting. Such practices are known in academic literature as "dark patterns."

117. Dark patterns are deceptive design choices that alter the consumer's decision-making for the designer's benefit and to the consumer's detriment. Dark patterns take advantage of behavioral tendencies to manipulate consumers into actions that are harmful to consumers or

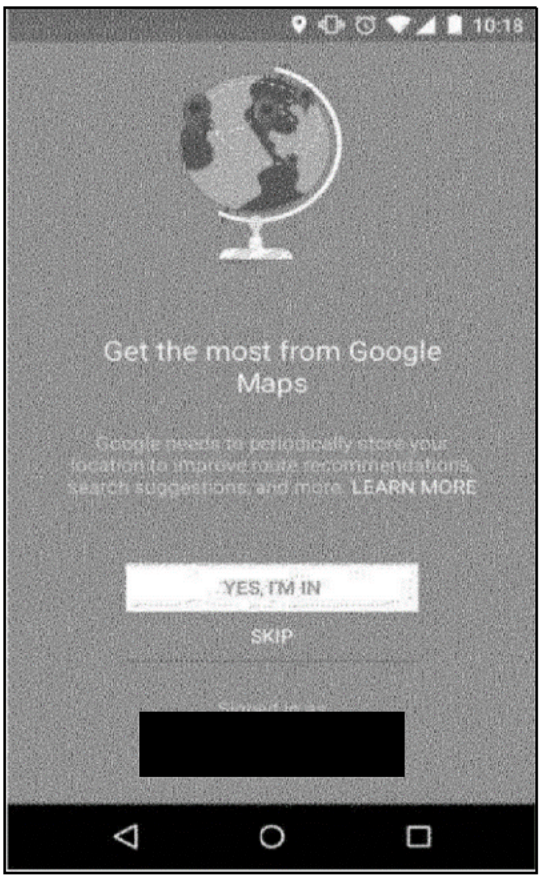
contrary to their intent. Common examples of "dark patterns" include complicated navigation menus, visual misdirection, confusing wording (such as double negatives), and repeated nudging.

118. Because location data is immensely valuable to the Company, Google makes extensive use of dark patterns, including repeated nudging, misleading pressure tactics, and evasive and deceptive descriptions of location features and settings, to cause consumers to provide more and more location data (inadvertently or out of frustration).

1. Dark Patterns in Google Account Settings

119. Some of Google's deceptive practices with respect to Google Account settings described above reflect the use of dark patterns. For example, Google's decision to enable by default the privacy-intrusive Web & App Activity feature by default, while failing to disclose this setting, was a deceptive use of design. Through this dark pattern, Google not only misled consumers about the extent of its location tracking, but also made it difficult for consumers to opt out of this tracking.

120. Google also uses dark patterns in "in-product" prompts to enable Google Account settings—i.e., prompts to enable these settings when a consumer begins to use Google apps and services on a device. For example, for at least part of the relevant time period, Google told consumers that certain Google products, such as Google Maps, Google Now, and Google Assistant "need[]" or "depend[] on," the Location History feature when setting up these products. *See:*

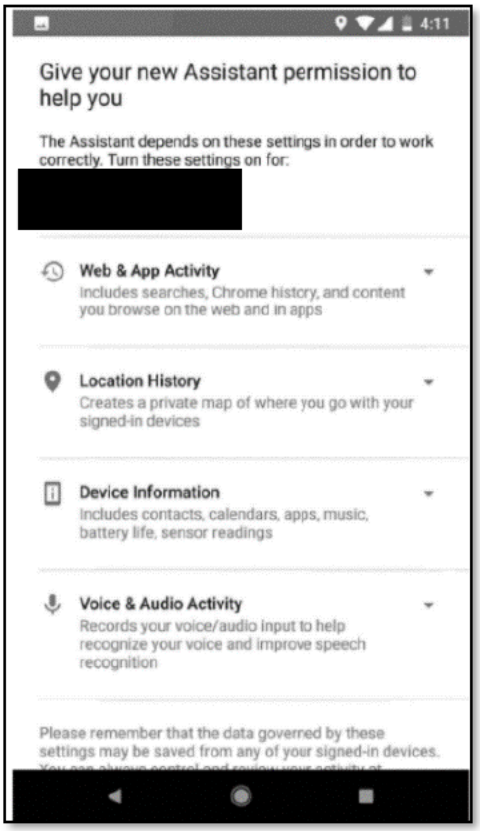


(*Text above:* "Get the most from Google Maps[:] Google needs to periodocally store your location to improve route recommendations, search suggestions, and more").

121. However, these products could properly function without consumers agreeing to constant tracking. [redacted] Because Google's statements falsely implied that consumers are not free to decline to enable Google Account settings if they wished to use a number of (often pre-installed) Google products as they were intended, consumers were left with effectively no choice but to enable these settings.

