

No. ____

In the Supreme Court of Texas

THE STATE OF TEXAS,

Petitioner,

v.

GOOGLE, LLC,

Respondent.

On Petition for Review
from the Thirteenth Court of Appeals, Corpus Christi-Edinburg

PETITION FOR REVIEW

KRISTINA WILLIAMS
State Bar No. 24078303
Norton Rose Fulbright US LLP
2200 Ross Avenue, Suite 3600
Dallas, Texas 75201
Tel.: (214) 855-8000

KEN PAXTON
Attorney General of Texas
BRENT WEBSTER
First Assistant Attorney General
AARON L. NIELSON
Solicitor General

JACOB C. BEACH
Assistant Solicitor General
State Bar No. 24116083
Jacob.Beach@oag.texas.gov

Office of the Attorney General
P.O. Box 12548 (MC 059)
Austin, Texas 78711
Tel.: (512) 936-1700
Fax: (512) 474-2697

Counsel for Petitioner

IDENTITY OF PARTIES AND COUNSEL

Petitioner:

The State of Texas

Appellate and Trial Counsel for Petitioner:

Ken Paxton
Brent Webster
Aaron L. Nielson
Ralph Molina
Jacob C. Beach (lead counsel)
Johnathan Stone
Brad Schuelke
Gabriella Gonzalez
Office of the Attorney General
P.O. Box 12548 (MC 059)
Austin, Texas 78711
Tel.: (512) 936-1700
Jacob.Beach@oag.texas.gov

Joseph M. Graham, Jr.
Jeffrey S. Wolff
Norton Rose Fulbright US LLP
1550 Lamar Street, Suite 2000
Houston, Texas 77010
Tel.: (713) 651-5151

Marc B. Collier
Julie N. Searle
Norton Rose Fulbright US LLP
98 San Jacinto Blvd., Suite 1100
Austin, Texas 78701
Tel.: (512) 474-5201

Kevin D. Cullen
Cullen, Carsner, Seerden and Cullen LLP
P.O. Box 2938
Victoria, Texas 77902
Tel.: (361) 573-6318

Kristina Williams
Josh Owings
Norton Rose Fulbright US LLP
2200 Ross Avenue, Suite 3600
Dallas, Texas 75201
Tel.: (214) 855-8000

Ronald B. Walker
Walker Keeling LLP
101 W. Goodwin, Suite 400
P.O. Box 108
Victoria, Texas 77902
Tel.: (361) 576-6800

Chris Cooke
Norton Rose Fulbright US LLP
111 W. Houston Street, Suite 1800
San Antonio, Texas 78205
Tel.: (210) 224-5575

Respondent:

Google LLC

Appellate and Trial Counsel for Respondent:

Stephen E. McConnico
Steven J. Wingard
Robyn B. Hargrove
John W. Ellis
Bryan D. Lauer
Shelby Hart-Armstrong
Scott Douglass & McConnico LLP
303 Colorado St., Suite 2400
Austin, Texas 78701
Tel.: (512) 495-6300
smcconnico@scottdoug.com

Benedict Y. Hur
Simona Agnolucci
Jonathan Patchen
Eduardo Santacana
Joshua Anderson
Harris Mateen
Willkie Farr & Gallagher LLP
333 Bush Street, 34th Floor
San Francisco, California 94104
Tel.: (415) 858-7401

Jim Cole
Cole, Cole, Easley & Sciba, P.C.
State Bar No. 04538500
302 West Forrest Street
Victoria, Texas 77901
Tel.: (361) 575-0551

TABLE OF CONTENTS

	Page
Identity of Parties and Counsel	i
Index of Authorities	iv
Record References & Abbreviations	vi
Statement of the Case	vii
Statement of Jurisdiction	viii
Issues Presented.....	viii
Introduction	1
Statement of Facts	2
I. Statutory Background	2
II. Factual Background	3
III. Procedural Background.....	5
Summary of the Argument.....	6
Standard of Review	7
Argument	7
I. The Court Should Grant Review and Hold that Google Is Subject to Personal Jurisdiction.	7
A. The opinion below conflicts with <i>Ford</i> and would hamstring civil-enforcement actions.....	9
B. The opinion below also flouts <i>Volkswagen</i>	16
II. The Court Should Grant the Petition to Clarify the Scope of Review for a Special Appearance.	18
Prayer.....	20
Certificate of Compliance	21

INDEX OF AUTHORITIES

Page(s)

Cases:

Auto-Owners Ins. Co. v. Millionder,
 No. 01-24-00221-CV, 2025 WL 375847 (Tex. App.—Houston [1st
 Dist.] Feb. 4, 2025, no pet. h.) (mem. op.).....19

Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.,
 592 U.S. 351 (2021)..... *passim*

Gaddy v. Fenenbock,
 652 S.W.3d 860 (Tex. App.—El Paso 2022, no pet.)19

Graves v. DJO, LLC,
 636 S.W.3d 321 (Tex. App.—Fort Worth 2021, pet. denied)19

Google LLC v. State,
 No. 13-23-00114-CV, 2025 WL 52611 (Tex. App.—Corpus Christi-
 Edinburg Jan. 9, 2025) (mem. op.)..... vii

JPMorgan Chase Bank, N.A. v. Campbell,
 No. 09-20-00161-CV, 2021 WL 2583573 (Tex. App.—Beaumont
 June 24, 2021, no pet.) (mem. op.).....19

Kelly v. Gen. Interior Constr., Inc.,
 301 S.W.3d 653 (Tex. 2010).....19

Luciano v. SprayFoamPolymers.com, LLC,
 625 S.W.3d 1 (Tex. 2021)..... 8

Moncrief Oil Int’l, Inc. v. OAO Gazprom,
 414 S.W.3d 142 (Tex. 2013) 8

Stanger v. Loetzerich,
 No. 14-21-00504-CV, 2023 WL 2884409 (Tex. App.—Houston
 [14th Dist.] Apr. 11, 2023, no pet.) (mem. op.)19

State v. Volkswagen Aktiengesellschaft,
 669 S.W.3d 399 (Tex. 2023) *passim*

Steward Health Care Sys. LLC v. Saidara,
 633 S.W.3d 120 (Tex. App.—Dallas 2021, no pet.) (en banc)19

<i>TV Azteca v. Ruiz</i> , 490 S.W.3d 29 (Tex. 2016)	10, 11, 13
<i>Volkswagen Aktiengesellschaft v. State</i> , 665 S.W.3d 22 (Tex. App.—Austin 2020), <i>rev'd</i> , 669 S.W.3d 399 (Tex. 2023)	16

Statutes:

Tex. Bus. & Com. Code Ann. § 17.44(a).....	2
Tex. Bus. & Com. Code Ann. § 17.46(b)(5).....	2
Tex. Bus. & Com. Code Ann. § 17.46(b)(9).....	2
Tex. Bus. & Com. Code Ann. § 17.46(b)(24).....	2
Tex. Bus. & Com. Code Ann. § 17.47(a).....	3, 14
Tex. Bus. & Com. Code Ann. § 17.47(b).....	3
Tex. Bus. & Com. Code Ann. § 17.47(e).....	3, 14
Tex. Bus. & Com. Code Ann. § 17.60	3, 14
Tex. Bus. & Com. Code Ann. § 17.61	3, 14
Tex. Gov’t Code Ann. § 22.001(a)	viii

Rules:

Tex. R. App. P. 53.1	viii
----------------------------	------

Other Authorities:

Br. of Appellant Google LLC, <i>Google LLC v. State</i> , No. 13-23-00114- CV (Tex. App.—Corpus Christi–Edinburg June 12, 2023)	13
Order Den. Google LLC’s Mot. to Dismiss, <i>Washington v. Google LLC</i> , No. 22-2-01103-3 SEA (Wash. Super. Ct. May 20, 2022)	15
Order, <i>District of Columbia v. Google LLC</i> , No. 2022 CA 000330 B (D.C. Super. Ct. Aug. 31, 2022).....	15

RECORD REFERENCES & ABBREVIATIONS

CR. ____	First four volumes of the Clerk’s Record (filed in the Thirteenth Court on 03/31/2023)
SCR. ____	Sealed fifth volume of the Clerk’s Record (filed in the Thirteenth Court on 03/31/2023)
1.SuppCR. ____	First Supplemental Clerk’s Record (filed in the Thirteenth Court on 05/25/2023) ¹
2.SuppCR. ____	Corrected Second Supplemental Clerk’s Record (filed in the Thirteenth Court on 07/19/2023) ²
3.SuppSCR. ____	Third Supplemental Sealed Clerk’s Record (filed in the Thirteenth Court on 07/25/2023) ³
App. ____	The appendix to this Petition for Review.

¹ Volume 2 of the First Supplemental Clerk’s Record (pages 162-253) was filed under seal in the Thirteenth Court, whereas Volume 1 (pages 1-161) was not filed under seal.

² Specifically, the State cites the Corrected Second Supplemental Clerk’s Record filed with the Thirteenth Court on July 19, 2023, not the Second Supplemental Clerk’s Record filed on July 6, 2023.

³ The Third Supplemental Sealed Clerk’s Record was filed in five volumes: Volume 1 (pages 1-11); Volume 2 (pages 12-501); Volume 3 (pages 502-1006); Volume 4 (pages 1007-1166); and Volume 5 (pages 1167-1189).

STATEMENT OF THE CASE

<i>Nature of the Case:</i>	The State of Texas (the “State”) seeks to hold Google LLC (“Google”) accountable for violations of the Deceptive Trade Practices-Consumer Protection Act (“DTPA”), Tex. Bus. & Com. Code Ann. §§ 17.41-17.63. 2.SuppCR.16-17, 73-76 (App.35-36, 92-95). ⁴ Specifically, Google used deceptive product designs and disclosures to collect data from users in Texas about their location in Texas and their online habits. 2.SuppCR.19-77 (App.38-96).
<i>Trial Court:</i>	377th Judicial District Court, Victoria County, Texas The Honorable Kemper Stephen Williams
<i>Disposition in the Trial Court:</i>	Denied Google’s verified amended special appearance. 4.CR.1233 (App.2).
<i>Parties in the Court of Appeals:</i>	Google was the appellant. The State was the appellee.
<i>Court of Appeals:</i>	The Court of Appeals for the Thirteenth Judicial District, Corpus Christi–Edinburg
<i>Court of Appeals’ Disposition:</i>	In an opinion written by Chief Justice Jaime Tijerina and joined by Justices Silva and Peña, <i>Google LLC v. State</i> , No. 13-23-00114-CV, 2025 WL 52611 (Tex. App.—Corpus Christi–Edinburg Jan. 9, 2025) (mem. op.), the Thirteenth Court reversed the trial court’s order denying Google’s special appearance and rendered judgment dismissing the State’s claims against Google for lack of personal jurisdiction. App.4-21. No motions for rehearing or en banc reconsideration were filed.

⁴ Because the State includes its First Amended Petition and the trial court’s order in the attached appendix, the State includes record citations and appendix citations for the Court’s convenience.

STATEMENT OF JURISDICTION

This Court has jurisdiction over this appeal because it presents a question of law important to the jurisprudence of the state. Tex. Gov't Code Ann. § 22.001(a). *See also* Tex. R. App. P. 53.1.

ISSUES PRESENTED

1. Whether the Thirteenth Court erred by holding that Google is not subject to personal jurisdiction in Texas despite it deceptively collecting data from Texans via mobile devices and applications sold to, owned by, and used by Texans, merely because Google claims that one part of the series of acts that constitutes a violation of the DTPA occurred in California?

2. Whether the Thirteenth Court erred by limiting its jurisdictional inquiry to the State's operative petition and accordingly ignoring additional details the State offered in response to Google's special appearance, thereby deepening a split amongst the court of appeals?

TO THE HONORABLE SUPREME COURT OF TEXAS:

Under the opinion below, Google can deceptively collect troves of personal data from millions of Texans Google knows to be located in Texas, and potentially make billions of dollars in profits from that deception, as long as some of Google's deceptive behavior occurs in California. And the Texas Attorney General ("OAG") cannot enforce Texas law in Texas to prevent Google from doing so. That is not the law in Texas (or anywhere).

Google reaches into Texas to market its goods (i.e., phones) and services (i.e., software) with the goal of collecting data in Texas for profit. Google gathers sensitive personal information generated in Texas by Texans through software and devices sold and used throughout Texas, relying on Google's physical data infrastructure built in Texas. Google misleads users about this data harvesting and, worse, leads them to believe they can turn it *off*. In fact, regardless of users' selected permissions, Google harvests information from millions of Texans without their knowledge, reaping astronomical profits from advertisements targeted to Texans based on their location in Texas. Yet the Thirteenth Court incredibly held that the State cannot enforce the DTPA against Google because the underlying disclosures were purportedly *drafted* in California.

That cannot be correct. A foreign defendant is subject to Texas's jurisdiction for claims *based on its business conduct within Texas*. The Thirteenth Court's laser-

focus on one aspect of Google’s conduct to the exclusion of all the rest was fundamentally erroneous for at least two reasons. First, it ignores that, regardless of where Google drafted the misleading statements, Google delivered those statements to Texans in Texas. Second, Google rendered those statements *misrepresentations* due to its in-state collection of individuals’ location and web activity.

The error below is egregious given the stakes. This is a civil-enforcement action brought by the State under Texas law to stop Google from deceptively collecting Texans’ data in Texas. If the decision below stands, Texas will be the only state facing *this exact issue* that forces its attorney general to ask California courts to protect Texans against Google’s violations of Texas law. And other bad actors will have a roadmap to avoid accountability for violating Texas law.

The Court should grant this petition, reverse the judgment below, and remand for trial.

STATEMENT OF FACTS

The Thirteenth Court correctly stated the nature of the case. *Supra* vii.

I. Statutory Background

The DTPA is “liberally construed” to protect consumers from myriad “[f]alse, misleading, or deceptive acts or practices.” *See, e.g.*, Tex. Bus. & Com. Code Ann. §§ 17.44(a), 17.46(b)(5), (b)(9), (b)(24). In an appropriate Texas district court, OAG may “bring an action in the name of the state against” anyone it “has

reason to believe” is violating or has violated the DTPA. *Id.* § 17.47(a), (b), (e); *see also id.* §§ 17.60, 17.61 (granting investigative powers).

II. Factual Background

Google⁵ offers products and services to millions of Texans. 2.SuppCR.13, 17 (App.32, 36). Google maintains physical data infrastructure in Texas, including its Midlothian data center, hardware to support its Google Fiber service, and roughly a million square feet of office space in multiple Texas cities. 2.SuppCR.17 (App.36); 3.SuppSCR.309. In 2021, Google’s Texas revenue topped \$10.5 billion. *See* SCR.1389.

Google offers the Android operating system (“Android”), which smartphone manufacturers install under contracts with Google and sell to Texans. *See* 2.SuppCR.19 (App.38). Google also sells its Google-branded Pixel phones directly to Texans. 3.SuppSCR.309.

Google developed software that comes preinstalled as part of Android. 2.SuppCR.19 (App.38). Several Google applications and services, such as Chrome and YouTube, can also be used on non-Android devices. 2.SuppCR.20, 38, 53 (App.39, 57, 72). Millions of Texans use Android and other Google software and services. 2.SuppCR.17 (App.36); SCR.1387-88. Google “generates revenues primarily by delivering both performance and brand advertising” on properties like Google Search and YouTube. 3.SuppSCR.346; 2.SuppCR.12-13, 19, 21 (App.31-32, 38, 40).

⁵ Many Google-affiliated businesses operate in Texas, and the State uses “Google” to refer to them collectively. SCR.1387.

Google collects massive amounts of its users' personal data to ensure these advertisements find a responsive audience. 2.SuppCR.21-22 (App.40-41). Google tracks users' location through Android and other software preloaded on Android phones. 2.SuppCR.19-20 (App.38-39). Google also logs location data when non-Android users access Google's applications and services. 2.SuppCR.24-25 (App.43-44). And Chrome logs user data, including websites visited and device location, even when it is set to Incognito Mode. 2.SuppCR.53-54, 60-61 (App.72-73, 79-80).

Google does not fully disclose its data collection to users. 2.SuppCR.23, 27-59 (App.42, 46-78). For example, Google told users that turning off a setting called "Location History" would disable location tracking, but Google failed to disclose that it could (and did) gather essentially the same information through a seemingly unrelated setting called "Web & App Activity." 2.SuppCR.24-26 (App.43-45). Google also maintains settings at different levels—account-level settings that apply wherever Texans sign into their Google accounts, device-level settings for individual Google devices, and even app-level settings specific to each Google service—which often allow Google to collect personal data even after consumers turn off other, similar settings. 2.SuppCR.23, 26-37 (App.42, 45-56).

Similarly, Chrome includes "Incognito Mode." 2.SuppCR.53 (App.72). Upon activation, Incognito Mode informs users that they can now "browse privately." 2.SuppCR.53-54 (App.72-73). Nonetheless, Google still tracks users' web activity during Incognito Mode. 2.SuppCR.59-61, 64-73 (App.78-80, 83-92).

III. Procedural Background

Despite acknowledging that it maintains a significant Texas presence, *see* 1.SuppCR.7; 3.SuppSCR.309, Google filed a Verified Amended Special Appearance (“Special Appearance”), 1.SuppCR.5-156. Google argued that the trial court lacked personal jurisdiction because the State based its claims on representations which *originated* outside Texas and were not “specific to or directed at” Texas because they were “publicly and freely available.” 1.SuppCR.7-9.

The State responded that Google reached into Texas to serve consumers and benefitted massively from its in-state activities. SCR.1398. And the State’s claims relate to Google’s data-collection business in Texas, including Google’s misrepresentations distributed throughout Texas. SCR.1408-12. The State supported its response with a declaration, SCR.1361-1437, and nearly 60 exhibits, 3.SuppSCR.17-501, 507-1006, 1012-1166. Following jurisdictional discovery and a hearing, the trial court denied Google’s Special Appearance. CR.1233.

Google appealed. CR.1260-61. The Thirteenth Court reversed and dismissed the State’s claims. App.21. First, the Thirteenth Court concluded that Google negated general jurisdiction.⁶ App.15. Second, it held that Texas lacked specific jurisdiction because, in the court’s view, the “evidence show[ed] that [Google’s] employees directed the alleged misleading statements from afar,” which meant that the State’s “principal complaint” about Google’s representations “require[d] that the

⁶ The State only challenges the Thirteenth Court’s decision regarding specific jurisdiction.

overwhelming evidence be directed at events outside of Texas.” App.20-21. The Thirteenth Court therefore could not “conclude that [the State] met its initial burden to show that [Google’s] allegedly tortious conduct occurring outside of Texas is sufficient to confer specific jurisdiction over [Google].” App.21.

SUMMARY OF THE ARGUMENT

First, the decision below conflicts with *Ford Motor Co. v. Montana Eighth Judicial District Court*, 592 U.S. 351 (2021). There, the Supreme Court held that specific jurisdiction does not require a strict causal relationship between a defendant’s forum contacts and claims against it. When a defendant serves a market in a state, it can reasonably anticipate facing suit there if its business conduct violates state law. Here, the Thirteenth Court erred by focusing on one aspect of the State’s claims—the out-of-state location of employees responsible for Google’s misrepresentations to Texans—and ignoring the wealth of other allegations about Google’s related conduct in the State. That decision is wrong and sets a troubling precedent for future civil-enforcement actions.

Second, even on the Thirteenth Court’s shockingly narrow view of the facts, Google is subject to personal jurisdiction under *State v. Volkswagen Aktiengesellschaft*, 669 S.W.3d 399 (Tex. 2023). There the Court held that a foreign defendant that technically avoids acting directly within Texas cannot avoid jurisdiction for civil-enforcement claims related to its profitable business in Texas. The defendant’s decision to craft software and related misrepresentations abroad for installation in Texas,

coupled with the resulting financial benefits it received from Texas, rendered it subject to jurisdiction. A far greater connection exists between Google’s Texas contacts—which not only involve Google sending its misrepresentations to Texans but also using those misrepresentations to siphon Texans’ *personal data* to serve its business here—and the State’s claims.

Finally, this case offers an opportunity to clarify procedure for special appearances. The Thirteenth Court ignored factual details the State provided in its response to Google’s special appearance, thereby diverging from decisions of other courts of appeals. This case provides a vehicle to resolve the split.

STANDARD OF REVIEW

Whether personal jurisdiction exists over a nonresident defendant is a question of law this Court reviews de novo. *Volkswagen*, 669 S.W.3d at 413. “Because no findings of fact were issued,” the Court is “obligated to view the record favorably to the trial court’s jurisdictional rulings.” *Id.* at 427-28.

ARGUMENT

I. The Court Should Grant Review and Hold that Google Is Subject to Personal Jurisdiction.

The decision below rests on a crabbed view of the State’s claims that, viewed properly, easily establish jurisdiction under controlling precedent. The touchstone of jurisdictional due process is “whether a nonresident’s conduct and connection to [Texas] are such that it could reasonably anticipate being haled into court []here.”

Moncrief Oil Int'l, Inc. v. OAO Gazprom, 414 S.W.3d 142, 152 (Tex. 2013). It is undisputed that Google does business in Texas, so Google can avoid jurisdiction only if such jurisdiction would conflict with constitutional limitations. See *Luciano v. SprayFoamPolymers.com, LLC*, 625 S.W.3d 1, 8 (Tex. 2021).

The Thirteenth Court decided specific jurisdiction on the ground that Google's Texas contacts are not related⁷ to the State's claims. App.19-21; e.g., *Luciano*, 625 S.W.3d at 14 (specific jurisdiction requires appropriate "nexus between the nonresident defendant, the litigation, and the forum" (citation omitted)). In the Thirteenth Court's view, Texas lacks jurisdiction because Google's misrepresentations—which misled its Texas users into divulging sensitive information to feed Google's targeted advertising services in Texas—were overseen by Google employees working outside of Texas. App.20-21. In effect, the Thirteenth Court accepted Google's invitation to treat this as a wandering plaintiff case in which Google cannot be held liable in Texas for merely making misrepresentations available on passive websites viewable in Texas. That holding ignores the State's Petition and evidence, and it conflicts with multiple decisions of this Court and the United States Supreme Court.

⁷ The Thirteenth Court rested its specific-jurisdiction analysis entirely on relatedness. App.18-21. Were the Court to review this case on its merits, the State would argue that all elements of personal jurisdiction are satisfied.

A. The opinion below conflicts with *Ford* and would hamstring civil-enforcement actions.

In *Ford*, the Supreme Court affirmed that a defendant's in-state business could support claims that were reasonably related to that business apart from any strict causal connection. 592 U.S. at 361-67. *Ford* involved claims arising from car accidents in two states, and in each the plaintiffs asserted that Ford's cars were defective. *Id.* at 354-56. Ford did not dispute that it generally served the car markets in both fora or that it sold many cars in each. *Id.* But Ford nonetheless objected to personal jurisdiction because it had not designed or built the specific cars at issue in the forum states, and it had sold the subject vehicles in other states decades earlier. *Id.* at 356-57. The state supreme courts in both cases rejected that argument, and the Supreme Court affirmed. *Id.* at 354-55.

In doing so, the Supreme Court clarified the required connection between a defendant's forum contacts and the plaintiff's claims. The Constitution requires "an affiliation between the forum and the underlying controversy, principally an activity or an occurrence that takes place in the forum State and is therefore subject to the State's regulation." *Id.* at 359-60 (cleaned up) (citation omitted). The ultimate concern is "fair warning" to a defendant, or "knowledge that a particular activity may subject" that defendant "to the jurisdiction of a foreign sovereign." *Id.* at 360 (citation omitted). But a strict causal connection between a defendant's forum contacts and the claims against it is not required. *Id.* at 361-62. As the Supreme Court explained, "Ford had systematically served a market" in the forum states "for the very

vehicles that the plaintiffs alleged malfunction and injured them in those States.” *Id.* at 365. Accordingly, it did not matter that Ford had first sold the subject cars outside the forum states. *Id.* at 366-67.

The Supreme Court also held that jurisdiction “treat[ed] Ford fairly.” *Id.* at 367. Ford’s substantial business in the forum states meant it “enjoy[ed] the benefits and protection of [their] laws.” *Id.* (last alteration original) (citation omitted). That “assistance to Ford’s in-state business create[d] reciprocal obligations” under those states’ laws, such that a “state court’s enforcement” of Ford’s obligations “can hardly be said to be undue.” *Id.* at 367-68 (citation omitted). Exercising jurisdiction over Ford was therefore “reasonable” and “predictable.” *Id.* at 368. Likewise, the forum states’ “significant interests” in providing courts for “redressing injuries inflicted by out-of-state actors” and “enforcing their own safety regulations” further supported jurisdiction over Ford. *Id.* at 368 (citation omitted).

This Court employed similar reasoning in *TV Azteca v. Ruiz*, 490 S.W.3d 29 (Tex. 2016), which involved allegations that a Mexican TV station defamed a Texan through programming broadcast from Mexico but viewable in Texas. *Id.* at 35-36. While the mere viewability did not subject the defendant to jurisdiction, the defendant’s *additional* conduct aimed at Texas—marketing, advertisements for Texas businesses, and Texas revenue—made jurisdiction constitutional even though that additional conduct did not give rise to the claims. *Id.* at 46-47, 53-54. Taken together, the

defendant's broadcasts caused harm in Texas, and its additional conduct showed that it had purposefully availed itself of the Texas market. *Id.* at 54.

So too here. The State's claims have two essential components: that Google (1) collects Texans' personal information for its own profit, 2.SuppCR.19-23, 64-73 (App.38-42, 83-92), while (2) misrepresenting to those same Texans that they can control what data Google collects, 2.SuppCR.23-61 (App.42-80). Google "can track the precise location of a device and its owner on a continuous basis" through information collected by "sensors" on Android devices and "transmitted by the device to Google." 2.SuppCR.20 (App.39). Google's platform-agnostic software and services, such as YouTube and Chrome, allow Google to "collect[] and store[] users' location data ... even when a user's location is not needed to support" that service's "core functionality." 2.SuppCR.20-21 (App.39-40). Google often enables this data collection by default through multiple settings at the device- and account-level that operate independently, and some forms of data collection cannot be disabled by Texans. 2.SuppCR.21 (App.40).

Meanwhile, Google misleads users as to how these settings function. For example, Google's description of its Location History setting told users that with the "Location History" setting turned off, "the places you go are no longer stored" and no "new location information" will be stored. 2.SuppCR.28 (App.47) (emphasis omitted). But that description did not disclose that *another* account setting—Web & App Activity—independently allowed Google to track their location anyway.

2.SuppCR.29, 32 (App.48, 51). Moreover, Google enables Web & App Activity “by default” despite its “privacy-intrusive” nature, yet Google does not disclose its location-tracking functionality to users when they first encounter the setting during account creation. 2.SuppCR.29-30, 44-45 (App.48-49, 63-64). Any number of Texans have therefore used their Android devices and other Google services believing their location to remain private by turning off one setting, all the while broadcasting their every move to Google by failing to turn off another.

Finally, all of this conduct serves Google’s Texas business. Rather than charge users directly, Google makes much of its money by “collect[ing] exhaustive personal data about its users,” “process[ing] this data to draw inferences about individuals and groups of users” and “monetiz[ing]” that information “through advertising and other business-facing services.” 2.SuppCR.21 (App.40). Location data, for example, can increase advertising revenue by “a double-digit percentage,” 2.SuppCR.22 (App.41), partly because Google can link advertisements Texans see with the stores they physically visit, 2.SuppCR.24 (App.43).

These facts easily establish jurisdiction over Google. Even if Google drafts its misrepresentations elsewhere, it delivers them in Texas whenever Texans look at the settings on their Android phones or Google accounts. *E.g.*, 2.SuppCR.23, 32-33 (App.42, 51-52) (pop-up window and settings pane). And the data collection that *renders* Google’s disclosures misleading occurs in Texas every time Google recovers personal data from Texans to support its business. *E.g.*, 2.SuppCR.21-23 (App.40-

42). Google even has offices, data centers, and electronic infrastructure in Texas, all of which serve its business here. *See, e.g.*, 3.SuppSCR.19-31, 69-70, 191, 193-94, 198. Under *Ford* and *TV Azteca*, these facts establish ample contacts between Google and Texas that relate directly to the State’s claims. Nor can Google seriously contest that it had adequate notice that it might be subject to a Texas court to the extent its course of conduct violates Texas law.

Google argued, and the Thirteenth Court agreed, that the only relevant conduct are Google’s (inadequate) disclosures, which were purportedly generated outside Texas and placed on a website viewed in Texas only because Google’s users wandered there. *E.g.*, Br. of Appellant Google LLC at 27, *Google LLC v. State*, No. 13-23-00114-CV (Tex. App.—Corpus Christi–Edinburg June 12, 2023); App.20-21 & n.3. Even leaving aside that the Thirteenth Court was required to view the record favorably to the trial court’s holding, *Volkswagen*, 669 S.W.3d at 411, that myopic approach cannot be squared with *Ford* or *TV Azteca*. It ignores that Google’s misrepresentations served Google’s *location*-based advertising business *in Texas* and helped Google generate “hundreds of millions” of dollars here. *E.g.*, 2.SuppCR.13, 22-23 (App.32, 41-42). Google is no mere passive recipient of data from Texans who happen to leave certain settings turned on; it actively seeks that information from Texans to serve its Texas business, and it misleads Texans to achieve its gains. *Supra* 3-5, 11-12.

Nor did the Thirteenth Court adequately address *Ford*. App.20-21 & n.3. It distinguished *Ford* because Ford’s cars caused injury in the forum states, while here the “injury” stems from misrepresentations crafted elsewhere. *Id.* But that analysis ignores that Texans’ information is siphoned *from their devices in Texas* based on misrepresentations they *received in Texas*. *Supra* 11-13. Moreover, the Supreme Court found jurisdiction over Ford even though no party disputed that the cars at issue reached the forum states only through secondary sales. *Ford*, 592 U.S. at 357, 366. That reasoning undercuts Google’s “wandering plaintiff” arguments raised below. Nor is there any credible argument that Google does not intentionally target Texans because *location* data is one of the key types at issue. That Google similarly targets users in other states does not diminish Google’s contacts with Texas. *See Volkswagen*, 669 S.W.3d at 406.

Moreover, the decision below gives foreign defendants a roadmap to violate Texas consumer-protection laws with impunity. Texas seeks to enforce the DTPA—a statute on the books for decades that specifically empowers OAG to protect Texans from deception. Tex. Bus. & Com. Code Ann. §§ 17.47(a), (e), 17.60, 17.61. The State’s claims fall squarely within that statute’s purview. 2.SuppCR.16-17 (App.35-36).⁸ If the State cannot sue Google in Texas for its violations of Texas law against

⁸ In its special-appearance response, the State estimated Texas Google users at over 26 million and further estimated that over half a million Texans bought and used Pixel phones designed by Google, many of which were sold by Google directly to Texans. *See* SCR.1388. Even were the State’s Petition insufficient (and it is not), these additional details established specific jurisdiction and should have been considered. *Infra* 18-19.

Texans, that raises the strange prospect of Texas suing in a California court to ask that court to interpret and enforce a Texas statute. The decision below therefore threatens to immunize Google—and any other technology company paying attention—from any liability for its deceptive, lucrative data-harvesting business in Texas so long as it avoids drafting its misrepresentations here.

Nor are Google’s violations of Texas law mere technicalities. With the information Google collects from Texans, it can infer extensive details about them: their “political or religious affiliation, sexual orientation, income, health status, and participation in support groups” as well as other personal life events such as marriage, divorce, or childbearing. 2.SuppCR.12, 29 (App.31, 48). Under the decision below, Google can run a private surveillance state over Texans for its own profit and cannot be held liable in Texas courts merely because *part* of that operation occurs elsewhere. That is not, nor should it be, the law in Texas.

It certainly is not the law elsewhere. Google has faced similar claims in other states, and Google’s personal-jurisdiction defense has been rejected by both courts that addressed it. *See generally* Order Den. Google LLC’s Mot. to Dismiss, *Washington v. Google LLC*, No. 22-2-01103-3 SEA (Wash. Super. Ct. May 20, 2022); Order, *District of Columbia v. Google LLC*, No. 2022 CA 000330 B (D.C. Super. Ct. Aug. 31, 2022). If the opinion below is left in place, Texas will be the only state that has forced its Attorney General to ask California to protect Texans.

B. The opinion below also flouts *Volkswagen*.

Even if the Thirteenth Court correctly focused solely on Google’s supposedly-out-of-state misrepresentations, its decision still flouts this Court’s decision in *Volkswagen*. There, the State sought to hold foreign vehicle manufacturers liable for surreptitiously installing emissions-beating software and parts onto vehicles in Texas in violation of Texas law. 669 S.W.3d at 405, 410-11. Although the manufacturers created the software at issue, knew it would be installed in Texas cars, and drafted the misrepresentations that misled car owners to install it, the court of appeals held that the manufacturers were not subject to personal jurisdiction largely because that conduct all occurred abroad and they had acted in Texas only through subsidiaries. *Volkswagen Aktiengesellschaft v. State*, 665 S.W.3d 22, 28-29, 32-34, 36-38 (Tex. App.—Austin 2020).

This Court reversed. The core of personal jurisdiction lay in “implied consent—that by invoking the benefits and protections of a forum’s laws, a nonresident consents to suit there.” *Volkswagen*, 669 S.W.3d at 426 (citation omitted). To avoid jurisdiction, therefore, a party cannot concoct artificial barriers between itself and Texas but must instead “structur[e] its transactions” so as to avoid “profit[ing] from the forum’s laws.” *See id.* (citation omitted). The foreign manufacturers failed to do so when they were ultimately responsible for the software installed on cars in Texas, when they benefitted from that installation in Texas, and when Texas was a substantial market for their cars. *Id.* at 426-27. Nor did the Court have trouble finding

that the manufacturers' contacts related to the State's claims, both because the claims targeted the manufacturers' conduct and because the State had a "strong interest in protecting its regulatory scheme." *Id.* at 431-32.

So too here. Google collects Texans' private information to benefit its profitable *location*-based advertising business *in Texas*, and Google's misleading explanations about how its various settings and services function are just one part of the scheme. *Supra* 4-5, 11-12. Similarly, Google runs its profitable data analytics business by siphoning personal data from Texans while misleading users about Incognito Mode's privacy features. *E.g.*, 2.SuppCR.53-55, 64-65, 73 (App.72-74, 83-84, 92).

Under *Volkswagen*, these Texas contacts more than suffice. Even if Google's misrepresentations originated outside Texas—which the State does not admit—Google's use of them *in Texas* to dupe *Texans* into disclosing personal information that Google collects *in Texas* to fuel location-targeted advertising revenue *from Texans in Texas* represent substantial, intentional contacts between Google and Texas. And because the State's claims relate to those exact contacts, *Volkswagen* establishes that Google can be haled into a Texas court.

The Thirteenth Court reached the opposite conclusion by focusing (at Google's request) solely on the out-of-state location of the employees who are supposedly responsible for Google's misrepresentations. App.20-21. But *Volkswagen* does not require a defendant to have any Texas employees. Just the opposite: the

foreign manufacturers were subject to personal jurisdiction even though they developed both their software and misrepresentations in Germany and even though they directed the software and misrepresentations to Texas through a third party. *Volkswagen*, 669 S.W.3d at 414-15. What mattered was that the foreign manufacturers sought to profit by targeting Texas car owners and that the State's claims related to that conduct. *Id.* at 426, 431-32.

So too here. Google reaps substantial revenue in Texas from the very data it takes from Texas and misleads Texans to disclose. *E.g.*, 2.SuppCR.19-22 (App.38-41). Regardless of where they are drafted, Google's misrepresentations are received by Texans in Texas to fuel Google's location-based advertising and data analytics profits from Texans in Texas. It is difficult to imagine a clearer case for personal jurisdiction over Google.

II. The Court Should Grant the Petition to Clarify the Scope of Review for a Special Appearance.

The Court should also grant review to address whether the State's subsequent clarifications satisfied its burden. Among other things, the State's special-appearance response provided evidence that Google not only loads its software onto phones sold in Texas but also actively markets and sells its *own* mobile devices here. *See* SCR.1384, 1388-89; 3.SuppSCR.309-10, 312, 319-20. Those allegations would cover any conceivable gap in the State's allegations. But the Thirteenth Court relied only on narrow parts of the State's Petition. App.18-19. And because courts are split over

whether additional details may be considered when raised in a response to a special appearance, the Court should clarify that standard here.

The pleadings' importance in the special-appearance analysis is clear. *See, e.g., Kelly v. Gen. Interior Constr., Inc.*, 301 S.W.3d 653, 658 (Tex. 2010) (a “defendant’s ... burden to negate jurisdiction is tied to the allegations in the plaintiff’s pleading”). But courts of appeals are split over whether a trial court may consider jurisdictional allegations in a special-appearance *response*. *See Gaddy v. Fenenbock*, 652 S.W.3d 860, 871 n.5 (Tex. App.—El Paso 2022, no pet.) (recognizing split). The First, Second, Ninth, and Fourteenth courts of appeals say yes.⁹ The en banc Fifth Court of Appeals says no.¹⁰ The Eighth Court of Appeals has declined to decide “whether the jurisdictional allegations are limited to the plaintiff’s petition.”¹¹

The Court should determine whether and to what extent allegations in a special-appearance response can supplement or clarify allegations in an operative pleading.

⁹ *See, e.g., Auto-Owners Ins. Co. v. Millionder*, No. 01-24-00221-CV, 2025 WL 375847, at *6 & n.10 (Tex. App.—Houston [1st Dist.] Feb. 4, 2025, no pet. h.) (mem. op.); *Stanger v. Loetzerich*, No. 14-21-00504-CV, 2023 WL 2884409, at *5 (Tex. App.—Houston [14th Dist.] Apr. 11, 2023, no pet.) (mem. op.); *Graves v. DJO, LLC*, 636 S.W.3d 321, 325, 329 (Tex. App.—Fort Worth 2021, pet. denied); *JPMorgan Chase Bank, N.A. v. Campbell*, No. 09-20-00161-CV, 2021 WL 2583573, at *4 (Tex. App.—Beaumont June 24, 2021, no pet.) (mem. op.).

¹⁰ *See Steward Health Care Sys. LLC v. Saidara*, 633 S.W.3d 120, 129 (Tex. App.—Dallas 2021, no pet.) (en banc).

¹¹ *Gaddy*, 652 S.W.3d at 871 n.5.

PRAYER

The Court should grant this petition, reverse the judgment below, and remand for trial.

Dated: February 24, 2025

KRISTINA WILLIAMS
State Bar No. 24078303
Norton Rose Fulbright US LLP
2200 Ross Avenue, Suite 3600
Dallas, Texas 75201
Tel.: (214) 855-8000

Respectfully submitted.

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

AARON L. NIELSON
Solicitor General

/s/ Jacob C. Beach

JACOB C. BEACH
Assistant Solicitor General
State Bar No. 24116083
Jacob.Beach@oag.texas.gov

Office of the Attorney General
P.O. Box 12548 (MC 059)
Austin, Texas 78711
Tel.: (512) 936-1700
Fax: (512) 474-2697

Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

Microsoft Word reports that this brief contains 4,495 words, excluding emptied text.

/s/ Jacob C. Beach

Jacob C. Beach

No. ____

In the Supreme Court of Texas

THE STATE OF TEXAS,

Petitioner,

v.

GOOGLE LLC,

Respondent.

On Petition for Review
from the Thirteenth Court of Appeals, Corpus Christi–Edinburg

APPENDIX

Tab

1. Order Denying Google’s Verified Amended Special Appearance
(February 22, 2023) (CR.1233) A
2. Thirteenth Court of Appeals’ Opinion (January 9, 2025).....B
3. Thirteenth Court of Appeals’ Judgment (January 9, 2025) C
4. Plaintiff’s First Amended Petition (2.SuppCR.6-79)..... D

**Tab A: Order Denying Google's Verified Amended Special
Appearance (February 22, 2023) (CR.1233)**

FILED

CAUSE NO. 22-01-88230-D

2023 FEB 22 AM 10:40

THE STATE OF TEXAS,
Plaintiff,

§
§
§
§
§
§
§

IN THE DISTRICT COURT OF

Cheryl A. ...
DISTRICT CLERK

v.

VICTORIA COUNTY, TEXAS

GOOGLE LLC,
Defendant

377th JUDICIAL DISTRICT

~~PROPOSED~~ ORDER DENYING
GOOGLE'S VERIFIED AMENDED SPECIAL APPEARANCE

This matter came before the undersigned Judge on Google LLC's VERIFIED AMENDED SPECIAL APPEARANCE (the "Special Appearance"). After considering the Special Appearance, The State of Texas' Response, Google LLC's Reply, and arguments of counsel, if any, the Court is of the opinion that the Special Appearance should be DENIED.

This Court finds that it has personal jurisdiction over the Defendant, Google, LLC. The Court will issue a separate scheduling order regarding the trial date and other applicable court deadlines.

Signed this the 22nd day of February, 2023.

[Signature]

Judge Presiding

**Tab B: Thirteenth Court of Appeals' Opinion
(January 9, 2025)**



NUMBER 13-23-00114-CV

COURT OF APPEALS

THIRTEENTH DISTRICT OF TEXAS

CORPUS CHRISTI – EDINBURG

GOOGLE LLC,

Appellant,

v.

THE STATE OF TEXAS,

Appellee.

**ON APPEAL FROM THE 377TH DISTRICT COURT
OF VICTORIA COUNTY, TEXAS**

MEMORANDUM OPINION

**Before Chief Justice Tijerina and Justices Silva and Peña
Memorandum Opinion by Chief Justice Tijerina**

This appeal is from the denial of a special appearance filed by appellant Google LLC. Appellee the State of Texas filed suit against appellant under the Texas Deceptive Trade Practices Act (DTPA) on its own behalf seeking civil penalties for alleged representations and omissions on appellant's website and software that are accessible nationwide. See TEX. BUS. & COM. CODE ANN. § 17.41 et seq. By three issues, Google

contends that the trial court erred in denying its special appearance because there is neither general nor specific jurisdiction in Texas, and traditional notions of fair play and substantial justice do not support the exercise of personal jurisdiction in Texas. We reverse and render.

I. STANDARD OF REVIEW AND APPLICABLE LAW

Subject-matter jurisdiction is essential to the authority of a court to decide a case. *Bland Indep. Sch. Dist. v. Blue*, 34 S.W.3d 547, 554–55 (Tex. 2000). A special appearance is a dilatory plea that challenges the trial court’s subject-matter jurisdiction without regard to whether the asserted claims have merit. *Harris County v. Sykes*, 136 S.W.3d 635, 638 (Tex. 2004). Whether the trial court has personal jurisdiction over a defendant is a question of law. *BMC Software Belg., N.V. v. Marchand*, 83 S.W.3d 789, 794 (Tex. 2002). Thus, we review the trial court’s ruling on a special appearance *de novo*. *Id.* The trial court determines the special appearance by referring to the pleadings, any stipulations made by and between the parties, any affidavits and attachments filed by the parties, discovery, and any oral testimony. TEX. R. CIV. P. 120a(3). Because the question of a court’s exercise of personal jurisdiction over a nonresident defendant is one of law, we review a trial court’s determination of a special appearance *de novo*. *Moki Mac River Expeditions v. Drugg*, 221 S.W.3d 569, 574 (Tex. 2007); *BMC Software Belg.*, 83 S.W.3d at 793.

Where, as here, the trial court does not issue findings of fact and conclusions of law, all facts necessary to support the judgment and supported by the evidence are implied, and we presume that the trial court resolved all factual disputes in favor of its

ruling. *BMC Software Belg.*, 83 S.W.3d at 795; *Am. Type Culture Collection v. Coleman*, 83 S.W.3d 801, 805–06 (Tex. 2002). These implied findings are not conclusive and may be challenged for legal and factual sufficiency if the appellate record includes the reporter’s and clerk’s records. *BMC Software Belg.*, 83 S.W.3d at 795.