122. Google also designed the set-up process for certain Google products in a manner that limited consumers' ability to decide whether to permit Google to track them. In particular, Google prompted consumers to enable Location History and Web & App Activity, along with

multiple other settings, in order to use products like Google Assistant or Google Now. In other words, consumers could only opt in or out of these settings collectively at set-up of the Google product. *See:*



(*Text above:* "Give your new Assistant permission to help you[.] The Assistant depends on these setting in order to work correctly. Turn these setting on for: . . . Web & App Activity[:] Includes searches, Chrome history, and content you browse on the web and in apps[;] Location History[:] Creates a private map of where you go with your signed-in devices").

123. By presenting consumers with an "all or nothing" opt-in, Google similarly denied consumers the ability to choose which data-sharing features to enable, unless consumers took the additional and burdensome action of trying to locate and disable these features after set-up.

124. Google also did not (and still does not) give consumers the choice to decline location tracking once and for all. For example, if users decline to enable Location History or Web & App Activity when first prompted in the set-up process for an Android device, Google continues

to repeatedly prompt users to enable these settings when using Google products—despite already refusing consent.

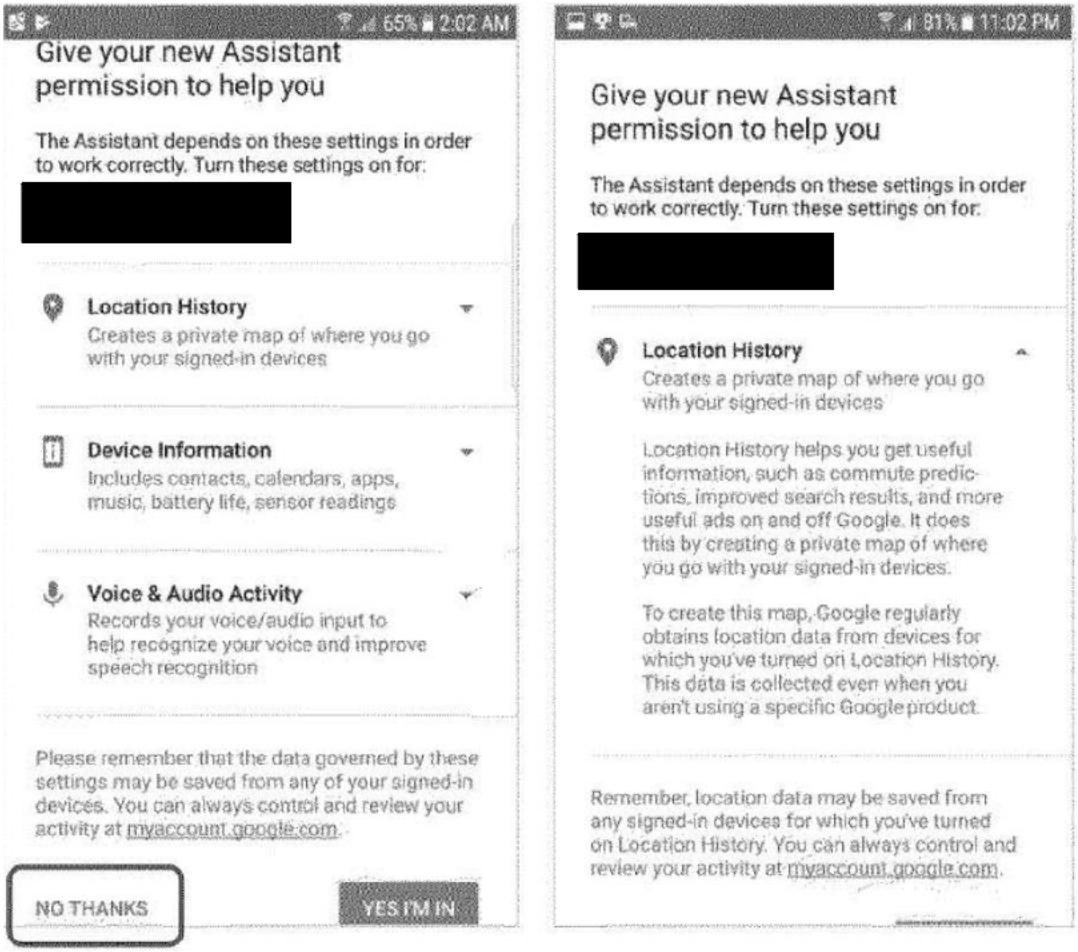
125. [redacted] By repeatedly "nudging" consumers to enable Google Account settings, Google increases the chances that a consumer will enable the setting inadvertently or out of frustration. Google does not and has never provided similarly frequent prompts to opt out of location sharing.

126. [redacted]

127. Further, until at least mid-2018, consumers who read Google's prompts to enable Google Account settings were provided only vague and imbalanced information about the consequences of enabling Google Account settings, unless consumers clicked on links that led to further information.