Texas courts may assert personal jurisdiction over a nonresident if (1) the Texas long-arm statute authorizes the exercise of jurisdiction, and (2) the exercise of jurisdiction is consistent with federal and state constitutional due-process guarantees. *Moki Mac*, 221 S.W.3d at 574; *Gray, Ritter & Graham, PC v. Goldman Phipps PLLC*, 511 S.W.3d 639, 654 (Tex. App.—Corpus Christi—Edinburg 2015, pet. denied). The Texas long-arm statute allows Texas courts to exercise personal jurisdiction over a nonresident defendant that “does business” in Texas. See TEX. CIV. PRAC. & REM. CODE ANN. § 17.042; *BMC Software Belg.*, 83 S.W.3d at 795. The Texas long-arm statute sets out several activities that constitute “doing business” in Texas; however, the list is not exclusive, and Texas’s long-arm statute’s “broad language extends Texas courts’ personal jurisdiction ‘as far as the federal constitutional requirements of due process will permit.’” *Id.* (quoting *U-Anchor Adver., Inc. v. Burt*, 553 S.W.2d 760, 762 (Tex. 1977)). Therefore, “the requirements of the Texas long-arm statute are satisfied if the exercise of personal jurisdiction comports with federal due process limitations.” *CSR Ltd. v. Link*, 925 S.W.2d 591, 594 (Tex. 1996).

Under the Due Process Clause of the Fourteenth Amendment of the United States Constitution, a Texas court has personal jurisdiction over a nonresident defendant when (1) the nonresident defendant has established minimum contacts with the forum state, and (2) the exercise of jurisdiction does not offend “traditional notions of fair play and

substantial justice.” *Int’l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945); *BMC Software Belg.*, 83 S.W.3d at 795; see U.S. CONST. amend. XIV, § 1. “The exercise of personal jurisdiction is proper when the contacts proximately result from actions of the nonresident defendant which create a substantial connection with the forum state.” *Guardian Royal Exch. Assurance, Ltd. v. Eng. China Clays, P.L.C.*, 815 S.W.2d 223, 226 (Tex. 1991).

The plaintiff bears the initial burden of pleading “sufficient allegations to bring a nonresident defendant within the provisions of the [Texas] long-arm statute.” *BMC Software Belg.*, 83 S.W.3d at 793. The Texas long-arm statute authorizes the exercise of jurisdiction over a nonresident defendant doing business in Texas. TEX. CIV. PRAC. & REM. CODE ANN. §§ 17.041–.045. Texas’s long-arm statute provides:

In addition to other acts that may constitute doing business, a nonresident does business in this state if the nonresident:

- (1) contracts by mail or otherwise with a Texas resident and either party is to perform the contract in whole or in part in this state;
- (2) commits a tort in whole or in part in this state; or
- (3) recruits Texas residents, directly or through an intermediary located in this state, for employment inside or outside this state.

Id. § 17.042.

Once the plaintiff pleads sufficient allegations to bring a nonresident defendant within the provisions of the Texas long-arm statute, the burden is on the defendant to challenge personal jurisdiction by filing a special appearance negating all bases of personal jurisdiction asserted by the plaintiff in its pleading. *Moki Mac*, 221 S.W.3d at 574;

BMC Software Belg., 83 S.W.3d at 793; *El Puerto de Liverpool, S.A. de C.V. v. Servi Mundo Llantero, S.A. de C.V.*, 82 S.W.3d 622, 628 (Tex. App.—Corpus Christi—Edinburg 2002, pet. dism'd w.o.j.).

The defendant's contacts with the forum state may establish either specific or general jurisdiction over the nonresident defendant. *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 414 (1984). General jurisdiction allows for the nonresident defendant to be sued in the forum state for all claims even if the claims are not related to the nonresident defendant's activities in that state. *BMC Software Belg.*, 83 S.W.3d at 796. In other words, the defendant is treated as if the defendant's contacts with the forum state have been so constant, the defendant has been essentially rendered "at home" in the forum state, which is the equivalent to the defendant either having a principal place of business in the forum state or being incorporated there. See *BNSF Ry. Co. v. Tyrrell*, 581 U.S. 402, 406 (2017); *Daimler AG v. Bauman*, 571 U.S. 117, 127 (2014).

Specific jurisdiction over the nonresident defendant is present if the defendant purposefully directed his activities at residents of Texas and the litigation arose from or related to those contacts. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 472 (1985); *Helicopteros Nacionales de Colombia, S.A.*, 466 U.S. at 414; *Guardian Royal Exch. Assurance, Ltd.*, 815 S.W.2d at 227.

Even if the nonresident defendant has purposefully availed himself of personal jurisdiction in Texas, we must also conclude that the defendant's liability arises from or is substantially connected to those contacts. See *Burger King*, 471 U.S. at 472; *Helicopteros Nacionales de Colombia, S.A.*, 466 U.S. at 414; *Guardian Royal Exch. Assurance, Ltd.*,

815 S.W.2d at 226. Thus, we review the substantial connection between the operative facts of the litigation based on the claims involved in the litigation and the defendant's contacts with Texas. *Retamco Operating, Inc. v. Republic Drilling Co.*, 278 S.W.3d 333, 340 (Tex. 2009).

II. GENERAL JURISDICTION

By its first issue, appellant contends that appellee failed to establish that it is “at home” in Texas; therefore, there is no evidence of general jurisdiction.

A. Applicable Law

General or all-purpose personal jurisdiction requires that a defendant be “essentially at home” in the forum state. *State v. Volkswagen Aktiengesellschaft*, 669 S.W.3d 399, 412 (Tex. 2023) (quotation marks omitted). “This kind of personal jurisdiction allows courts to render a binding judgment against a defendant even if the plaintiff's claims neither arise from activities conducted in the forum state nor relate to the forum state or the defendant's activity there.” *Id.* (cleaned up). Under general jurisdiction, the cause of action “may concern events and conduct anywhere in the world.” *Id.* (quotation marks omitted).

Specific jurisdiction requires that the operative facts of the defendant's acts relate to the plaintiff's claims; general jurisdiction allows a defendant to be sued “on any and all claims against it, wherever in the world the claims may arise.” *Daimler AG*, 571 U.S. at 121. In other words, under general jurisdiction, there is no need to tie the defendant's acts with the plaintiff's claims. *Id.* at 132 (“[A] corporation's ‘continuous activity of some sorts within a state is not enough to support the demand that the corporation be amenable to

suits unrelated to that activity.”); see also *Grupo Mex. S.A.B. de C.V. v. Mt. McKinley Ins. Co. and Everest Reinsurance Co.*, No. 13-17-00134-CV, 2020 WL 486501, at *4 (Tex. App.—Corpus Christi—Edinburg Jan. 30, 2020, pet. denied) (mem. op.) (“General jurisdiction, on the other hand, does not require a nexus between the defendant’s in-state contacts and the plaintiff’s claim; instead, the focus is solely on the defendant’s contacts with the forum.”). We must only focus on the defendant’s contacts with the forum state. See *Helicopteros Nacionales de Colombia, S.A.*, 466 U.S. at 414; see also *Grupo Mex.*, 2020 WL 486501, at *4.

B. Discussion

Appellant contends that it met its burden to negate general jurisdiction because “the undisputed facts confirm that this is not an exceptional case for general jurisdiction.” Specifically, appellant argues that its “operations in Texas represent a small fraction of its operations across the country and across the world” because it employs 58,500 people in California and 169,000 people worldwide, while in contrast it has a total of 2,400 permanent employees in Texas. Appellant states that even considering its temporary employees, interns, advisers, vendors, and other miscellaneous employees which total approximately 5,500 employees in Texas, its number of employees in Texas is not enough to support a conclusion that appellant is “essentially at home” in Texas. In addition to tying appellant to Texas based on appellant’s 5,500 Texas employees, appellee claims that general jurisdiction applies because appellant has one of its four data centers in

Texas.¹ According to appellee, “Texas accounts for approximately 8.9%” of appellant’s U.S. revenue and 4% of its worldwide revenue. Thus, appellee argues that general jurisdiction over appellant exists due the number of employees appellant has in Texas, the fact that appellant has one of four data centers in Texas, and 8.9% of appellant’s revenue in the United States and 4% of its worldwide revenue is made in Texas.

In *BNSF Ry.*, the United States Supreme Court stated that under general jurisdiction principles, its due process precedent under the Fourteenth Amendment does not support for “a State to hale an out-of-State corporation before its court when the corporation is not ‘at home’ in the State” 581 U.S. at 405–06. The Court explained that “[t]he ‘paradigm’ forums in which a corporate defendant is ‘at home’ . . . are the corporation’s place of incorporation and its principal place of business.” *Id.* at 413. However, only in an “exceptional case,” the Court explained could “a corporate defendant’s operations in another forum” be “so substantial and of such a nature as to render the corporation at home in that State.” *Id.* The Court cited *Perkins v. Benguet Consol. Mining Co.*, as being one such exceptional case. 342 U.S. 437, 447–48 (1952). In that case, the corporation was forced by war “to temporarily relocate the enterprise from the Philippines to Ohio.” *BNSF Ry.*, 581 U.S. at 413. Therefore, according to the United States Supreme Court, Ohio had general jurisdiction over the defendant corporation “[b]ecause Ohio then became ‘the center of the corporation’s wartime activities.’” *Id.* In *Daimler AG*, the United States Supreme Court clarified that it has

¹ According to appellee, appellant has 250 employees at the Texas data center.

“declined to stretch general jurisdiction beyond limits traditionally recognized” in *Perkins*. 571 U.S. at 132.

The *BNSF Ry.* Court emphasized that the defendant was not amenable to general jurisdiction because it had not been incorporated in the forum State and did not maintain a principal place of business there. *BNSF Ry.*, 581 U.S. at 414. The Court noted that the defendant corporation, BNSF, had over 2,000 miles of railroad track and more than 2,000 employees in the forum state; however, general jurisdiction analysis “does not focus solely on the magnitude of the defendant’s in-state contacts.” *Id.* The activities of the defendant must amount to having its principal place of business in the forum state. See *id.*

Here, it is undisputed that appellant is not incorporated in Texas and does not maintain a principal place of business there. See *id.* at 413. “Those affiliations have the virtue of being unique—that is, each ordinarily indicates only one place—as well as easily ascertainable.” *Daimler AG*, 571 U.S. at 137. Additionally, allegations that the defendant maintains in-state business alone does not suffice to subject a corporation to general jurisdiction. See *id.* at 137–38. The United States Supreme Court rejected the argument that a State has general jurisdiction over that defendant because the defendant conducts some business in that state. See *id.* The Court stated, “Plaintiffs would have us look beyond the exemplar bases [such as having a principal place of business in the state or being incorporated in the states as] *Goodyear* identified, and [instead] approve the exercise of general jurisdiction in every State in which a corporation ‘engages in a substantial, continuous, and systematic course of business’”; however, “[t]hat

formulation . . . is unacceptably grasping.” *Id.* (discussing *Goodyear Dunlop Tires Ops., S.A. v. Brown*, 564 U.S. 915, 919, 924 (2011)).

The United States Supreme Court explained that “the words ‘continuous and systematic’ were used in *International Shoe* to describe situations in which the exercise of specific jurisdiction would be appropriate.” *Id.* at 138. Instead, the proper question in a general jurisdiction analysis is: “whether [a foreign] corporation’s ‘affiliations with the State are so continuous and systematic as to render [it] essentially at home in the forum State.’” *Id.* at 138–39 (internal quotations omitted).

In *Perkins*, the defendant admittedly and indisputably moved its principal place of business to Ohio; that is not the case here. *See id.*; *see also BNSF Ry.*, 581 U.S. at 413; *Daimler AG*, 571 U.S. at 132 (setting out that “the placement of a product into the stream of commerce ‘may bolster an affiliation germane to *specific* jurisdiction,” but “such contacts ‘do not warrant a determination that, based on those ties, the forum has *general* jurisdiction over a defendant”). Appellant has not temporarily relocated its business to Texas, and we find no authority supporting a conclusion that it is sufficient to find general jurisdiction based merely on appellant conducting the amount of business it performs in Texas or employing its number of employees in Texas. Thus, we are not persuaded that appellant’s contacts with Texas are sufficient to find under guiding precedent that appellant is “essentially at home” in Texas. *See BNSF Ry.*, 581 U.S. at 413; *see also Daimler AG*, 571 U.S. at 129 (explaining that *Perkins* “remains the textbook case of general jurisdiction appropriately exercised over a foreign corporation that has not consented to suit in the forum”) (internal quotations omitted). To subject appellant to

general jurisdiction in Texas, would allow that appellant “be sued on any and all claims against it [in Texas], wherever in the world the claims may [have] arise[n]” because its business in Texas equates with it having its principal place of business in Texas. See *Daimler AG*, 571 U.S. at 121. The crux of *Perkins*, according to the United States Supreme Court, is that Ohio, the forum state, had become “the corporation’s principal, if temporary, place of business.” *Daimler AG*, 571 U.S. at 130 (citing *Keeton v. Hustler Mag., Inc.*, 465 U.S. 770, 780, n.11 (1984)). Here, that is not the case; it is undisputed that appellant has not made Texas its temporary principal place of business and appellee has not made such a claim. Furthermore, we are without authority to support a conclusion that appellant’s business dealings as previously set out above in Texas have in essence made Texas its principal place of business. See *id.* We agree with appellant that general jurisdiction requires that the out-of-state corporate defendant’s in-state activities be equivalent to the defendant incorporating or establishing a principal place of business in the forum that is rendering them “essentially home in the forum state.” See *Goodyear*, 564 U.S. at 919, 924; *Volkswagen*, 669 S.W.3d at 412; see also *Grupo Mex.*, 2020 WL 486501, at *4. The small percentage of business that appellant performs in Texas as alleged by appellee does not even amount to substantial, continuous, and systematic contacts, but even if it does, the United States Supreme Court has disavowed that rubric as the proper measure of analyzing general jurisdiction. See *Goodyear*, 564 U.S. at 919, 924; *Volkswagen*, 669 S.W.3d at 412; see also *Grupo Mex.*, 2020 WL 486501, at *4. Instead, general jurisdiction analysis “calls for an appraisal of a corporation’s activities in their entirety, nationwide and worldwide.” See *Daimler AG*, 571 U.S. at 139 n.20. From

our appraisal of the record before us, appellant’s activity in Texas compared with its nationwide and worldwide activity does not support a conclusion that appellant has made Texas its home. See *id.* Appellee’s allegations are insufficient to meet its initial burden. Moreover, without more, these allegations effectively negate the trial court’s general jurisdiction. Appellant cannot be “essentially at home” in every foreign jurisdiction where it operates. See *BNSF Rye.*, 581 U.S. at 413; *Daimler AG*, 571 U.S. at 139 & n.20; *Goodyear*, 564 U.S. at 919; *Perkins*, 342 U.S. at 447–48; see also *Grupo Mex.*, 2020 WL 486501, at *6.

Therefore, we conclude that appellant negated general jurisdiction in Texas under these facts and that the trial court should have granted its special appearance on general jurisdiction grounds. See *Daimler AG*, 571 U.S. at 132 (“[A] corporation’s ‘continuous activity of some sorts within a state is not enough to support the demand that the corporation be amenable to suits unrelated to that activity.’”). We sustain appellant’s first issue.²

² In its response to appellant’s special appearance, appellee lists all properties owned by appellant as evidence that general jurisdiction applies. Specifically, appellee lists the following:

- 800,000 square feet in the 35-floor Google Tower (Austin)
- The top 10 floors of the 500 West 2nd building (Austin)
- 150,000 square feet across all seven floors of a Saltillo building (Austin)
- 11,000 square feet in the One Buffalo Heights building (Houston)
- At least one office in Dallas, Texas (Dallas)
- A \$600 million data center (Midlothian)
- A planned \$600 million data center (Red Oak)
- A Google Fiber Kiosk (San Antonio)

III. SPECIFIC JURISDICTION

By its second issue, appellant contends that in its petition, appellee did not allege facts supporting a conclusion that Texas has specific jurisdiction over appellant and that it negated specific jurisdiction. Specifically, appellant argues that its contacts do not amount to purposeful availment and no substantial connection exists between its contacts with Texas and the operative facts of the litigation.

A. Applicable Law

Specific personal jurisdiction focuses on the defendant's connections with the state and its relationship to the plaintiff's claims. See *Volkswagen*, 669 S.W.3d at 412. In our specific-jurisdiction analysis we measure the two co-equal components of relatedness and purposeful availment. *Moki Mac*, 221 S.W.3d at 579. The relatedness inquiry defines "the appropriate 'nexus between the nonresident defendant, the litigation, and the forum.'" *Luciano v. SprayFoamPolymers.com, LLC*, 625 S.W.3d 1, 14 (Tex. 2021) (quoting *Moki Mac*, 221 S.W.3d at 579). "[T]he exercise of specific jurisdiction is prohibited if 'the suit' does not 'arise out of or relate to the defendant's contacts with the forum.'" *Id.* (alterations omitted). Thus, the lawsuit must arise from or relate to "some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws." *Id.* at 9 (citing *Hanson v. Denckla*,

• Additional Google offices (Addison)

However, as set out by the United States Supreme Court, we must appraise appellant's contacts in Texas by comparing them with appellant's nationwide and worldwide business. See *Daimler AG v. Bauman*, 571 U.S. 117, 139 n.20 (2014). And here there is no evidence that appellant's contacts in Texas are the same, equal to, or greater than its worldwide and nationwide contacts as to render Texas its principal place of business.

357 U.S. 235, 253 (1958)).

“The ‘touchstone of jurisdictional due process [is] ‘purposeful availment.’” *Id.* The defendant’s act in the forum state must amount to it purposefully availing “‘itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws.’” *Id.* (quoting *Hanson v. Denckla*, 357 U.S. 235, 253 (1958)). A defendant that has “‘deliberately’ engaged in significant activities within a state,” has “‘manifestly . . . availed himself of the privilege of conducting business there.’” *Id.* (quoting *Burger King*, 471 U.S. at 475–76 (cleaned up)). Therefore, because the defendant has availed itself of the “‘benefits and protections’ of the forum’s laws, it is ‘presumptively not unreasonable to require him to submit to the burdens of litigation in that forum as well.’” *Id.*

Whether the defendant has had minimum contacts with the forum state depends solely on the defendant’s acts within that state. *Id.* Additionally, “fortuitous” or “attenuated” contacts cannot “be relied upon to satisfy the requirements of due process.” *Id.* “Rather, whether due process is satisfied depends upon ‘the quality and nature of the activity in relation to the fair and orderly administration of the laws.’” *Id.* (quoting *Int’l Shoe*, 326 U.S. at 319).

Even when a defendant has had purposeful contacts with the forum states, “the exercise of specific jurisdiction is prohibited if ‘the *suit*’ does not aris[e] out of or relat[e] to the defendant’s contacts with the forum.” *Id.* at 14. This relatedness doctrine requires a nexus between the defendant’s contacts and the litigation and the forum. *Id.* There must be a “substantial connection” between the operative facts of the litigation and the

defendant's contacts with the state. *Id.* In other words, "there must be 'an affiliation between the forum and the underlying controversy, principally, [an] activity or an occurrence that takes place in the forum State and is therefore subject to the State's regulation.'" *Id.*

B. Relatedness

Appellant argues that we should begin our analysis of specific jurisdiction by examining the relatedness doctrine first. Appellant states, that appellee's "live petition identifies various general business contacts that Google has with Texas, which are insufficient to be 'at home' in the state and also wholly unrelated to this case." Appellant claims that "[e]ven a 'flood' of purposeful contacts with a forum state is irrelevant if 'the *suit*' does not 'arise out of or relate to the defendant's contacts with the *forum*.'" Because we agree with appellant, we will first analyze whether the contacts as alleged by appellee are related to the operative facts and the State of Texas. *See id.*

1. The Allegations

Appellee sued appellant pursuant to the DTPA. Appellee alleged that appellant has become one of the richest companies in the world, in part, by deceiving Texans and profiting off their confusion. Specifically, [appellant] has systematically misled, deceived, and withheld material facts from users in Texas about how and why their behavior is tracked and how to stop [appellant] from monetizing their personal data. As relevant to this Petition, [appellant]'s deceptive practices fall into two closely related buckets: tracking location history and tracking private-browsing activity.

Appellee accused appellant of deceiving Texas residents into believing that users can disable location tracking. In addition, appellee accused appellant of collecting Texas users browsing history, even when the users believe that they are not being tracked by

appellant because appellant claims that its users can go incognito, which appellee claims is a sham. According to appellee, appellant lies about how it tracks and collects data about its Texas users, and Texas residents are unaware of this deception. Appellee avers that appellant's deception to Texas users is motivated by appellant's desire for more profits from the information it gathers unbeknownst to its users. Appellee alleged that appellant misleads Texas users through both misrepresentations and omissions.

Appellee stated that appellant does the following:

[(1)] uses its window into millions of Texans' personal lives to sell "targeted" advertising designed to exert the maximum influence over those users. In so doing, the Company has reaped spectacular gains at the expense of Texans' privacy. Indeed, [appellant] has generated hundreds of millions—if not billions—of dollars of advertising revenues from ads presented to users in Texas alone.

. . . .

[(2)] has caused and will cause adverse effects to consumers in Texas, to legitimate business enterprises which lawfully conduct trade and commerce in this state, and to the State of Texas. Therefore, the Consumer Protection Division of the Office of the Attorney General of the State of Texas is of the opinion that these proceedings are in the public interest.

2. Discussion

To prevail, appellee must show that there is a "substantial connection" between appellant's contacts and the operative facts of the litigation." *Id.* If the focus of the trial involves facts that occur outside of the forum state, then the operative facts are not sufficiently related. *Moki Mac*, 221 S.W.3d at 585. Thus, if the events that took place outside of Texas would "consume most if not all of the litigation's attention" and "the overwhelming majority of the evidence [would] be directed" at events outside of Texas,

then the contacts are not sufficiently related to the litigation’s operative facts. *Id.* “[A] nonresident directing a tort at Texas from afar is insufficient to confer specific jurisdiction.” *Moncrief Oil Int’l Inc. v. OAO Gazprom*, 414 S.W.3d 142, 157 (Tex. 2013). In our analysis of the relatedness doctrine, we consider what the principal complaint involves. *TV Azteca v. Ruiz*, 490 S.W.3d 29, 53 (Tex. 2016).

Appellees do not specifically plead allegations that the operative facts of the litigation are related to appellant’s contacts with Texas. *See Luciano*, 625 S.W.3d at 8 (the plaintiff bears the initial burden to plead allegations sufficient to confer jurisdiction). Nonetheless, the evidence shows that appellant’s alleged contacts with Texas were made by appellant’s employees who were not in Texas. Appellee has not alleged that any of appellant’s Texas employees made the misleading statements. Thus, the evidence shows that appellant’s employees directed the alleged misleading statements from afar, which is insufficient to confer specific jurisdiction. *See Moncrief Oil Int’l Inc.*, 414 S.W.3d at 157. The principal complaint that the terms of service and disclosures made by appellant were misleading requires that the overwhelming evidence be directed at events outside of Texas.³ *Id.* Stated differently, appellee has not identified an “activity or

³ In *Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 592 U.S. 351, 365 (2021), the product that the defendant marketed in the forum state caused injury in that state. *See id.* The *Ford* court explained that the allegations that the products caused the plaintiffs’ injuries in the forum state was related to Ford’s activities of selling its products in the forum states and emphasized that the ads in the local media and in-state activities possibly caused the plaintiffs to purchase the vehicles. *Id.* at 367. Thus, the operative facts of the litigation regarding the plaintiff’s injuries occurring in the forum states were related to Ford’s activities in the forum states. *See id.* Here, appellee has not alleged that the product itself caused the injury. Instead, appellee asserts that appellant’s employees who were not in Texas caused the complained-of injuries while not in Texas. Thus, the operative facts all occurred outside of Texas, and we cannot conclude that under these facts, *Ford* applies. *See id.* at 366 (“That is why this Court has used this exact fact pattern (a resident-plaintiff sues a global car company, extensively serving the state market in a vehicle, *for an in-state accident*) as an illustration—even a paradigm example—of how specific jurisdiction works.” (emphasis

occurrence . . . that takes place in” Texas. See *Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 592 U.S. 351, 362 (2021) (cleaned up). Accordingly, we cannot conclude that appellee met its initial burden to show that appellant’s allegedly tortious conduct occurring outside of Texas is sufficient to confer specific jurisdiction over appellant. See *Moncrief Oil Int’l Inc.*, 414 S.W.3d at 157; see also *Ford Motor Co.*, 592 U.S. at 362 n.3 (rejecting the “view that a state court should have jurisdiction over a nationwide corporation . . . on any claim, no matter how unrelated to the State or [the corporation’s] activities there” and explaining that “[r]emoving the need for any connection between the case and forum State would transfigure our specific jurisdiction standard as applied to corporations”). We sustain appellant’s second issue.

IV. CONCLUSION

The trial court’s order denying the special appearance is reversed and judgment is rendered dismissing all of appellee’s claims against appellant for want of personal jurisdiction.

JAIME TIJERINA
Chief Justice

Delivered and filed on the
9th day of January, 2025.

added)).

**Tab C: Thirteenth Court of Appeals' Judgment
(January 9, 2025)**



THE THIRTEENTH COURT OF APPEALS

13-23-00114-CV

GOOGLE LLC
v.
THE STATE OF TEXAS

On Appeal from the
377th District Court of Victoria County, Texas
Trial Court Cause No. 22-01-88230-D

JUDGMENT

THE THIRTEENTH COURT OF APPEALS, having considered this cause on appeal, concludes the judgment of the trial court should be reversed and rendered. The Court orders the judgment of the trial court REVERSED and RENDERS judgment in accordance with its opinion. Costs of the appeal are adjudged against appellee.

We further order this decision certified below for observance.

January 9, 2025

**Tab D: Plaintiff's First Amended Petition
(2.SuppCR.6-79)**

CAUSE NO. 22-01-88230-D

THE STATE OF TEXAS, Plaintiff,	§	IN THE DISTRICT COURT OF
	§	
v.	§	VICTORIA COUNTY, TEXAS
	§	
GOOGLE LLC, Defendant	§	377 th JUDICIAL DISTRICT

PLAINTIFF’S FIRST AMENDED 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:

Table of Contents

I. INTRODUCTION 4

II. DISCOVERY CONTROL PLAN 11

III. PUBLIC INTEREST 11

IV. JURISDICTION 11

V. DEFENDANT..... 12

VI. VENUE 13

VII. TRADE AND COMMERCE 13

VIII. ACTS OF AGENTS..... 13

IX. NOTICE BEFORE SUIT 13

X. Factual Allegations 14

A. Google’s False, Misleading, and Deceptive Practices Regarding Location History..... 14

1. Google’s Business Model Relies on Constant Surveillance of Texans.....14

2. Google Cloaks Its Location Monitoring in a Web of Unrelated Settings.18

3. Google Deceives Users Regarding Their Ability to Protect Their Privacy Through
Google Account Settings.....22

4. Google Deceives Users Regarding Their Ability to Protect Their Privacy Through
Device Settings.36

5.	Google Deploys Deceptive Practices that Undermine Users’ Ability to Make Informed Choices About Their Data.....	39
<i>B.</i>	<i>Google’s False, Misleading, and Deceptive Practices Regarding Incognito Mode.....</i>	<i>48</i>
1.	Google Deceptively Represents that “Incognito Mode” Allows Texans to Control What Information Google Sends and Collects.	48
2.	Google’s Privacy Settings Deceptively Lead Texans to Believe They Can Prevent Google From Sending and Collecting Browsing Data.	51
3.	Google’s Private-Browser Cookies Deceptively Continue to Track and Send Data About a Texan’s Incognito Activity.....	54
4.	Internally, Google Recognizes the Deceptive Nature of Its Incognito Mode Representations.	57
5.	Google Uses Additional Data-Collection Tools to Collect and Store Data About Texans’ Incognito Sessions, and Incognito Deceptively Does Not Prevent This.	59
6.	Google Is Able to Unmask Texans By Combining Their Incognito Data with Additional Data.....	65
XI.	CAUSE OF ACTION	68
XII.	TRIAL BY JURY.....	72
XIII.	PRAYER FOR RELIEF	72

I. 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 and why their behavior is tracked and how to stop Google from monetizing their personal data. As relevant to this Petition, Google's deceptive practices fall into two closely related buckets: tracking location history and tracking private-browsing activity.

As to the former, 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 History" off means their location history is no longer tracked. But even with Location History off, Google deceptively continues to track users' location history unless they successfully navigate a counterintuitive labyrinth of seemingly unrelated settings. And even if a user does survive the Google gauntlet of privacy controls to disable all the appropriate location-related settings available to them, the Company *still* proceeds to determine that user's location using, among other things, IP-address, Device ID, and, if available, Cell Site Location Information. In other words, *no matter what actions a user takes*, Google continues to track a user's location, even after the user has expressly denied Google to the right to do so.

Location

- Precise location requested in OOBEE or elsewhere
 - "If I know where your device is, I can help you find stuff more easily. Can I have access to your device's location?"
 - If denied, GA will still use IP based locations
- Population area-based filter applied to Footprints & logs
- Used as normal in search paths

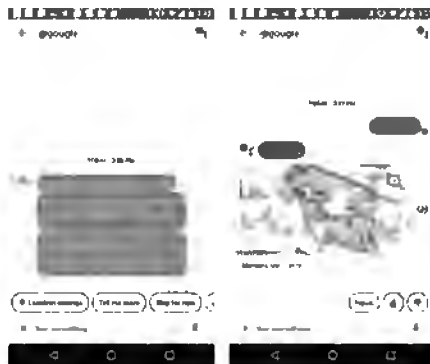


Figure 1. An exemplary internal Google presentation disclosing that Google will still track a user's location when the user denies Google permission to track device location.

As Google employees themselves have recognized, this is “[d]efinitely confusing from a user point of view.” Yet much of the deception relates to programs and practices that receive input straight from the top of the organization.

Sundar likes “coarsening” over time. Why not. Possible, but retention might be better.

Issues brought up by the article

- It's surprising that WAA contains locations
 - Imagine if Location History did not exist. It is surprising.
- LH does not disable all location histories
 - WAI. There are lots of “location histories”, like WAA, Fi, Photos. Probably others. Impossible to find them all and prevent new ones from being created. Recipe for disaster.
 - Infeasible to change. Infeasible to respect the LR setting control as required. LH not made to be a Google wide control, we don't want to force fit this to existing logging.
 - Solvable through messaging
-

Figure 2. An internal Google email noting Google CEO Sundar Pichai's express preferences on the granularity of location tracking.

Of course, Google’s deception does not stop with location tracking. Google also misleads users to believe that they have meaningful control over whether Google collects personal information during private-browsing sessions and what information is collected.

Texans engage in the Google-offered option of “private browsing”—known as Incognito mode—for a wide variety of legitimate purposes, including viewing highly personal websites that might indicate, for example, their medical history, political persuasion, or sexual orientation. Or maybe they simply want to buy a surprise gift without the gift recipient being tipped off by a barrage of targeted ads. Google, however, has misled such Texans to believe that they have meaningful control over whether Google collects personal information during so-called Incognito sessions. In reality, Google deceptively collects an array of personal data even when a user has engaged Incognito mode.

As with Google’s general approach to location tracking, Google provides a confusing selection of options that purportedly empower users to limit what data Google tracks. But these controls are not what they seem. Even when Texans follow each convoluted step they believe necessary to protect their data, Google still intercepts the sensitive information Texans seek to keep private. The end result is that Google misleads and deceives the Texans who trust Google when it insists that its privacy controls, features like Incognito mode, and supposed commitments to privacy are designed to give Texans control over when and how Google collects their data. In reality, these “controls,” features, and commitments are no more than a smokescreen—with Texans effectively unable to prevent Google from collecting their personal data.

One might wonder why it is so important to Google to mine its users’ personal information. The answer is simple: *Profit*.

The majority of Google’s revenues derive from business-facing services—namely, targeted advertising and advertising analytics. And to support this lucrative arm of its business, Google harvests location and other personal information, which Google uses both to market to its users and to evaluate the effectiveness of the advertisements it serves. *Profit* is also why Google represents to Texans that, for example, its Incognito mode allows users to “browse privately, [and] other people who use this device won’t see your history.”¹ Critically, Google omits from Incognito disclosure that it still collects a user’s personal information *even when the user has taken Google at its word and affirmatively elected to enable Incognito mode*.

Under this model, every Texan Google user is a potential unwitting profit center. As Google knows, location and other personal information are among the most sensitive and informative data the Company collects. Aggregated over time, this data paints an intimate mosaic that can effectively reveal a person’s identity and routines. Location and private browsing data, for example, can be used to infer an individual’s home address, political or religious affiliation, sexual orientation, income, health status, and participation in support groups. It can also suggest major life events, such as marriage, divorce, and the birth of children.

This information is even more powerful in the hands of Google due to the near ubiquity of Google products in users’ pockets, homes, and workplaces. The prevalence of Google technology allows the Company to derive detailed insights about users they may not even realize they have revealed—especially when Google misleads those users to believe they have disabled the collection of sensitive information.

¹ *How Private Browsing Works in Chrome*, GOOGLE CHROME HELP, <https://support.google.com/chrome/answer/7440301?hl=en&co=GENIE.Platform%3DAndroid>.

The upshot is that Google uses its window into millions of Texans’ personal lives to sell “targeted” advertising designed to exert the maximum influence over those users. In so doing, the Company has reaped spectacular gains at the expense of Texans’ privacy. Indeed, Google has generated hundreds of millions—if not billions—of dollars of advertising revenues from ads presented to users in Texas alone.

Google, therefore, has a powerful financial incentive to obscure the details of its location-tracking and Incognito-tracking practices and to make it difficult for users to opt out. Google’s ability to amass troves of data about its users as they move throughout Texas translates into improved advertising capabilities and an outsized share of the multibillion-dollar digital-advertising market.

Google’s incentive to cash in on the collection of Texans’ movements and browsing activity is inherently in conflict with its legal and ethical obligations as one of the world’s most powerful technology companies. Indeed, Google correctly admits that “[u]sers are not the experts in privacy and security, it’s actually Google,” and that “Google should be telling users what’s wrong, we should point out the anomalies, and guide users through their settings.”² Notwithstanding these acknowledgements, Google has long understood that its design choices deceive reasonable users. In one 2014 internal presentation, for instance, Google employees considered a specific scenario in which a Google user would reasonably be deceived by Google’s design choices. Google’s own internal example involved a hypothetical individual who “opted out of Google location” but then finds that, nevertheless, “Google maps has house-level accurate

² Lily Hay Newman, *The Privacy Battle to Save Google from Itself*, WIRED (Nov. 1, 2018), <https://www.wired.com/story/google-privacy-data/>.

location,” leaving the user wondering,—in Google’s words—“how does Google know my location? I thought I said no!”

Despite Google’s obvious understanding of its obligation to users and the ongoing risk of deception, the truth is that Google’s exhaustive surveillance practices are most effective and profitable to Google when users have no meaningful awareness of the intimate details they are sharing, how their data is used and monetized, and no clear idea of how to limit Google’s access to details about their personal lives. As such, when given a choice between (a) doing the right thing by its Texan users and (b) using false, deceptive, and misleading practices to fuel profits—Google ignores its obligations to Texans and chooses profits. And Google effectuates this decision through false and deceptive misrepresentations as well as omissions.

Google’s capturing of location data is demonstrated, for example, by an August 13, 2018, Associated Press (“AP”) article, which revealed that Google “records your movements even when you explicitly tell it not to.”³ The reporting concerned Google’s “Location History” setting, discussed above. As reported by the AP, Google had promised users that “with Location History off, the places you go are no longer stored.”⁴

That promise was false and deceptive. Specifically, even when users had explicitly opted out of location tracking through the Location History setting, Google nevertheless recorded users’ locations via other means, including (but not limited to) a separate and seemingly unrelated setting called “Web & App Activity.” When the Web & App Activity setting is enabled, Google collects and stores a large swath of data, including location data, whenever the user interacts with Google

³ Ryan Nakashima, *Google tracks your movements, like it or not*, AP NEWS (Aug. 13, 2018), <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb>.

⁴ *Id.*

products and services. Notably, the Web & App Activity setting is automatically enabled for all Google Accounts, yet Google’s disclosures during Google Account creation did not even mention the Web & App Activity setting until 2018.

In the days following the AP report, many users disabled one or both of these location-related settings, presumably having learned for the first time that Google was keeping an alarmingly meticulous record of their whereabouts over days, weeks, months, and years. Even Google employees expressed surprise upon learning that the Company was collecting location data under the auspices of the seemingly unrelated Web & App Activity setting.

Similar to its deceptive practices relating to the Web & App Activity setting, Google misleadingly and deceptively represents that, for example, its Incognito mode allows users to “browse privately, [and] other people who use this device won’t see your history.”⁵ Critically, however, Google fails to disclose that it *still* collects a user’s personal information even when the user has taken Google at its word and affirmatively elected to enable Incognito mode. As it turns out, unbeknownst to Texas users, no one is “incognito” to Google. Yet, Google continues to assure its users that “[y]ou’re in control of what information you share with Google.”⁶ These misleading representations and omissions about Incognito mode, like Google’s other deceptive practices, deceive Texans on the one hand but serve to maximize Google’s profits on the other.

Google’s statements about how to protect user privacy have all the reliability of the fox telling hens how to prevent fox intrusions. Google’s ambiguous, contradictory, and incomplete statements about these controls all but guarantee that users do not understand when their personal

⁵ *How Private Browsing Works in Chrome*, GOOGLE CHROME HELP, <https://support.google.com/chrome/answer/7440301?hl=en&co=GENIE.Platform%3DAndroid>.
⁶ *Search & Browse Privately*, GOOGLE SUPPORT, <https://support.google.com/websearch/answer/4540094?hl=en&ref=topic>.

information and location is retained by Google or for what purposes. In fact, Google’s claims to give users “control” and to respect their “choice” largely serve to obscure the reality that, regardless of the settings users select, Google is still hard at work collecting, storing, and monetizing the very location and other personal information users seek to keep private.

II. DISCOVERY CONTROL PLAN

1. The discovery in this case is intended to be conducted under Level 3 pursuant to Tex. R. Civ. P. 190.4.
2. This case is not subject to the restrictions of expedited discovery under Tex. R. Civ. P. 169 because the State’s claims include a claim for nonmonetary relief and claims for monetary relief, including penalties and attorneys’ fees and costs in excess of \$1,000,000.

III. PUBLIC INTEREST

3. Plaintiff has reason to believe that Defendant has engaged in, and will continue to engage in, the unlawful practices set forth below. Plaintiff has further reason to believe Defendant has caused and will cause adverse effects to consumers in Texas, to legitimate business enterprises which lawfully conduct trade and commerce in this state, and to the State of Texas. Therefore, the Consumer Protection Division of the Office of the Attorney General of the State of Texas is of the opinion that these proceedings are in the public interest.

IV. JURISDICTION

4. This action is brought by Attorney General KEN PAXTON in the name of the State of Texas and in the public interest under the authority granted him by section 17.47 of the Texas Deceptive Trade Practices-Consumer Protection Act, TEX. BUS. & COM. CODE ANN. § 17.41 et seq. (“DTPA”) upon the grounds that Defendant has engaged in false, deceptive, and misleading acts and practices in the course of trade and commerce as defined in, and

declared unlawful by, subsections 17.46(a) and (b) of the DTPA. In enforcement suits filed pursuant to section 17.47 of the DTPA, the Attorney General is further authorized to seek civil penalties, redress for consumers, and injunctive relief.

5. Google has extensive and ongoing business operations throughout Texas, including operations conducted by itself and by various other affiliated entities Google has registered with the State. This has been the case for many years. Google has appeared as a party to many lawsuits in Texas state and federal courts, as both plaintiff and defendant. Google provides products and services to millions of Texans across every corner of the State, has multiple corporate offices in multiple cities in the State, uses the State's residents and resources to test new products and services, such as Google Fiber, and is, therefore, essentially at home in Texas. Google also maintains a major data center in Midlothian, Texas, which helps keep Google's products and services running. The allegations herein relate to many, but not all, of Google's overwhelming contacts with the State and arise from Google's conduct vis-à-vis users Google knows to be using Google's products and services in the State. Google is doing business in Texas and is subject to both general and specific personal jurisdiction of this Court. Solely by way of illustrative examples, Google contracts by mail or otherwise with Texas residents and either party is to perform the contract in whole or in part in this state, Google commits torts in whole or in part in this state, and Google recruits Texas residents, directly or through an intermediary located in this state, for employment inside or outside this state.

V. DEFENDANT

6. Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

7. Google is a technology company that specializes in Internet-related products and services, which include online advertising technologies, search, cloud computing, and other software and hardware.
8. Google markets, advertises, offers, and provides its products and services throughout the United States, and the number of Google's Texas users is likely in the millions.

VI. VENUE

9. Venue of this suit lies in Victoria County, Texas because, under DTPA subsection 17.47(b), Defendant and its agents have done business in Victoria County, Texas by offering its goods and services to consumers and businesses in Victoria County, Texas.

VII. TRADE AND COMMERCE

10. Defendant has, at all times described below, engaged in conduct which constitutes "trade" and "commerce" as those terms are defined by subsection 17.45(6) of the DTPA.

VIII. ACTS OF AGENTS

11. Whenever in this Petition it is alleged that Defendant did any act, it is meant that Defendant performed or participated in the act or Defendant's officers, agents, or employees performed or participated in the act on behalf of and under the authority of the Defendant.

IX. NOTICE BEFORE SUIT

12. The Consumer Protection Division informed Defendant in general of the alleged unlawful conduct described below at least seven days before filing suit, as may be required by subsection 17.47(a) of the DTPA.

X. FACTUAL ALLEGATIONS

A. Google's False, Misleading, and Deceptive Practices Regarding Location History

1. Google's Business Model Relies on Constant Surveillance of Texans.

13. Google's business is profiting from user data. Through its many consumer products and services, Google collects and analyzes the personal and behavioral data of billions of people. In turn, the Company uses this information to build user profiles and provide analytics that support Google's digital advertising business. Google's advertising products generated nearly \$150 billion in revenue in 2020.

a) *Google Collects Texans' Location Data Via the Android OS and Google Apps and Services.*

14. Much of Google's location data collection occurs by way of Google's Android operating system ("Android" or "Android OS"). Android has been used on a majority of smartphones in the world and approximately half of smartphones in the United States since at least 2015.⁷ The Android operating system is free and open-source software. However, most Android devices on the market include a suite of Google apps and application programming interfaces ("APIs")⁸ (collectively, "Google Mobile Services") that are preinstalled on a user's device under a licensing agreement between Google and Android device manufacturers ("OEMs").

⁷ The smartphone market is generally split between two operating systems ("OS"): Apple's "iOS" and Google's Android OS. Apple's iOS is used on all iPhone and iPad devices.

⁸ An API is a software interface that connects computers or pieces of software to each other.

15. The basic functioning of the Android OS provides Google with a steady stream of location data from Android devices. Through sensors and APIs installed on Android devices,⁹ Google can track the precise location of a device and its owner on a continuous basis, using GPS coordinates, cell tower data, Wi-Fi signals, and other signals that are transmitted by the device to Google.

Google

Device Location

- A precise lat/lng of user's location of presence from GPS/WiFi/Cell tower triangulation.
- Considered as the ground truth, used to calibrate other signals like IP.
- Two types, both up to 24 hours old:
 - Zwbk cookie based current device location.
 - GAIA based historical device location.
- ■■■ conditioned RPM increase and better AQ.

Figure 3. Excerpt from an internal Google document discussing some of the inputs used to triangulate a user's precise location.