128. These prompts misleadingly emphasized a few benefits that Location History provided to consumers—such as commute notifications or more personalized search results—without providing a similar emphasis and disclosure about the advertising and monetary benefits

to Google. Indeed, Google only revealed that it used this comprehensive data for advertising purposes in separate linked or drop-down disclosures that consumers would likely never see. *See*:



129. [redacted]

130. At relevant times, consumers who paused Location History or deleted Location History entries also received vague warnings implying that disabling or limiting Location History would hinder the performance of Google apps. For example, consumers who disabled Location History were told that doing so "limits functionality of some Google products over time, such as Google Maps and Google Now" and that "[n]one of your Google apps will be able to store location data in Location History." Consumers who deleted Location History entries were also warned that "Google Now and other apps that use your Location History may stop working properly." These warnings were misleading because they failed to provide consumers with sufficient information to understand what, if any, services would be limited, and falsely implied that Google products would not function unless the consumer agreed to provide location data on a continuous basis.

2. Dark Patterns in Device Settings.

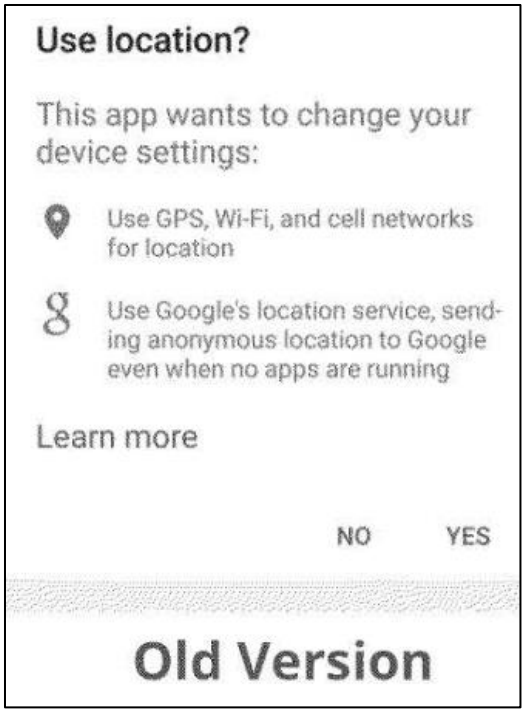
131. Users who seek to limit Google's location data collection through Android device settings are also confronted with various dark patterns. For example, consumers may try to disable location settings on their devices, such as through the location "master switch" or the app-specific location permission settings. However, after disabling these settings, consumers are subject to repeated prompting to re-enable location when using a Google app. [redacted]

132. Once location settings are re-enabled on a consumer's device, other Google apps and services can access the consumer's location, including (in some versions of the Android OS) when the consumer is not interacting with the app. The only way to avoid such access is if the consumer remembers to disable location settings again, a process which the consumer is discouraged to undertake because it requires a number of steps and must be repeated every time a consumer wants to permit (and then deny) Google access to their location.

133. During the relevant time period, Google also actively sought to increase the percentage of consumers who enabled location settings on Android devices by providing vague disclosures and making it more difficult for consumers to disable these settings. For example, in one version of Android, Google offered a toggle that allowed consumers to disable location from a pull-down menu at the top of their screen. This made the setting more easily accessible to consumers. However, Google removed this toggle from Android phones that Google manufactured, [redacted]

134. [redacted]

135. Around the same time, Google also changed the dialogue box that consumers would see when prompted by Google to enable location, so that more consumers would consent to report their locations to Google. Pursuant to this change, consumers were no longer advised that they were agreeing to persistent tracking of their precise location by Google, as shown below*:*



136. [redacted]

137. Google took these actions because it has profound financial incentives to pressure consumers into enabling location services and other location settings on their devices. Without these settings enabled, Google has a substantially reduced ability to ascertain, extract, and monetize the locations of its consumers.

CAUSES OF ACTION

COUNT I

Google Committed Unfair, Abusive, and/or Deceptive Acts, Omissions, and/or Practices in Violation of Ind. Code. § 24-5-0.5-3(a)

138. The State of Indiana incorporates herein by reference all preceding paragraphs as if fully set forth herein.

JURY DEMAND

The State of Indiana demands a trial by jury by the maximum number of jurors permitted by law.

Respectfully submitted,

THEODORE E. ROKITA
Indiana Bar No. 18857-49
Indiana Attorney General

Date: January 24, 2022 By: */s/ Douglas S. Swetnam*
DOUGLAS S. SWETNAM
Indiana Bar No. 15860-49
Douglas.Swetnam@atg.in.gov

/s/ Vanessa Voigt Gould
VANESSA VOIGT GOULD
Indiana Bar No. 26719-49
Vanessa.Voigt@atg.in.gov

/s/ Jennifer Van Dame
JENNIFER M. VAN DAME
Indiana Bar No. 32788-53
Jennifer.VanDame@atg.in.gov

Deputy Attorneys General
302 West Washington Street
IGCS – 5th Floor
Indianapolis, IN 46204
(317) 232-6294 (Swetnam)
(317) 232-7979 (Fax)

Counsel for State of Indiana