16. Google's other consumer products include apps and web-based services, such as Google Search, Google Maps, Chrome web browser, YouTube, Google Play Store, and Google Assistant, many of which can be used on both Android and Apple iOS devices (such as iPhones). These products are also critical to Google's ability to extract location data. Google collects and stores users' location data when they interact with certain Google apps

⁹ As used herein, the term "Android device" refers to mobile devices that use Google's Android OS and that come pre-installed with Google-licensed software and APIs (Google Mobile Services), including the Google Play Store and Google Play Services API.

and services, even when a user's location is not needed to support the core functionality of the app or service.

17. On Android devices, certain Google apps are granted permission to collect users' location data by default. Other Google apps ask permission from users to allow Google to collect location data. On many versions of Android, once apps are permitted to collect a user's location data, they may continue to collect and transmit location data to Google unless the user remembers to revoke permission. And if a user elects not to grant permission, an app may continue to prompt the user to enable location settings until the user relents.
18. Furthermore, even when a user disables the settings that allow their device to transmit location data to Google, Google still approximates that user's location, for example, through its [REDACTED] service and by using IP address¹⁰ information that is transmitted when the user interacts with many Google apps and services. Google's "IPGeo" service, in fact, maps IP addresses to geographic locations and that service cannot be disabled.

b) *Location Data Is Highly Valuable to Google.*

19. Some of Google's consumer products can be used at no direct financial cost to the user. But that is simply because it is the user that is for sale. Instead of charging money for its products, Google collects exhaustive personal data about its users when they engage with Google products, including their browsing history, location data, and information from their email. Google processes this data to draw inferences about individuals and groups of users that it monetizes through advertising and other business-facing services.

¹⁰ An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol."

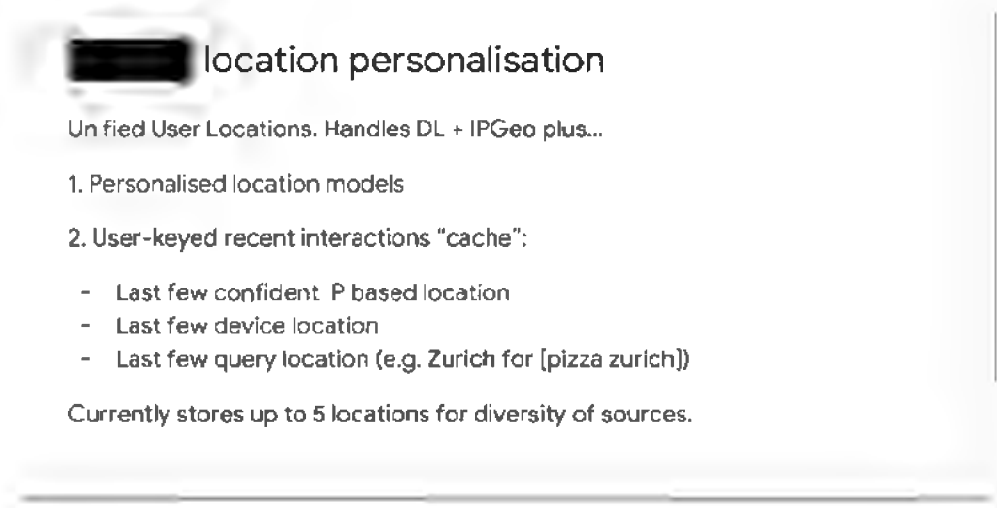


Figure 4. Internal Google document discussing Google's personalized-location modeling and the [redacted] program.

20. Google's advertising business is dependent on its collection of this personal data, and location data is particularly valuable. According to Google documents, "ads revenue goes up a double-digit percentage when location is attached." In marketing materials directed at advertisers, Google actively publicizes its ability to provide better advertising services through location-based analytics and geo-targeted consumer advertising.
21. Because location data is key to Google's lucrative advertising business, the Company has a strong financial incentive to dissuade users from withholding access to that data. As detailed herein, Google has employed and continues to employ a number of deceptive practices to make it nearly impossible for users to stop Google from collecting their location data when using Google products. These practices include privacy-intrusive default location settings, hard-to-find location settings, misleading descriptions of location settings, repeated nudging and pressuring to enable location settings, and incomplete or misleading disclosures of Google's location-data collection and processing.

22. In one striking example, Google dramatically reworded a pop-up window that prompted users to enable a setting so that the prompt no longer disclosed on its face that enabling the setting allowed Google to continuously collect the user's location. Google's express goal was to increase the number of users reporting their location to Google. *See infra* § E(2). The roll-out of this vague prompt was celebrated within Google when it resulted in a dramatic increase in users who "agreed" to be tracked.

2. Google Cloaks Its Location Monitoring in a Web of Unrelated Settings.

23. Google misleads its users by presenting them with a maze of settings the users must navigate should they dare to try to keep their whereabouts private. Aside from the sheer number of confusing settings, Google's deception lies in the reality that many of the settings ostensibly have nothing to do with location, some are activated by default, and some are simply insufficient to protect one's privacy, despite what Google leads users to believe. Google promises a path to its users out of the Google-created blizzard of location harvesting; however Google made sure to plant deceptive sign posts masquerading as privacy settings so no reasonable user could likely escape becoming a Google profit center.

24. At the highest level, Google's settings can be classified into two categories: Google Account settings and device-level settings. Google Account settings apply to data collected from *any* device signed in¹¹ to a user's Google Account. In contrast, device settings apply *only* to the specific device on which the setting appears. Below is a brief description of the settings most pertinent to Google's deceptive representations and omissions regarding location tracking.

¹¹ A device (or user) is "signed-in" to Google if the user has signed into the user's Google Account at device set-up or in connection with a Google app.

a) *Location-Related Google Account Settings.*

25. Google’s collection and use of location data is purportedly subject to at least three Google Account settings: Location History, Web & App Activity, and Google Ads Personalization (“GAP”).
26. Location History is a Google Account feature that captures all the places where a signed-in user goes. Location History collects the user’s device location hundreds of times a day, regardless of whether the user is interacting with a Google product. Location History has existed in some form since approximately 2009. The data collected by Location History is derived from signals made available via the location sensors on a user’s device, such as sensors for GPS, cell tower, Wi-Fi, and Bluetooth signals. Using those various signals, Google can track a user’s precise location,¹² including both outside and inside buildings.
27. Google applies internal tools to analyze a user’s Location History and logs this information with the user’s Google Account. Using this information, Google builds a “private map” of all the places a user has been.
28. The primary value of Location History data for Google lies in its profitability for advertising uses. This data informs what advertising Google will present to that user.
29. In addition, Google uses Location History data to provide advertisers with “store conversion” rates—i.e., the rate at which users who view an ad actually visit the advertised store. Google’s ability to follow their users’ movements in the physical world after they click on digital ads is a unique selling point for its advertising business.
30. Web & App Activity is a separate Google Account setting that collects, stores, and monetizes user location. Whereas Location History passively collects location information

¹² As used herein, “precise location” refers to the user’s exact longitude and latitude.

on all of a user's movements, Web & App Activity records a user's "transactional location"—i.e., the location of a signed-in user's device when the user is interacting with certain Google products.¹³ For example, when a signed-in user conducts a search for "chocolate chip cookie recipe" on the Google Search app, Google collects the user's location at the time of the search, along with details about the search, and stores that information to the user's Web & App Activity log. Later, if the user searches for an address on Google Maps, Google again stores the user's location at the time of that search, along with details about what was searched, to the same log.

31. Google uses Web & App Activity data to deduce user habits and interests for advertising purposes. Google's ability to target ads to users based on information about their locations is critical to the success of its billion-dollar advertising business. From in or around 2015 to in or around 2019, Google used the Web & App Activity setting to log a user's precise latitude and longitude.
32. Because Location History and Web & App Activity are independent settings, disabling one does not impact whether a user's location is collected and stored by the other. In other words, even if a user attempts to prevent location tracking by disabling one of these settings, Google still tracks and monetizes that user's location through the other. And until recently, Google kept the data stored in connection with these settings indefinitely, unless the user manually deleted the data.
33. Google also offers users a Google Account setting related to personalized advertising—the GAP setting. The GAP setting purports to provide signed-in users the ability to opt out of

¹³ A "supplemental" Web & App Activity setting also collects and stores information about the user's interactions with non-Google apps and with non-Google websites on Google's Chrome browser.

personalized ads served by Google. Google told users that with this setting enabled, “Google can show you ads based on your activity on Google services (ex: Search, YouTube), and on websites and apps that partner with Google.”

b) *Location-Related Device Settings.*

34. Location-related device settings control whether a specific device transmits location information to apps, APIs, or other services on the user’s device. Android devices have multiple location-related device settings.
35. First, Android devices have a location “master switch” that controls whether the device can share the device’s location with any other apps on the device. When this “master switch” is enabled, apps and services can request and access the device’s location. If a user disables this setting on their device, then no apps or services can access the device’s location.
36. Second, Android devices have “app-specific” location settings. Using these settings, users can grant or deny a specific app, such as Google Maps or Uber, permission to access the device’s location. On some versions of Android, apps with permission to access device location could access a user’s location in the background—i.e., even when no apps requiring location were in active use.
37. On Android devices, these two types of settings control the flow of location information to Google. For example, enabling the location “master switch” allows Google to collect and use location information from the user’s device to improve an internal Google platform called Google Location Services.¹⁴ In addition, when specific apps access an Android device’s location, that location data is also shared with Google, even if the app in question is a non-Google app.

¹⁴ Google Location Services is also referred to as Google Location Accuracy.

38. Android mobile devices also have other settings that purportedly give users control over other types of data collection that Google uses to determine the users' location. For example, Android users can control whether their device scans for nearby Wi-Fi access points or Bluetooth devices, both of which technologies Google uses to determine a user's location. Certain versions of the Android OS also include "Low Battery" and "High Accuracy" modes that control whether Google uses Wi-Fi, Bluetooth, cellular signals, and Google Location Services, in addition to GPS, to ascertain the user's precise location.
39. This complex web of settings misleads users into believing that they are not sharing their location with Google when, in fact, they are.

3. Google Deceives Users Regarding Their Ability to Protect Their Privacy Through Google Account Settings.

40. One way that Google misleads users regarding their location data is through the Google Account settings described above. As a result of deceptive practices with respect to these settings, Google has collected enormous amounts of location data from unwitting Texans and monetized that data in the service of Google's advertising offerings without Texans' knowledge or consent.
- a) *Google Misrepresented the Characteristics of the Location History and Web & App Activity Settings.*
41. Google misrepresented and omitted material information regarding the Location History and Web & App Activity settings until at least 2019. These misrepresentations and omissions confused users about which settings implicate location data, making it more likely that Google would capture, store and profit from such data without users' knowledge or consent.

42. For years, Google assured Android users on a public webpage that “[y]ou can turn off Location History at any time. *With Location History off, the places you go are no longer stored.*” Google similarly explained that Apple users could log into their online Google account and select “Stop storing location” in order to turn off Location History, and that turning Location History off would “*stop[] saving new location information.*” Google thus represented Location History as the setting that, when turned off, empowered users to prevent Google from storing or saving their personal location information.
43. That representation was false. Even when Location History was off, Google deceptively continued to collect and store users’ locations through other means. Namely, depending on a user’s other settings, Google collected and stored location data through Google’s Location Services feature, Web & App Activity, Google apps on the user’s device, Wi-Fi and Bluetooth scans from the user’s device, the user’s IP address, and location data shared with Google by companies that use Google advertising products.
44. Google’s statements prompting users to turn on Location History also falsely implied that only this setting controlled whether Google stores a user’s location. For example, at various times, Google told users that enabling Location History “lets Google save your location;” allows Google to “store and use” the “places you go;” permits Google to “periodically store your location;” “allows Google to store a history of your location;” or allows Google “to save and manage your location information in your account.” Like Google’s statements on its webpages, these statements obscured the fact that the Location History setting does not alone control whether Google collects and saves a user’s location data.
45. Google’s misleading statements and omissions regarding Location History were exacerbated by separate misleading statements and omissions in connection with the Web

& App Activity setting. Specifically, Google did not disclose to users that even when Location History is disabled, the Company still collects, stores, and uses location data through the Web & App Activity feature. This despite the fact that Google knew that location information is uniquely sensitive.

46. As alleged above, Web & App Activity collects location data when a user interacts with certain Google products. For example, if a user asks Google Assistant to search for the author of a book, Web & App Activity would save the user's location and the time when the query was made—even with Location History off. Google also collects and stores information that could implicitly reveal a user's location, such as the places a user inputs into Google Maps.
47. The 2018 AP story illustrated the extent of Google's location tracking through Web & App Activity. The report provided a visual map of the data Google collected from the AP investigator's device when Web & App Activity was enabled but Location History was disabled. The resulting map reflected that in only eight hours, Google captured almost two dozen precise, time-stamped GPS coordinates.
48. Google recognizes that the mosaic of the locations of individual users over time constitutes sensitive information. Despite this, Google concealed the fact that the Web & App Activity setting controlled Google's storage and use of location information. Moreover, users could not reasonably avoid Google's deceptive storage and use of their location because it occurred without their knowledge.
49. First, Google failed to disclose the Web & App Activity setting when users set up Google Accounts for the first time. Yet at this stage, the Web & App Activity setting is defaulted "on" for all Google Accounts. Thus, a user who sets up a Google Account is unknowingly

automatically opted-in to location tracking (via Web & App Activity) unless the user learns about and affirmatively changes this setting. But until 2018, the Google Account set-up process made no mention of the Web & App Activity setting.

50. Furthermore, Android phones effectively require a user to sign in to a Google Account,¹⁵ and Google apps like Search and Maps are granted location permission on Android devices by default. As a result, a new Android user could create a new Google Account, be automatically opted in to the Web & App Activity surveillance program, and then defaulted into granting location permissions to multiple Google apps, meaning Google could track that user's location across the user's Google Account and through several apps without disclosing the existence of the setting or presenting the user with an option to opt out.
51. One of the only ways users would even become aware that Web & App Activity was storing location data was if they happened to navigate to a separate webpage where Google recorded data stored under the Web & App Activity setting, called "My Activity." But when users first landed on this webpage, Location History was presented as the only setting that related to location data. For example:

¹⁵ A user must sign in to a Google Account on their Android device to access the Google Play application ("app") store, which is needed to download new apps or receive app updates that enable apps to function properly and safely. On information and belief, once Android users sign in to their Google Account, users can not sign out of Google. If they do not want to be signed in, their only option is to fully remove their Google Account(s) from their device.



Figure 5. A screen capture representative of Google's Account set-up disclosures in 2018.

52. In 2018, Google revised its Google Account set-up process to include the option to disable Web & App Activity. However, the Company still deceptively concealed from new users the fact that location data was captured by the setting. Until at least mid-2018, this information was only revealed to new users who first clicked on a link to see “More options” to customize settings and then selected a second link to “Learn More” about the Web & App Activity setting. Google’s own studies show that many users do not take these additional steps when setting up their Google Accounts because they are focused on setting up their account quickly.

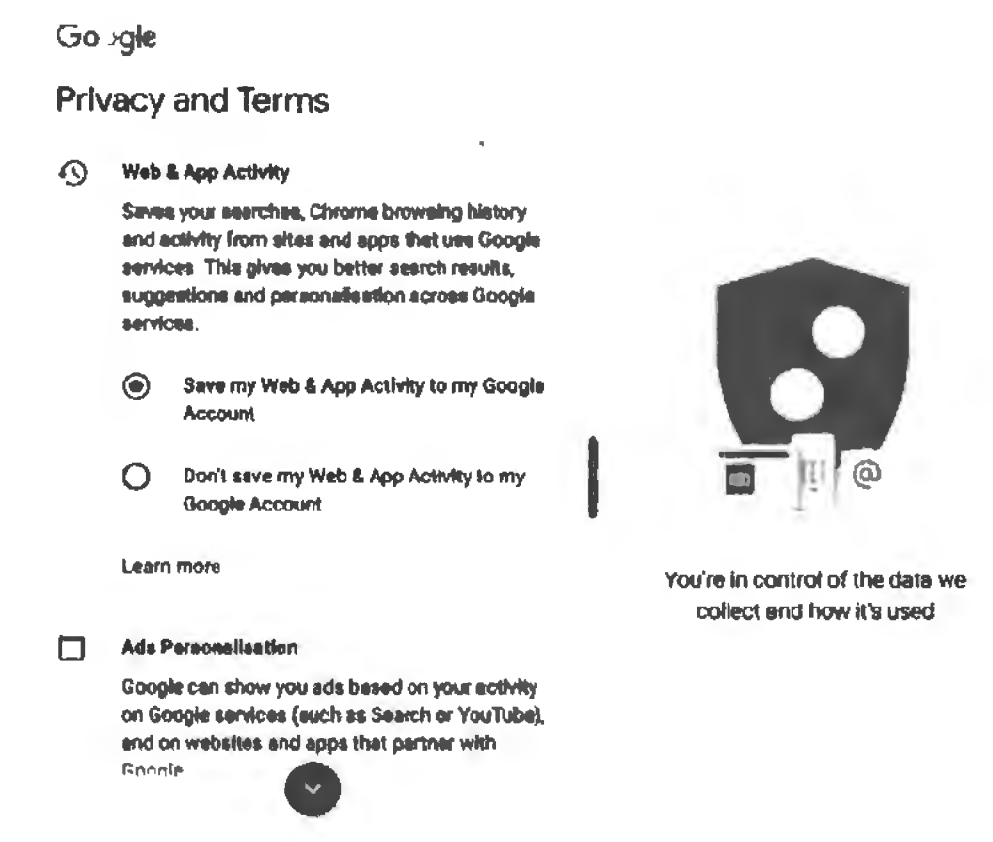


Figure 6. A screen capture demonstrating Google's failure to inform Texans that Web & App Activity was used to track location.

53. Second, Google failed to disclose the Web & App Activity setting to users when they set up new devices using existing Google Accounts. A user's Web & App Activity "enabled" or "disabled" status applies to all devices signed in to the user's Google Account. Thus, any time a user signed in to an existing Google Account on any device, Google could begin tracking that device as long as Web & App Activity was enabled on the user's Account. Because Android devices need to be signed in to a Google Account to use critical functionalities and because users sign in to Google at Android device set-up, Google was able to track Android users via Web & App Activity as soon as they set up new devices on their Google Accounts. Users did not receive a separate notification that Google had begun storing the location of the new device via the Web & App Activity setting.

54. Third, Google did not identify Web & App Activity as a location-related setting in the places where a user would expect to find that information. For example, until around 2019, users who explored location settings on their Android devices would not find Web & App Activity listed among them. Likewise, a Google webpage titled “Manage your Android’s device location settings,” which described Google’s location-based settings, discussed Location History without mention of the Web & App Activity setting. Google’s Privacy Policies also omitted mention of the Web & App Activity setting. For instance, the December 18, 2017 version of Google’s Privacy Policy lists examples of information about “your actual location” that Google “may collect and process.” These examples include a specific mention that “Location History allows Google to store a history of your location data,” but make no reference to the Web & App Activity setting.
55. Finally, many of Google’s affirmative disclosures regarding Web & App Activity also failed to disclose that this setting authorized Google to store and use location data. Google routinely described the Web & App Activity setting as allowing the Company to store things like Google search history and activity on Google apps—without mention of location (unless the user clicked on a link to a pop-up window for more information). Yet Google stores Web & App Activity data in, among other places, a data store it calls Footprints. It is difficult to imagine a more misleading incongruence than an arrangement where users are told they can prevent the storage of their location history by disabling a setting called Location History while the Company continues to store the users’ location history in a data store called Footprints using a setting that the Company does not clearly advertise as implicating location history.

56. These design choices all reinforce Google’s underlying deception that disabling Location History was sufficient to prevent Google from storing a user’s location history, as Google promised. The name “*Location* History” gives users every reason to believe that the setting controls the collection of their *location* history while nothing about the name “*Web & App* Activity” gives users a reason to believe that setting tracks one’s *location* history. A reasonable user would be misled and deceived. And that is even before considering Google’s false promise that “with Location History off, the places you go are no longer stored.”
57. In sum, Google misrepresented that disabling Location History stopped Google from storing a user’s location and concealed that the Web & App Activity setting also stored location data. This tended to mislead users to believe that the Web & App Activity setting did not impact the collection, storage, or use of location data; that the Location History setting alone controlled whether Google retained and used location data; and that the Location History setting would prevent Google from retaining and using the user’s historical locations on an ongoing basis.
58. Both the gravity and the flagrance of these misrepresentations are demonstrated by Google’s response to the public revelation in the 2018 AP article that Google “store[s] your location data even if you’ve used a privacy setting that says it will prevent Google from doing so.” Within Google, a self-titled “Oh Shit” meeting was convened the day the AP story was published to begin brainstorming responses to the article. Soon after, Google CEO Sundar Pichai and other senior executives became directly involved in crafting the Company’s response. After being caught red-handed by the AP story, Google updated its

help page to remove the false promise that “With Location History off, the places you go are no longer stored.”

59. In addition, within only a few days of the story’s publication, over one million Google users flocked to an “Activity Controls” webpage, where they could adjust the Location History and Web & App Activity settings. At its peak, the number of users who disabled at least one of these settings increased by over 500%. The Company also observed a significant decline in user trust as a result of the AP story’s revelations.
60. Internally, Google employees agreed that Google’s disclosures regarding Location History were “definitely confusing” and that the user interface for Google Account settings “feels like it is designed to make things possible, yet difficult enough that people won’t figure it out.” One IT specialist at Google admitted, “I did not know Web and App Activity had anything to do with location.”
61. Even before the AP article was published, however, Google’s own studies showed that users had a poor understanding of the Google Account settings. Yet Google did not act to correct this misleading impression or attempt to clarify the Web & App Activity and Location History settings until after the Company’s misconduct was made public.
 - b) *Google Misrepresents the Characteristics of its Other Google Account Settings.*
62. Google also misleads users about its location tracking practices by misrepresenting and omitting material facts regarding the extent to which Google Account settings prevent Google’s collection and use of location data. Google Account settings offer seemingly simple “privacy controls” to attract users and lull them into a sense of security, but Google continues to exploit users’ location data regardless of the choices users make with respect to these settings.

63. For years, Google has made misleading promises that users can control the information that Google collects, stores, and uses about them by adjusting their Google Account settings. In numerous iterations of Google’s Privacy Policies and other disclosures, Google has pointed to Google Account settings as features that, among other things, allow users to make “meaningful choices about how [the information Google collects] is used;” “control the collection of personal information;” “decide what types of data...[they] would like saved with [their] account when [they] use Google services;” or “make it easier for [them] to see and control activity that’s saved to [their] account and how it’s used.” For example:

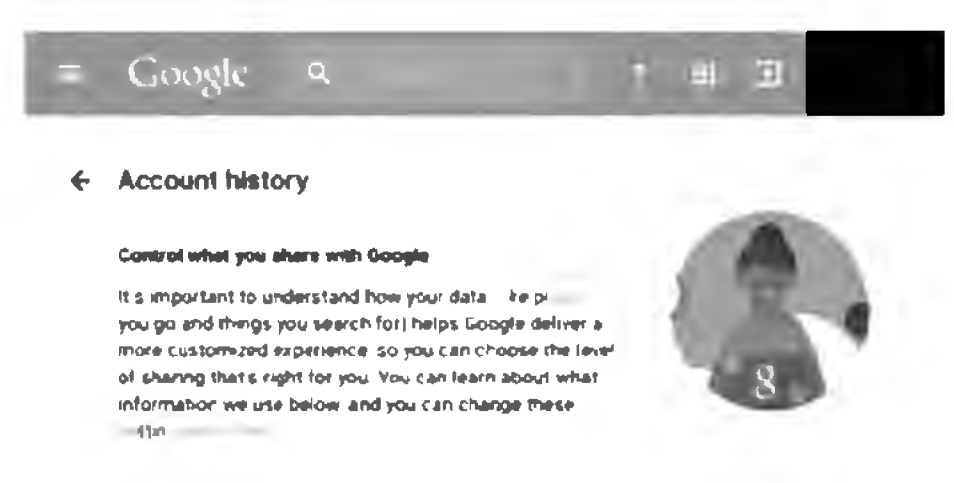


Figure 7. An example of Google's representations about user control.

64. Since May 25, 2018, Google’s Privacy Policy has explained that “across our services, you can adjust your privacy settings to control what we collect and how your information is used.” In its Terms of Service and Privacy Policies, Google has also represented that it would “respect the choices you make to limit sharing or visibility settings in your Google Account.”

65. As part of setting up a Google Account, Google expressly tells users, “You’re in control. Depending on your account settings, some ... data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data.... You can always adjust your controls later or withdraw your consent....”
66. In another example, since 2019, Google has maintained a webpage devoted to explaining “How Google uses location information.” This webpage states that “[i]f Web and App Activity is enabled, your searches and activity from a number of other Google services are saved to your Google Account. The activity saved to Web and App Activity may also include location information.... Pausing Web & App Activity will stop saving your future searches and activity from other Google services.”
67. In statements like these, Google frames Google Account settings as tools that allow a user to easily control Google’s collection and use of their personal information. The Company’s reassuring statements about these settings misleadingly imply that a user can stop Google from storing or deploying the user’s location information by disabling these settings.
68. But this is not true. Regardless of whether the user has disabled Web & App Activity or Location History, Google collects, stores, and uses location data when a user uses certain Google products, such as the Google Play Store, Music, Search, and Maps. Furthermore, for signed-in users, Google sometimes associates this information with the user’s Google Account even if the user has not enabled Web & App Activity or Location History.
69. In other words, while touting user’s ability to control personal-data collection through Google Account settings, Google flouts that control by continuing to collect, store, and use location data regardless of whether the user disables these settings.

70. Google further misleads users by providing them only partial visibility into the location data Google collects. For example, Google’s current Privacy Policy claims that users can manage their privacy because they can “review and control information saved in [their] Google Account” and “decide what types of activity [they would] like saved in [their] account.” Earlier versions of the Privacy Policy likewise indicated that Google provides “transparency and choice” by allowing users to “access, manage, or delete information that is associated with [their] Google Account,” and stated that Google provides these tools in order to “be clear about what information [it] collects.” In other disclosures, Google explains that the My Activity webpage “allows [users] to review and control data that’s created when [they] use Google services” and that “My Activity is a central place where [users] can view and manage [their] saved activity.”
71. Google’s representations that users can “control” their saved location data fail to disclose that users can control only a subset of the location data Google saves. The My Activities webpage reflects only some of the location data stored when users interact with certain Google products (e.g., Search, Assistant, and Maps). Users can delete this subset of location data, as well as Location History. But Google also collects and stores this location data when users interact with many other Google products and services, such as Google Play Movies and TV, Music, YouTube, and the Google Play Store. And when a user is signed in to Google, Google associates this location data with the user’s Google Account without making this data visible to users on the My Activities webpage.
72. Google does not disclose that it retains location data tied to a user’s Google Account that the user cannot review and control. By allowing users to manage only a partial set of the

location data it collects, Google further misleads users regarding the extent of data collection and use in the service of its business.

73. Despite claiming to endeavor to “be clear about what information [Google] collects, so that [users] can make meaningful choices about how it is used,” Google also failed to disclose that Google collects location data when users are not signed in to a Google Account.
74. Signing out of or declining to set up a Google Account (and thus opting out of Google Account settings altogether) does not protect users from Google’s pervasive location tracking. Google collects and stores the same type of location data from signed-out users when they use Google products as it collects and stores from signed-in users. Google merely associates the location data of signed-out users with a unique “pseudonymous” identifier rather than the user’s Google Account.
75. Until May 2018, Google did not disclose in its Privacy Policy that it stores information from signed-out users, who cannot prevent this form of data collection. Even today, the webpage devoted to explaining “How Google uses location information” only explains how location data is “saved in [a] Google Account,” without explaining that Google also stores and deploys the location data of users who are not signed in to Google Accounts when they use Google products.
76. Put simply, contrary to the Company’s representations, disabling or enabling Google Account settings does not control whether Google will collect, store, or use a user’s location data. Even disabling all Google Account settings or signing out of a Google Account is not effective to prevent Google from storing and using a user’s location data. As a result of Google’s misleading statements with respect to these settings, users cannot reasonably avoid Google’s access to and use of their location data.

77. Google is aware that users do not understand Google Account settings or how these settings interact with other location-related settings. Google employees themselves admit that “many of us in Location don’t fully understand the interactions and implications of the three bits: Location History, [Location reporting], [and Location master switch]. If it’s difficult even for us to understand it, our users are SOL [Shit Out of Luck] figuring this stuff out” and that the location toggles need to be simplified “to the point where neither us nor our users are confused by it” because hundreds of millions of users are in “confusing states [with respect to location],” meaning users disabled location tracking in one place but enabled it (or failed to disable it) in another.

c) *Google Misrepresented the Characteristics of the Google Ad Personalization Setting.*

78. Google’s deceptive practices extend to the GAP setting as well. The GAP setting purportedly allows users to opt out of personalized advertising. Similar to Google’s other practices, this setting allows users to “control” the Company’s use of their location data only to an extent.

79. Google has explained that enabling the GAP setting will “Let Google use [a user’s Google Account activity] to show [the user] more relevant ads on [Google’s] services and on websites and apps that partner with [Google].” In connection with explaining this setting, Google told users that they should “let Google know [their] location,” so that “[they] won’t get ads for stores in other regions.”

80. The GAP setting and Google’s disclosures indicate that a user has control over whether Google will serve “personalized” ads based on the user’s location. But this setting only provides an illusion of control. In reality, Google continues to target ads based on a user’s

location—both on and off Google products—even if the user opts out of ads personalization by disabling the GAP setting.

81. Rather than curing its deception, Google chose not to disclose to users who disable ad personalization that Google would continue to serve targeted ads based on the user's location anyways.

4. Google Deceives Users Regarding Their Ability to Protect Their Privacy Through Device Settings.

82. Google further confuses and misleads users into sharing more location data than they intended through deceptive practices that contradict the Company's representations and users' expectations regarding location-related device settings. Google conceals from users that, even when they deny Google permission to access their location via device settings, Google continues to collect and store the users' location regardless of the user's explicit attempt to block Google's access to that information. Google misleads users in at least three respects.

83. ***First***, Google tells users that they can control the flow of location data via the location “master switch.” Google includes this “master switch” on Google-licensed Android phones in order to provide this functionality. Furthermore, beginning with its May 2018 Privacy Policy, Google has represented that “the types of data [Google] collect[s] depend in part on [the user's] device and account settings. For example, [a user] can turn [an] Android device's location on or off using the device's setting app.” Google also provided Help pages explaining how to turn off Android device location, including explanations such as: “If [a user] turn[s] off Location for [a] device, then no apps can use [the user's] device location.” Today, Google tells users: “[Users] can allow Google and other apps to provide

[users] with useful features based on where [a] device is located” “if [the user] choose[s] to turn on [the] device location.”

84. These representations, as well as the Android device setting itself, mislead users to believe that if they disable the master location setting, Google does not collect, store, or use their location to provide “services” (including ads) to the user. However, for years, including through today, Google has deceived users by failing to disclose that regardless of whether the user *explicitly forbids* Google from accessing location via a device, Google derives and stores the user’s location and uses that information for geo-targeted advertising.
85. Specifically, when a user turns the location “master switch” off, believing that they are not sharing location information, Google nevertheless uses the user’s IP address and other sources of stored data (such as historical location data) to infer the user’s location. Users have no control over whether Google derives their location using this method to serve its commercial ends.
86. **Second**, app-specific device settings are also ineffective. Google includes these settings on Android devices to allow a user to deny device location information to specific apps. Further, Google provides Help pages explaining that, on Android devices, a user can choose which apps can access and use a user’s device location. But contrary to what Google leads users to expect, Google still determines a user’s approximate location based on the user’s IP address, past activity, or location data shared with other Google apps or services or by other devices, even when a user has denied location access to the app.
87. Yet, in disclosures up to at least 2019, Google claimed that IP addresses revealed only the *user’s country*, and that Google would merely use this information to provide search results and identify the correct language—with no mention of advertising. Even today, on its

webpage explaining “How Google uses location information,” the Company downplays the accuracy and precision with which it infers a user’s location based on the user’s IP address. The Company proffers only that IP addresses are “roughly based on geography” and allow Google to “get some information about your general area.”

88. **Third**, device settings related to specific location signals on Android phones, such as Wi-Fi and Bluetooth, are confusing and conflicting, making it very challenging for users to limit Google’s access to this data when they intend to. For example, Google uses Wi-Fi scans to compute device location more accurately and precisely. Android phones include a “Wi-Fi scanning” setting among other location-related settings. However, if this setting is “off,” Google can still obtain Wi-Fi scans. If a user has enabled a separate “Wi-Fi 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.
89. 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.
90. 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. Google employees acknowledge that “giving someone a location reporting opt out makes them think it applies broader than ... it does,” that users would be “surprised” to learn that Google bypasses these settings, and that users (and even Google engineers themselves) do not understand how to deploy location-related settings to protect their privacy because “current settings for location and Location History don’t align with user expectations or present

obvious information on how they work.” 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.”

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

91. 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.
92. 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.
93. 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.
 - a) *Dark Patterns Exist in Google Account Settings.*
94. 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.

95. 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. For example:

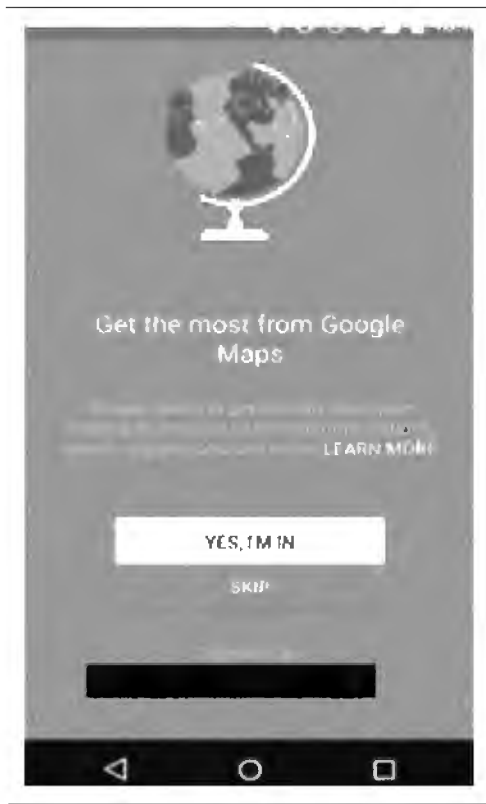


Figure 8. An example of the pressuring Google deploys during set up to lead Texans to consent to location tracking.

96. 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.
97. 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. For example:

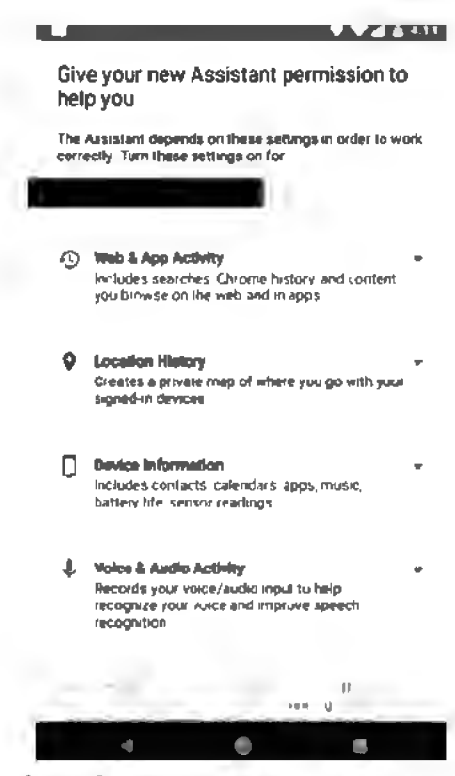


Figure 9. An example of Google's representations that data permissions were necessary for applications to work.

98. 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.
99. 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.
100. Google knows from its own studies that users who are prompted to enable settings while trying to take another action often provide “consent” without reading disclosures closely—simply to get on with whatever action the user was seeking to take. 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.

101. On several occasions, Google’s own employees complained that these practices put unjustified pressure on users to enable Location History and Web & App Activity settings. For example, one Google employee complained, “I’m feeling increasingly bullied by Google to enable Web & App History and I’m about as pro-Google as you can get. Now on Tap doesn’t work[] and Now cards were intentionally made useless.” Another Google employee, noting the “dark patterns” used by Assistant, raised that “Assistant on my phone is requesting Location History tracking, Web / Search / App activity, Device information (contacts / calendar), Voice & Audio Activity even for queries that don’t need them.” A third employee noted that “It is impossible to use the Google Home app without turning on Location History for this account as the assistant setup forces this on. This is particular silly for this account since it never ‘leaves home.’”
102. 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.
103. 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.

For example:

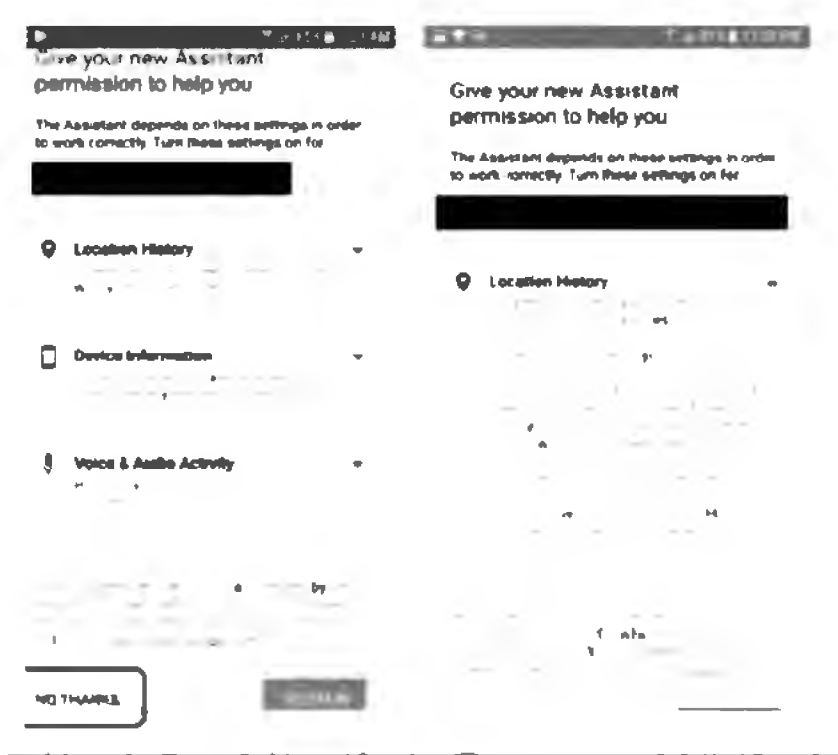


Figure 10. An example showing how Google buries information about its use of Texans' data for commercial purposes in layers of disclosures.

104. Google understood that users were unlikely to seek out information hidden behind links and drop-downs and that users would instead tend to enable settings simply in order to proceed with setting up their devices. Further, Google employees recognized that the “personalization” benefits Google touts are limited, noting for example that “the number of [Location History personalization] features with a personal, immediate user value is smaller,” and that because Google only personalizes 2-3% of searches, “[a]s a user, it’s really not clear to me how Search is using my data for my benefit.”
105. 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 include statements and omissions that 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.

b) *Dark Patterns Exist in Device Settings.*

106. 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, “Maps refuses to take No for an answer[.] Although I turned off location services 20 seconds earlier, Maps is trying to make me second guess my conscious decision. This is the ‘Not Now, maybe later’ antipattern that we still can’t seem to wean ourselves off of.”
107. 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.

108. 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),¹⁶ 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, despite concerns raised by Google's internal privacy group, after it observed that users were opting out of location tracking at higher rates when this toggle was available.
109. Google also convinced other Android OEMs to do the same. In discussions with Android manufacturers, Google told OEMs that customers were accidentally turning off location services or to save battery, even though its own studies suggested user privacy was also a significant reason why users sought to disable location. Removing the toggle, which made the location "master switch" less accessible, resulted in a significant decline in users who disabled location services on their Android devices.
110. 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:

¹⁶ Android KitKat was publicly released on October 31, 2013.

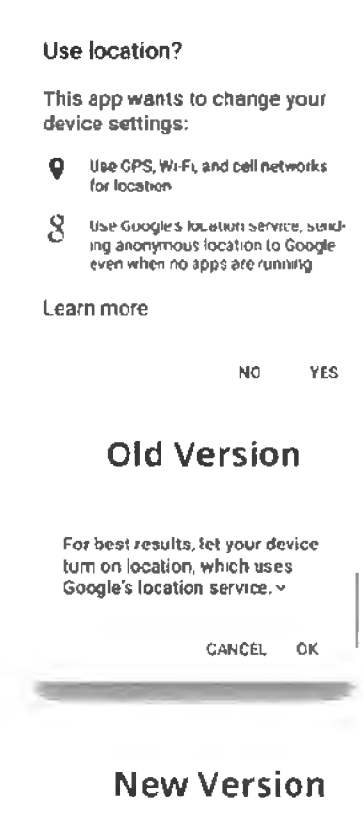


Figure 11. An example of Google's design changes deployed to increase location-tracking permissions.

111. This decision to offer users *less* information about their choices was celebrated within Google for increasing the percentage of users who enabled location settings in Search from 16% to 45% and in Maps from 30% to 53%.
112. 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.

B. Google’s False, Misleading, and Deceptive Practices Regarding Incognito Mode

1. Google Deceptively Represents that “Incognito Mode” Allows Texans to Control What Information Google Sends and Collects.

113. In addition to the deceptive location-tracking practices described in the above paragraphs, Google deceptively captures Texans’ information while they are in Incognito mode. Google does this despite repeatedly assuring Texans that they have control over what information generated during an Incognito session is shared with Google and others.
114. “Incognito mode” is a feature Google offers that can be used with Google’s own web browser, Google Chrome. Incognito mode can be used in Chrome on desktop computers as well as on tablets, iPhones, and Android phones. Google apparently carefully chose the name Incognito as the average Texan would understand the word “incognito” to mean having “one’s identity concealed.”¹⁷
115. Consistent with the ordinary and common usage of the term “incognito,” when a Texan opens an Incognito session in Google Chrome, a standard splash screen appears (hereinafter “Incognito Screen”). Until at least June 2020, the Incognito Screen appeared as follows:

¹⁷ *Incognito*, MERRIAM-WEBSTER DICTIONARY (last visited January 25, 2022), <https://www.merriam-webster.com/dictionary/incognito>.

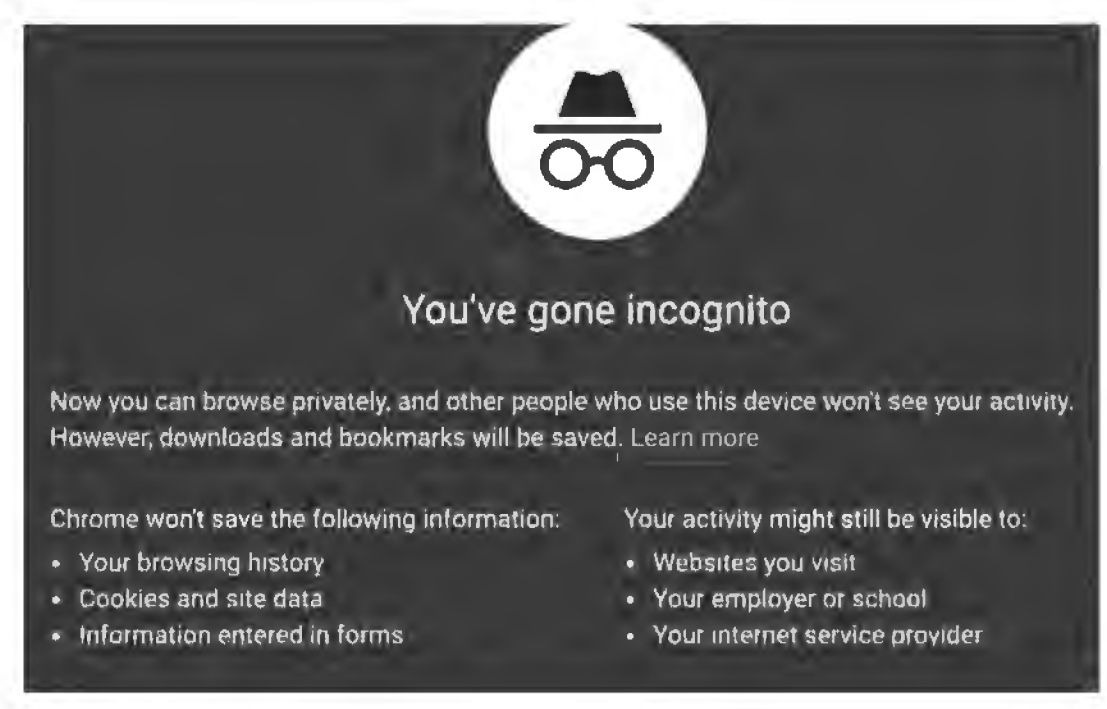


Figure 12. A screen capture representing Google's Incognito Screen in June 2020.

116. A screen with identical or substantially similar text appears when Incognito mode is launched on the iPhone or Android Chrome app.
117. Google's Incognito Screen is deceptive because it is insufficient to alert Texans to the amount, kind, and richness of data-collection that persists during Incognito mode. Based on the representations on the Incognito Screen, Texans reasonably expect that Google will not collect their data while in Incognito mode. Texans reasonably understand "*You've gone incognito*" and "*Now you can browse privately*" to mean the Texans can browse privately without Google continuing to track and collect their data.
118. Texans further have every reason to believe that the privacy controls Google advertises are designed to, and actually, allow Texans to prevent Google from tracking their information, because Google has made representations such as:

- a. “***You’re in control*** of what information you share with Google when you search. To browse the web privately, ***you can use private browsing***, sign out of your account, change your custom results settings, or delete past activity.”
- b. “You can use our services in a variety of ways to manage your privacy . . . across our services, ***you can adjust your privacy settings to control what we collect and how your information is used.***”
- c. “Privacy is personal, which makes it even more vital for companies to give people clear, individual choices around how their data is used.”
- d. “You can also choose to ***browse the web privately*** using Chrome in Incognito mode.”
- e. “Your searches are your business. . . . When you have [I]ncognito mode turned on in your settings, your search and browsing history ***will not be saved.***”
- f. “If you can search it, browse it, or watch it, you can delete it from your account.”

119. Based on Google’s misleading designs and representations, Texans reasonably expect that if they use Incognito mode, Google cannot and will not collect and record data about the Texans’ Incognito activity. In fact, although the Incognito Screen has some information about limits on its protection, nowhere on the Incognito Screen does it disclose that Google may still track users in Incognito mode. However, as described below, Google has deceived Texans, because Google has many opportunities to collect data—and, in fact, does collect data—about Texans using Incognito mode.

2. Google's Privacy Settings Deceptively Lead Texans to Believe They Can Prevent Google From Sending and Collecting Browsing Data.

120. In addition to Google's specific statements about Incognito mode and Google's misleading Incognito Screen, Google's Privacy Policy leads Texans to believe that they have control over when and how Google collects certain data. So, even Texans who take the extra time and effort to dig deeper to protect their privacy come away confused and deceived about Incognito mode.
121. Currently, Google directs users interested in controlling what Google collects to the "Control Panel" of the current Privacy Policy.¹⁸ When users click on "Go to My Activity" to control their data, they are presented with the option to click "Activity controls."¹⁹ When users click on "Learn more," they are taken to a page for "Privacy Controls" in Google's Safety Center. Assuming a Texan has made it three levels deep into Google Privacy Policy, they are greeted by a page that purports to provide the ways in which Google can help users control their privacy and what information is and is not collected by Google. The reassuring title sums up Google's public position: "Your privacy is protected by responsible data practices."²⁰

¹⁸ *Privacy & Terms*, <https://policies.google.com/privacy?hl=en-US> (last visited Jan. 19, 2022)

¹⁹ *Activity Controls*, https://myactivity.google.com/activitycontrols?utm_source=my-activity&hl=en_US (last visited Jan. 19, 2022)

²⁰ *Data Practices*, <https://safety.google/intl/en-US/privacy/data/> (last visited Jan. 19, 2022)



Your privacy is protected by responsible data practices.

Data plays an important role in making the products and services you use every day more helpful. We are committed to treating that data responsibly and protecting your privacy with strict protocols and innovative privacy technologies.

Figure 13. An example of Google's misleading representations about its data-harvesting practices.

122. Separately, Google's Search Help Center provides users information on how to allegedly search and browse privately. There, Google assures users that: "You're in control of what information you share with Google when you search."²¹ But Google deceptively fails to disclose that programs such as Google Analytics remain able to (and, in fact, do) collect data about a Texan's browsing activity even when that Texan is in Incognito mode. Nor does Google disclose where, when, or which websites implement such data-collection tools.
123. Elsewhere in Google's sprawling Help Center, Google discusses its ubiquitous Web & App Activity setting.²² The page conspicuously lacks any reference to what Google keeps when a user turns off Web & App Activity. The only reference is a link to learn more about "[h]ow your saved activity is used."²³ Instead, Google deceptively represents that

²¹ *Search & Browse Privately*, [https://support.google.com/websearch/answer/4540094?](https://support.google.com/websearch/answer/4540094?hl=en)

²² *Find & Control Your Web & App Activity*, https://support.google.com/websearch/answer/54068?hl=en&ref_topic=3378866 (last visited Jan. 19, 2022)

²³ *Safety Center*, <https://safety.google/> (last visited Jan. 19, 2022)

searching and browsing in “private browsing mode” will “turn off” any “search customization” “using search-related activity”:

How Web & App Activity works when you're signed out

Your search and ad results may be customized using search-related activity even if you're signed out. To turn off this kind of search customization, you can search and browse privately. [Learn how.](#)

Figure 14. An image depicting Google's representations that private browsing prevents search customization.

124. Yet when users click the “Learn how” link, they are redirected back to the “Search & Browse Privately” page. And there, Google states that Incognito users “might see search results and suggestions based on your location or *other searches you've done during your current browsing session*”—a representation that is apparently in conflict with the representation that a Texan can “turn off this kind of search customization” by “search[ing] and brows[ing] privately.”

How private browsing works

Private browsing works differently depending on which browser you use. Browsing in private usually means:

- The searches you do or sites you visit won't be saved to your device or browsing history.
- Files you download or bookmarks you create might be kept on your device.
- Cookies are deleted after you close your private browsing window or tab.
- You might see search results and suggestions based on your location or other searches you've done during your current browsing session.

Figure 15. An image depicting Google's contradictory representation that search customization persists in Incognito mode.

125. In sum, Google's Help Center generally leads Texans to believe that they can “control” and limit the information they share with Google by entering Incognito mode. But when Texans dig deeper into the maze, they are presented with misleading, deceptive, and seemingly inconsistent information that leaves Texans unable to make informed, intentional, and consent-driven decisions about the data they share.

126. Moreover, throughout several iterations of its customer-facing privacy policy, Google has stated since at least May 2018 that “[y]ou can use our services in a variety of ways to manage your privacy... [y]ou can also choose to browse the web privately using Chrome in Incognito mode.” When it updated the Google Chrome app for iOS to feature Incognito Mode, Google’s Director of Product Management posted on the company Blog that users would have “[m]ore control with Incognito mode” as “[y]our searches are your business. That’s why we’ve added the ability to search privately with Incognito mode in the Google app for iOS. When you have Incognito mode turned on in your settings, your search and browsing history will not be saved.” In a 2019 New York Times article, Google’s CEO Sundar Pichai represented to users that Google has “stayed focused on the products and features that make privacy a reality for everyone” while championing the company’s rollout of “Incognito mode, the popular feature in Chrome that lets you browse the web without linking any activity to you, to YouTube.”
127. All of these representations lead Texans to believe that Incognito mode gives users the control to browse privately without being tracked.

3. Google’s Private-Browser Cookies Deceptively Continue to Track and Send Data About a Texan’s Incognito Activity.

128. Google could have disclosed on the Incognito Screen that Google is able to (and does) track and collect data on Texans browsing privately, and that Google is able to use the data once the private session is ended. But Google did not. Instead, Google intimated through its privacy policies, help screens, and Incognito Screen that Texans are able to browse *privately* with only limited exceptions—none of which disclosed Google’s private-browsing data-collection practices.

129. The Incognito Screen is false, misleading, and deceptive in several ways. First, Google represents that Google “won’t save . . . [y]our browsing history . . . cookies and site data[.]” This is misleading. On information and belief, even the temporary private-browser cookies Google uses for Texans who use Incognito mode while signed out of their Google account contain bits of data such as device identification, location, and other sensitive data sent to Google’s servers during private browsing sessions. On information and belief, Google could use that data to build, update, and monetize detailed profiles on Texans.
130. Indeed, while Google publicly represents that it “won’t save . . . [y]our browsing history . . . cookies and site data,” Google internally acknowledges that the concept that “Google doesn’t store [Incognito mode] activity at all” is an *unsupported belief*:

Use Cases for Incognito in Chrome

- ◆ **Action:** Logging-in to an account (including social media) in order to provide a sense of ‘safety’ from local and remote attackers
 - Supported Beliefs
 - IM prevents local storage of login information, protecting accounts from other users ✓
 - IM allows multiple logins to same website ✓
 - Unsupported Beliefs
 - IM protects password information from 3rd parties ☐
 - Employers can’t see social media logins on corp devices ☐
 - IM provides anonymity when logging-in to accounts ☐
- ◆ **Action:** Keeping sensitive searches and adult content activity hidden from other users and remote entities
 - Supported Beliefs
 - IM prevents local storage of search terms and activity ✓
 - IM prevents search terms and activity from being tied to my account ✓
 - IM prevents recommendation pollution ✓
 - Unsupported Beliefs
 - Google and ISPs don’t store IM searches and activity ☐

Figure 16. An excerpt from internal Google documents listing the beliefs Google knows users to hold about Incognito that Google knows to be unsupported.

131. This disparity is highly misleading and deceptive to Texan Incognito users.
132. Second, Google represents in the Incognito Screen that “[n]ow you can browse privately and other people who use this device won’t see your activity.” This is misleading. In fact,

“other people who use this device” can often discern what preceding users of an Incognito session did by way of targeted ads served by Google based on browsing activity that took place during that “private” browsing session.

133. Notably, it is only possible to serve targeted ads to Texans who are using Incognito mode because Google deceptively continues to send and receive detailed data about Texans’ “private” browsing activity.
134. Third, Google represents on the Incognito Screen that entities to whom a Texan’s “activity might still be visible” are “the websites you visit[,] [y]our employer or school[, and] [y]our internet service provider[.]” This is misleading. Texans’ private-browsing activity is visible to Google in a variety of ways and across a spectrum of granularity and anonymity. As noted above, Google continues to collect an array of data through its temporary, private-browser cookies. Furthermore, Google is able to collect additional data on the website side of a Texan’s private-browsing activity if a visited website deploys certain Google-powered data-collection tools, such as Google Analytics or Google Ad Manager, as described more fully below.
135. Despite all this, Google has consistently represented to Texans that they can control what information is shared with Google, especially through the use of Incognito mode. Missing from Google’s statements, help pages, and splash screens, however, is a disclosure that Google is able to, and does, continue to track users while they are in private-browsing mode. As a result, users reasonably reach the *opposite* conclusion, believing that Incognito mode prevents Google from collecting data during a private-browsing session.

4. Internally, Google Recognizes the Deceptive Nature of Its Incognito Mode Representations.

136. Google employees themselves have identified the disconnect. For example, one Google presentation reported, “Our name conveys privacy but might also be overpromising.”

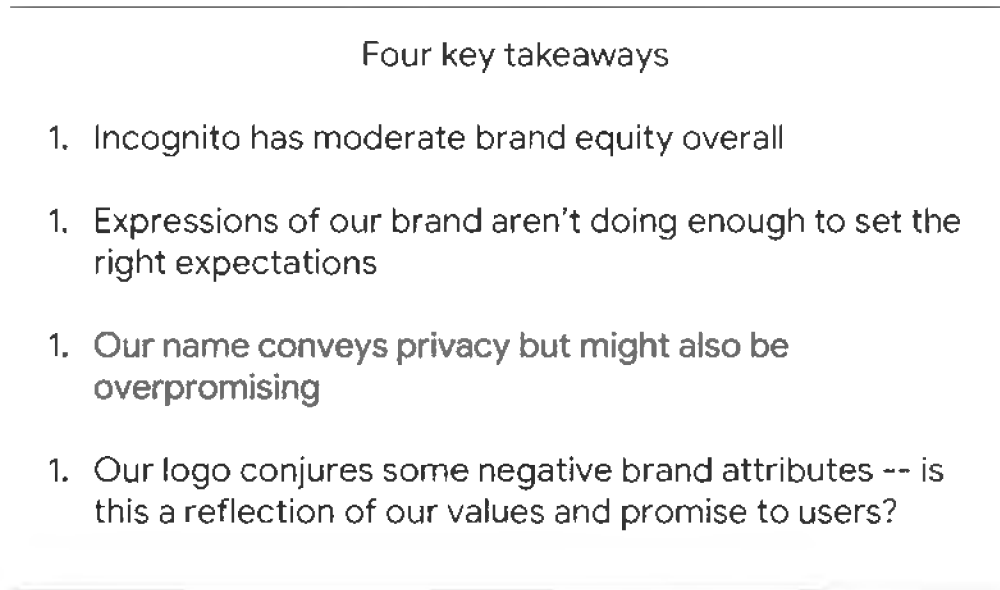


Figure 17. An excerpt from internal Google documents demonstrating Google's understanding that users are deceived about Incognito's functions.

137. Another internal Google communication discloses that one of the major aspects of Incognito that “users misunderstand” is that “[m]any users believe private browsing gives them anonymity.”

And we know users misunderstand these nuances...

1. Many users believe private browsing gives them **anonymity** ([Gao et al. 2014](#))
2. Many users believe private browsing **obscures location** ([Wu et al., 2018](#))
3. Many users believe private browsing **actively blocks ad tracking** ([DuckDuckGo, 2017](#); [Habib et al. 2018](#))
4. Many users believe private browsing **prevents search engines from remembering their searches** ([DuckDuckGo, 2017](#))
5. Most users believe that their private browsing activity **won't be remembered by Google**, even after they sign into their account ([Wu et al., 2018](#))

Chrome UXR

Figure 18. An excerpt from internal Google documents listing the many ways Google knows users to be misled about Incognito mode.

138. Another Google presentation helpfully visualizes the “gap” between what Google leads Texans to believe about Incognito and what Incognito really is:

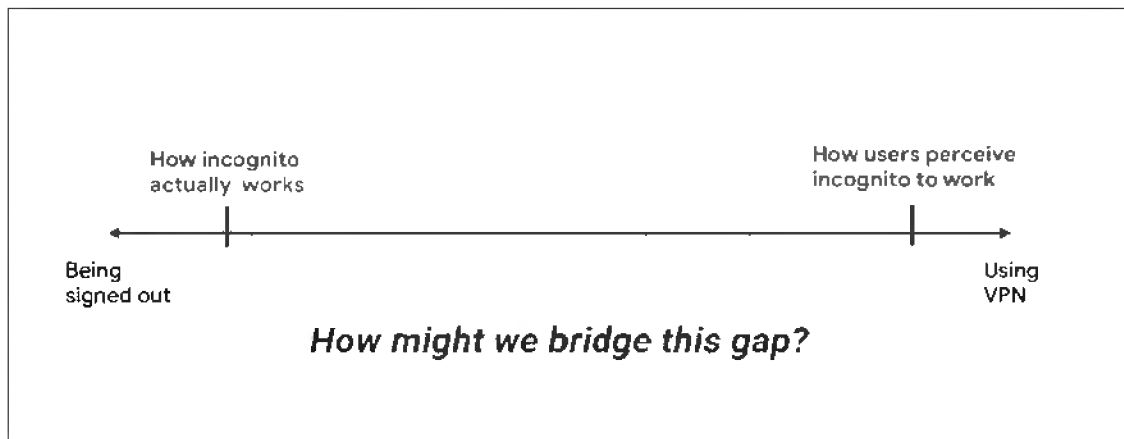


Figure 19. An excerpt from internal Google documents visualizing users' confusion about Incognito mode.

139. And Texans may be surprised to learn that, according to what Google says internally, as opposed to what it represents externally, Incognito mode “Doesn’t protect you against Google or websites tracking you.”

2016-02-17: GYB & Chrome Incognito

Attendees: Sabine, Pauline, Kelsey, Lexie

Incognito mode

- Protects from people who use the same device as you (e.g. spouses)
- Doesn't protect you against Google or websites tracking you
- User's activity is not logged & minimize communication with users from Google
 - If user clicks on auto-complete suggestion (pulling from previous Chrome browsing data)
- Gives you privacy on your local device. Does not make you invisible on the web
 - If you close your last incognito mode on your machine, then there's no history of your activity
- Visual styles
 - Does shield raise a misconception that users think incognito mode is more secure? Working to clarify that it's not more secure than it is
 - Chrome team doing testing before updating visuals; targeting launch Q2
 - Testing shield in gray and blue (GCS)
 - GCS can run for a few days, will have results end of next week (2/26)
 - AI: Pauline to share existing studies

Figure 20. An excerpt from internal Google documents describing what Incognito mode does and does not do.

140. Google's representations about Incognito mode are false, deceptive, and misleading. Not only do users not know that Google is able to and does collect data on them during private browsing, users effectively have no way to avoid much of Google's data-collection practices. Google itself—internally, at least—recognizes the deception that lies within this disconnect.

5. Google Uses Additional Data-Collection Tools to Collect and Store Data About Texans' Incognito Sessions, and Incognito Deceptively Does Not Prevent This.

141. Upon information and belief, even when a Texan enables Incognito mode, when the Texan visits a website that is running Google Analytics or Google Ad Manager, Google's software scripts that drive those programs surreptitiously direct the user's browser to send a secret, separate message to Google's servers. This message contains at least:

- a. The “GET request” sent from the user’s computer to the website. When an individual internet user visits a web page, his or her browser sends a message called a “GET request” to the webpage’s server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user. The copy of the “GET request,” which is sent to Google, enables Google to learn exactly what content the user’s browsing software was asking the website to display. The GET request also transmits a referrer header containing the URL information of what the user has been viewing and requesting from websites online;
 - b. The IP address of the user’s connection to the internet;
 - c. Information identifying the browser that the user is using; and
 - d. The location of the user, if available.
142. The below diagram illustrates the flow of a Texan’s data while in Incognito mode when, for example, clicking on a link to content the Texan wishes to view on ESPN.com. Since ESPN.com is running Google Analytics, Google’s embedded code, written in JavaScript, communicates with the Texan’s browser without alerting the user and, in doing so, covertly duplicates the data communicated between the Texan’s web browser and the ESPN.com website.

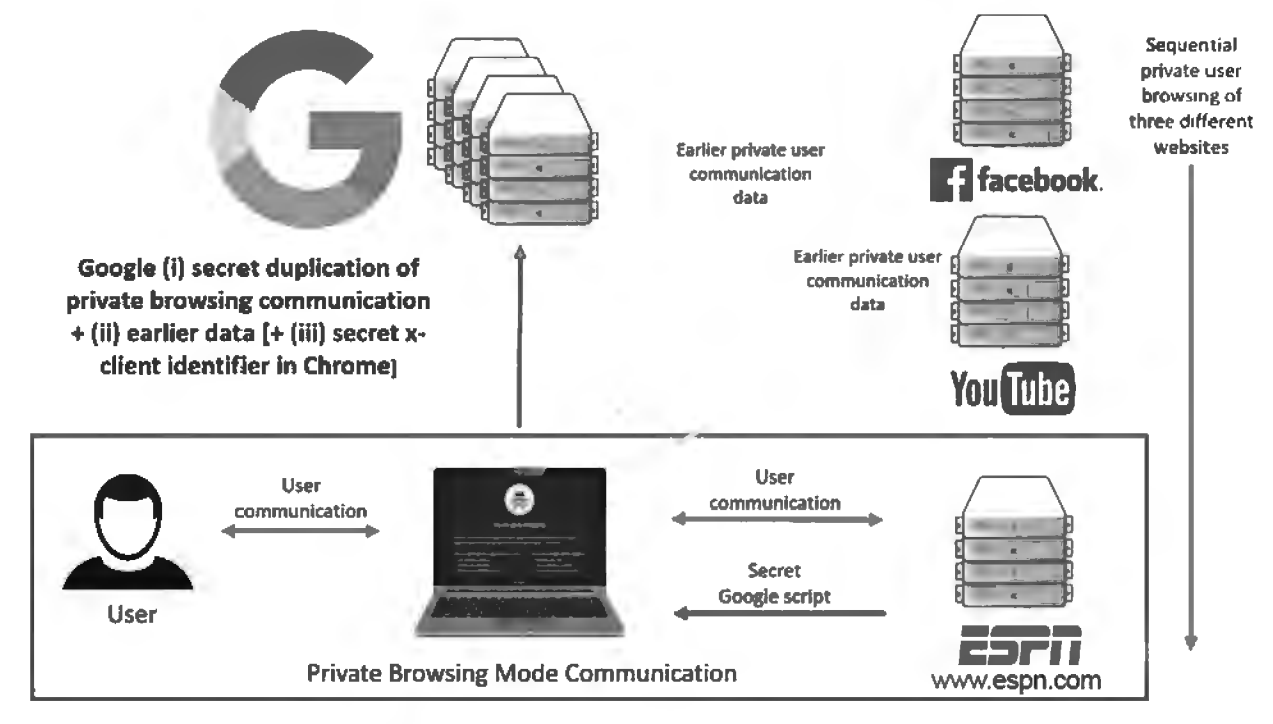


Figure 21. A visual example of how data flows between a Texan's machine, a website running Google Analytics, and Google's servers during an Incognito session.

143. As another example, take a Texan who visits USPS.com while in private-browsing mode. Even after enabling private-browsing mode, Google Analytics and Google Ad Manager continue to track his data. The following screen shot, a feature not customarily presented to the individual and accessible only by using developer tools, demonstrates this:

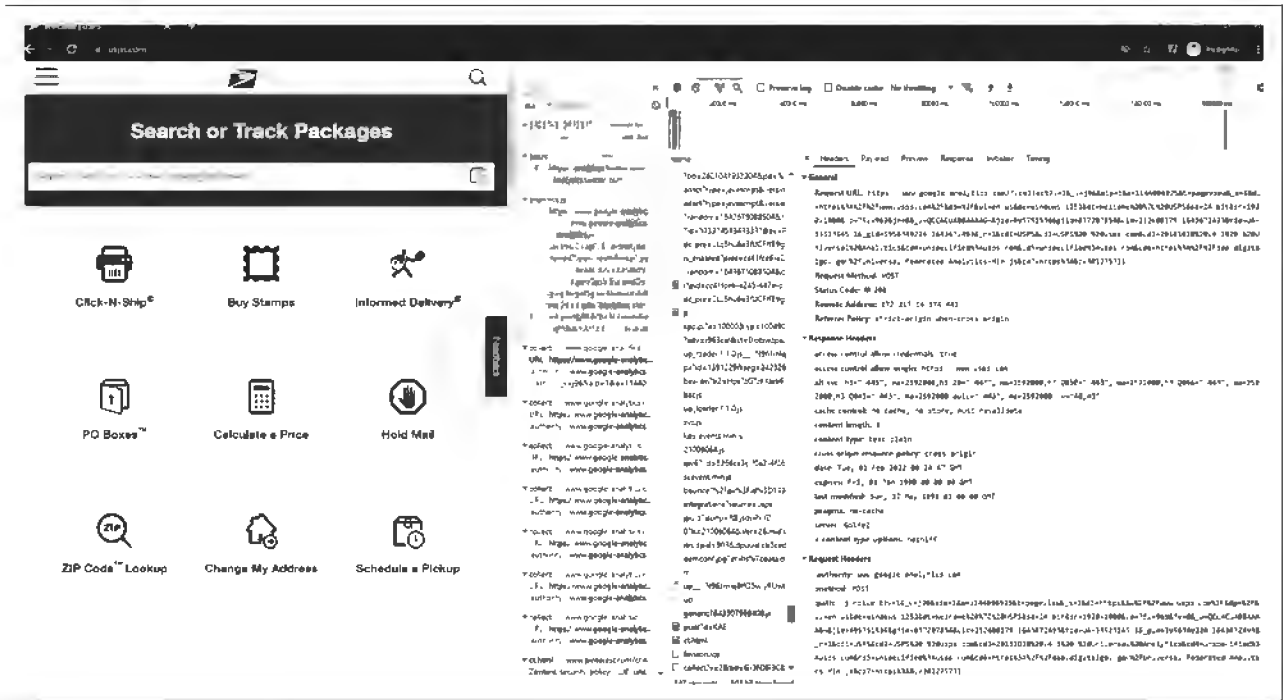


Figure 22. An example of the kind of data tracked when a Texan in Incognito Mode visits a website running Google Analytics and Google Ad Manager.

144. As described above, Google’s secret JavaScript code from Google Analytics causes the user to concurrently send to Google not only a duplicated copy of the requesting webpage with the website but also additional data from the browser, such as cookies, browser information, and device information. And Google’s Ad Manager intercepts not only the user’s communication with the websites, but it concurrently combines the duplicated communications with data from other Google processes.

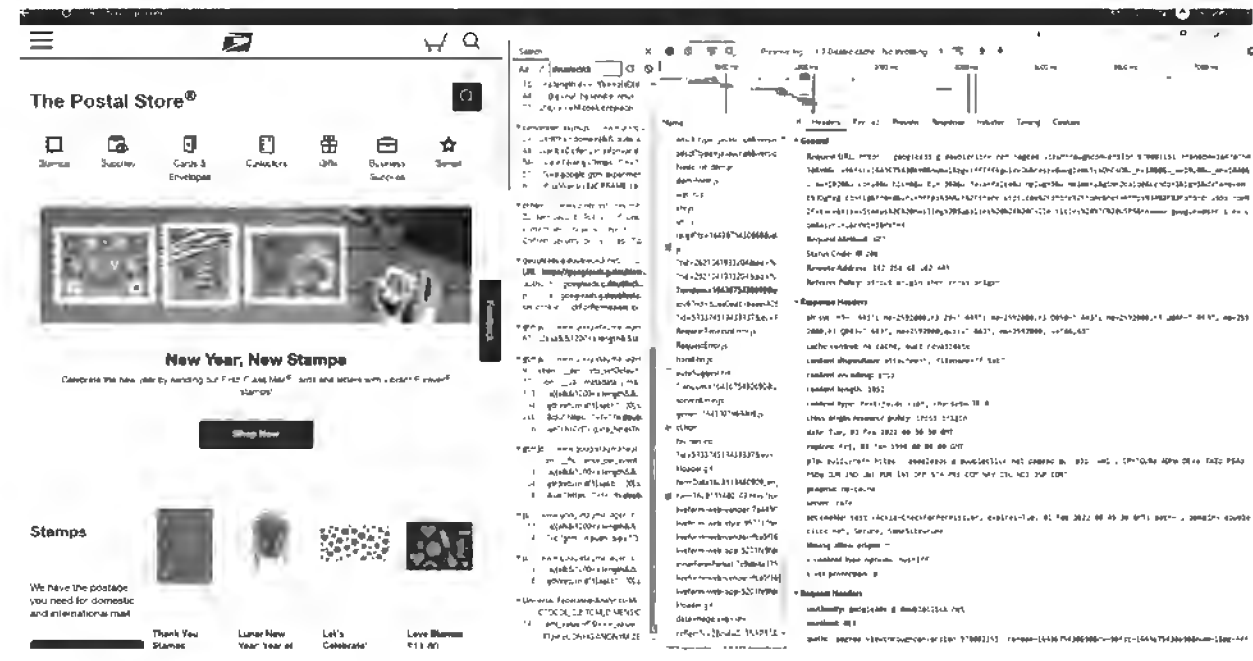


Figure 23. An example of the kind of data tracked when a Texan in Incognito Mode visits a website running Google Analytics and Google Ad Manager.

145. Thus, even when Texans are browsing the internet in Incognito mode, Google continues to track them, profile them, and profit from their data whenever they visit websites using Google Analytics or Google Ad Manager. Said another way, Google collects precisely the type of private, personal information from which Texans wish and expect to be protected even when they have undertaken the steps that Google instructs them to take to obtain that protection. Google’s tracking occurred—and continues to occur—no matter how sensitive or personal Texans’ online activities are and no matter what steps a Texan takes to prevent it.
146. Google does not notify Texans that it is able to collect and manipulate data in the ways identified above, even when the user is in Incognito mode. And Given Google’s persistent representations to the contrary, most Texans would be shocked to learn this—especially

since the operative code and data collection is hidden from the average Texas user. Texans also have no way to remove the operative Google script or to opt out of its functionality.

147. In fact, even though Google changed its Incognito Screen in or around 2020 to allow Texans the option to block third-party cookies, the new Incognito Screen, shown below, deceptively fails to disclose that the new option does *not* prevent tracking by the first-party cookies used by Google Analytics and Google Ad Manager.



Figure 24. A screen capture representing Google's current Incognito Screen.

148. Google's overarching design, at the device level, the account level, and at the website API level, renders it virtually impossible for users to prevent Google from accessing their data,

and Incognito mode is no exception. As Google tells Texans, private browsing modes are supposed to provide users with privacy. Google’s own software, however, appears to enable Google to secretly collect Texans’ data to profile and profit off their personal information. Specifically, Google pierces the purported privacy protections of private-browsing modes like Incognito by deploying tools like Google Analytics.

6. Google Is Able to Unmask Texans By Combining Their Incognito Data with Additional Data.

149. Although Google purportedly terminates cookies (at the device level) generated during a given Incognito session, in certain circumstances, Google is still able to attribute anonymous data created during an Incognito session to a specific Texan user.
150. For starters, Google uses tracking tags that allow Google to catalogue things like a Texan’s device, unique browser, and location data, even during Incognito sessions. This is unsurprising, since Google admits it serves targeted ads with data collected during Incognito mode. The kicker, however, is that Google is capable of linking data and events from a Texan’s Incognito session to searches and conduct the Texan previously conducted while in private-browsing mode and, potentially, with non-private-browsing data, too.
151. Vanderbilt University Professor of Computer Science Douglas Schmidt has written about these issues and has run his own diagnostics to identify the data Google is able to collect on individuals during their “private”-browsing sessions and how.
152. As a baseline, Professor Schmidt’s research demonstrated how Android phones’ frequent “check-in” data sync with Google’s servers contained significant personally identifying information, including the user’s Gmail account, the device MAC address, the International Mobile Equipment Identity (“IMEI”) and Mobile Equipment Identifier (“MEID”), and device serial number. With this information, Google can link a user with an Android

device's permanent identifiers. When that same user interacts with a Google server, such as completing a ReCaptcha user verification, Google receives communications including device identifiers that could link the data generated during that private-browsing session to the user's personal information.

153. Professor Schmidt's testing proceeded with four steps:
- i. First, Professor Schmidt "Opened a new (no saved cookies, e.g. Private or Incognito) browser session (Chrome or other)";
 - ii. Second, he "Visited a 3rd-party website that used Google's DoubleClick ad network";
 - iii. Third, he "Visited the website of a widely used Google service (Gmail in this case)"; and
 - iv. Fourth, he "Signed in to Gmail."
154. According to Professor Schmidt,

53. After completion of step 1 and 2, as part of the page load process, the DoubleClick server received a request when the user first visited the 3rd-party website. This request was part of a series of requests comprising the DoubleClick initialization process started by the publisher website, which resulted in the Chrome browser setting a cookie for the DoubleClick domain. This cookie stayed on user's computer until it expired or until the user manually cleared cookies via the browser settings.

54. Thereafter, in step 3, when the user visited Gmail, they are prompted to log in with their Google credentials. Google manages identity using a "single sign on (SSO)" architecture, whereby credentials are supplied to an account service (signified by *accounts.google.com*) in exchange for an "authentication token," which can then be presented to other Google services to identify the users. In step 4, when a user accesses their Gmail account, they are effectively signing into their Google Account, which then provides Gmail with an authorization token to verify the user's identity.⁵⁴ This process is outlined by Figure 24 in Section IX.E in the Appendix.

55. In the last step of this sign-on process, a request is sent to the DoubleClick domain. This request contains both the authentication token provided by Google and the tracking cookie set when the user visited the 3rd-party website in step 2 (this communication is shown in Figure 11). This allows Google to connect the user's Google credentials with a DoubleClick cookie ID. Therefore, if the users do not clear browser cookies regularly, their browsing information on 3rd-party webpages that use DoubleClick services could get associated with their personal information on Google Account.

Figure 11: Request to DoubleClick.net includes Google's authentication token and past cookies



Figure 25. An excerpt from Professor Douglas Schmidt's research findings.

155. At bottom, if a user is in Incognito mode and accesses a Google service for which the user has a signed-in Google account, Google will generate an authentication token for the user as if the user is signing into their Google Account. At that point, with the user still in Incognito mode, Google is able to link the user's previously anonymous browsing data from the Incognito session with the user's Google Account, effectively unmasking the user

vis-à-vis their private browsing activity that occurred in the session prior to interacting with their Google Account.

156. Professor Schmidt’s research appears to reveal what Google has—internally, at least—recognized as something users ought to know:

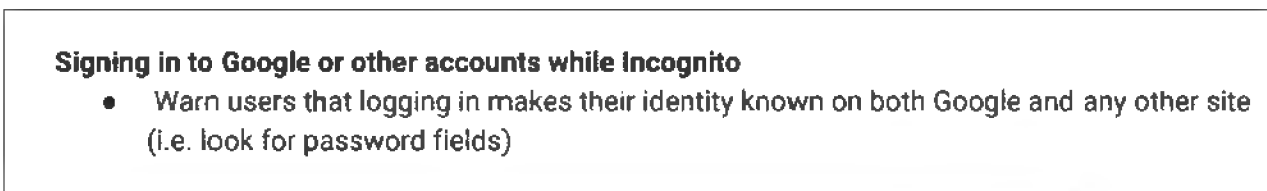


Figure 26. An excerpt from internal Google documents demonstrating Google understood it needed to warn users of the risks of unmasking during Incognito sessions.

157. The critical context is that the core of Google’s business model is data collection and analytics. The bulk of Google’s annual hundreds of billions of dollars in revenue comes from what companies pay Google for data. Because Google has already collected detailed “profiles” on each user and their devices, Google is easily able to associate data collected during a Texan’s private-browsing sessions with that Texan’s pre-existing Google “profile.” And doing so improves the “profile,” which allows Google to sell more targeted data.

XI. CAUSE OF ACTION

Violations of the Texas Deceptive Trade Practices-Consumer Protection Act, TEX. BUS. & COM. CODE ANN. § 17.41 et seq.

158. Defendant, as alleged above and detailed below, has in the course of trade and commerce engaged in false, misleading and deceptive acts and practices declared unlawful in §§17.46(a) and (b) of the DTPA. Such acts include:
- A. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has

a sponsorship, approval, status, affiliation, or connection which he does not have, in violation of DTPA § 17.46(b)(5), including by representing, directly or by implication or omission, that:

1. The Location History setting controlled whether Google retained and used users' location information;
2. That disabling the Location History setting would prevent Google from retaining and using users' location information going forward;
3. The Web & App Activity setting did not impact Google's collection, storage, or use of location information;
4. Users could prevent Google from retaining and using their location information by disabling Google Account settings;
5. Users could review and manage all location data associated with their Google Account and/or otherwise retained by Google for its commercial use;
6. Users had a choice about or could control whether Google collected their personal or location information;
7. Users could prevent Google from using their personal or location to target advertisements by disabling Google Account settings;
8. Users could prevent Google from collecting, storing, and using users' location by adjusting device settings that control whether device location is enabled;
9. Users could prevent Google from collecting, storing, and using users' location by adjusting device settings that control whether device location is shared with specific Google apps;
10. Users could prevent Google from collecting, storing, using, and profiting

from users' data by enabling Incognito mode or another private browsing mode;

11. Users could prevent Google from collecting, storing, using, and profiting from users' data by enabling Incognito mode and blocking third-party cookies;

12. Users could prevent Google from collecting, storing, using, and profiting from users' data by disabling the use of cookies;

13. Users could implement the steps provided by Google to prevent Google from collecting, storing, using, and profiting from users' data;

14. Users could control whether Google and Websites could access, collect, store, use, and profit from their data;

15. That Incognito mode actually meant that a user could keep their browsing private from Google.

B. Representing that an agreement confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law, in violation of § 17.46(b)(12); and

C. Failing to disclose information concerning goods or services which was known at the time of the transaction with the intent to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed in violation of § 17.46(b)(24), including failing to disclose the following material facts:

1. Google continued to collect and store users' location information even with Location History disabled (i.e., turned off);

2. Personal and location information was collected through the Web & App Activity feature;
3. Users cannot not prevent Google from retaining and using users' locations by adjusting Google Account settings;
4. Users cannot prevent Google from using their location to target advertisements by disabling Google Account settings;
5. Google continues to collect location information even when a device's location is turned off; and
6. Google apps that are denied permission to access location data can still obtain that data from other sources available to Google, including other Google apps;
7. Users cannot prevent Google from collecting user data by enabling Incognito mode;
8. Users cannot prevent third-parties from collecting user data by enabling Incognito mode;
9. Users cannot prevent Google from collecting user data by enabling Incognito mode and blocking third-party cookies;
10. Users cannot control Google's access to their personal information through the means provided by Google.
11. Even if users could theoretically control Google's access to their personal information, Google's false, misleading and deceptive statements coupled with its use of dark patterns was designed to ensure that users could not effectively control Google's access to their personal information.

XII. TRIAL BY JURY

159. Plaintiff herein requests a jury trial and will tender the jury fee to the County District Clerk's office pursuant to TEX. R. CIV. P. 216 and the TEX. GOV'T CODE ANN. § 51.604.

XIII. PRAYER FOR RELIEF

160. Plaintiff further prays that Defendant be cited according to law to appear and answer herein; that after due notice and hearing a TEMPORARY INJUNCTION be issued; and upon final hearing a PERMANENT INJUNCTION be issued, restraining and enjoining Defendant, Defendant's officers, agents, servants, employees and attorneys and any other person in active concert or participation with Defendant from violating the DTPA.
161. In addition, Plaintiff respectfully prays that this Court will:
- A. Order Defendant to pay restitution to restore all money or other property taken from identifiable persons by means of unlawful acts or practices;
 - B. Adjudge against Defendant civil penalties in favor of Plaintiff in the amount of not more than \$10,000 per violation of the DTPA;
 - C. Order Defendant to pay Plaintiff's attorney fees and costs of court pursuant to the TEX. GOVT. CODE, § 402.006(c);
 - D. Order Defendant to pay both pre-judgment and post judgment interest on all awards of restitution or civil penalties, as provided by law.
162. 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

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

Darryl Anderson
Texas State Bar No. 24008694
Darryl.anderson@nortonrosefulbright.com

M. Miles Robinson
Texas State Bar No. 24110288
Miles.robinson@nortonrosefulbright.com

Barbara Light
Texas State Bar No. 24109472
Barbara.light@nortonrosefulbright.com

Zachery Newton
Texas State Bar No. 24126971
Zachery.newton@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
(361) 576-6800 – Tel
(361) 576-6196 – Fax

/s/ Kevin D. Cullen

Kevin D. Cullen
State Bar No. 0528625
kcullen@cullenlawfirm.com

CULLEN, CARSNER, SEERDEN AND
CULLEN LLP
P.O. Box 2938
Victoria, Texas 77902
361-573-6318 – Tel

KEN PAXTON
Attorney General

/s/ Shawn 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

Automated Certificate of eService

This automated certificate of service was created by the eFiling system.
The filer served this document via email generated by the eFiling system
on the date and to the persons listed below:

Toni Shah on behalf of Jacob Beach
Bar No. 24116083
toni.shah@oag.texas.gov
Envelope ID: 97743118
Filing Code Description: Petition
Filing Description: Google States PFR
Status as of 2/25/2025 8:29 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Jacob Beach		Jacob.Beach@oag.texas.gov	2/24/2025 7:10:47 PM	SENT
Athena Leyton		athena.leyton@oag.texas.gov	2/24/2025 7:10:47 PM	SENT
Toni Shah		toni.shah@oag.texas.gov	2/24/2025 7:10:47 PM	SENT
Stephen McConnico		smconnico@scottdoug.com	2/24/2025 7:10:47 PM	SENT
Kristina Williams		Kristina.Williams@nortonrosefulbright.com	2/24/2025 7:10:47 PM	SENT
Aaron Nielson		Aaron.Nielson@oag.texas.gov	2/24/2025 7:10:47 PM	SENT
Kevin Cullen		kcullen@culllawfirm.com	2/24/2025 7:10:47 PM	SENT
Ronald Walker		rwalker@walkerkeeling.com	2/24/2025 7:10:47 PM	SENT
Joseph Graham		Joseph.graham@nortonrosefulbright.com	2/24/2025 7:10:47 PM	SENT
Brent Webster		brent.webster@oag.texas.gov	2/24/2025 7:10:47 PM	SENT
Joseph Wolff		Joseph.Wolff@nortonrosefulbright.com	2/24/2025 7:10:47 PM	SENT
Julie Searle		julie.searle@nortonrosefulbright.com	2/24/2025 7:10:47 PM	SENT
Josh Owings		Josh.Owings@nortonrosefulbright.com	2/24/2025 7:10:47 PM	SENT
Marc Collier		Marc.Collier@nortonrosefulbright.com	2/24/2025 7:10:47 PM	SENT
Jim Cole		jcole@cofirmerservice.com	2/24/2025 7:10:47 PM	SENT
Jonathan Patchen		jpatchen@willkie.com	2/24/2025 7:10:47 PM	SENT
Harris Mateen		hmateen@willkie.com	2/24/2025 7:10:47 PM	SENT
Joshua Anderson		janderson@willkie.com	2/24/2025 7:10:47 PM	SENT
Eduardo Santacana		esantacana@willkie.com	2/24/2025 7:10:47 PM	SENT
Benedict Hur		bhur@willkie.com	2/24/2025 7:10:47 PM	SENT
Bryan Lauer		blauer@scottdoug.com	2/24/2025 7:10:47 PM	SENT
Shelby Hart-Armstrong		sharmstrong@scottdoug.com	2/24/2025 7:10:47 PM	SENT
John Ellis		jellis@scottdoug.com	2/24/2025 7:10:47 PM	SENT
Steven Wingard		swingard@scottdoug.com	2/24/2025 7:10:47 PM	SENT

Automated Certificate of eService

This automated certificate of service was created by the eFiling system. The filer served this document via email generated by the eFiling system on the date and to the persons listed below:

Toni Shah on behalf of Jacob Beach
Bar No. 24116083
toni.shah@oag.texas.gov
Envelope ID: 97743118
Filing Code Description: Petition
Filing Description: Google States PFR
Status as of 2/25/2025 8:29 AM CST

Case Contacts

Steven Wingard		swingard@scottdoug.com	2/24/2025 7:10:47 PM	SENT
Robyn Hargrove		rhargrove@scottdoug.com	2/24/2025 7:10:47 PM	SENT
Chris Cook		christopher.cooke@nortonrosefulbright.com	2/24/2025 7:10:47 PM	SENT
Warren Paxton		Kenneth.Paxton@oag.texas.gov	2/24/2025 7:10:47 PM	SENT
Brad Schuelke		Brad.Schuelke@oag.texas.gov	2/24/2025 7:10:47 PM	SENT
Gabriella Gonzalez		Gabriella.Gonzalez@oag.texas.gov	2/24/2025 7:10:47 PM	SENT
Johnathan Stone		Johnathan.Stone@oag.texas.gov	2/24/2025 7:10:47 PM	SENT