

MARK BRNOVICH
ATTORNEY GENERAL
Firm State Bar No. 14000

Joseph A. Kanefield (State Bar No. 15838)
Brunn W. Roysden III (State Bar No. 28698)
Oramel H. Skinner (State Bar No. 032891)
Michael S. Catlett (State Bar No. 025238)
Christopher Slood (State Bar No. 034196)

Assistant Attorneys General
2005 N. Central Ave.
Phoenix, Arizona 85004
Telephone: (602) 542-8958
Beau.Roysden@azag.gov
O.H.Skinner@azag.gov
Michael.Catlett@azag.gov
Christopher.Slood@azag.gov
ACL@azag.gov

[Additional Counsel on Signature Page]

Attorneys for Plaintiff
State of Arizona ex rel. Mark Brnovich,
Attorney General

THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

STATE OF ARIZONA, *ex rel.* MARK
BRNOVICH, Attorney General,

Plaintiff,

v.

GOOGLE LLC, a Delaware limited liability
company,

Defendant.

) Case No: CV2020-006219

) **NOTICE OF LODGING**
) **UNREDACTED COMPLAINT AND**
) **EXHIBITS PURSUANT TO**
) **ARIZONA RULE OF CIVIL**
) **PROCEDURE 5.4(g)(3)**

) Assigned to the Hon. Timothy Thomason

) **(COMPLEX CALENDAR)**

TABLE OF CONTENTS

I.	PROCEDURAL POSTURE AND THE STATE’S REQUESTS.....	1
II.	BACKGROUND.....	1
III.	ARGUMENT	3
A.	The Requirements in Rule 5.4 Apply to the State’s Complaint and Exhibits.....	3
B.	The Public Also has a Constitutional Right to Access the State’s Complaint and Exhibits.....	4
C.	The Public’s Constitutional Right to Access Is Extremely Strong Here.	5
D.	Google Cannot Meet the Requirements of Rule 5.4(c)(2) for Sealing.	7
1.	Publicly Available Information Cannot Be Sealed.	9
2.	Internal Information That Is Not Confidential Cannot Be Sealed.	10
3.	Information Concerning Arizona’s Investigation Cannot Be Sealed.....	12
E.	Google Cannot Meet The Requirements of Rule 5.4 for Sealing Nearly All Exhibits in Their Entirety.....	13
F.	Google Has Waived Any Assertions of Confidentiality.....	14
G.	Google’s Other Likely Arguments Fail.....	15
IV.	CONCLUSION	17

1 The State files this Notice of Lodging pursuant to Civil Rule 5.4(g)(3). The documents
2 being lodged pursuant to Rule 5.4(e) are: Exhibit B, an unredacted version of the Complaint
3 with yellow highlights of the parts that (post-meet and confer) Google will timely seek to seal
4 pursuant to Rule 5.4(g)(4); Exhibit C, unredacted copies of the Complaint’s non-public exhibits
5 with green highlights for portions the State believes *at a minimum* should not be sealed; and
6 Exhibit F, an exhibit identifying “buckets” of information in the Complaint to facilitate the
7 Court’s determination of what, if any, portions meet Rule 5.4(c)(2)’s requirements for sealing.

8 **I. PROCEDURAL POSTURE AND THE STATE’S REQUESTS**

9 This lodging is the first step in the process of determining what parts of the Complaint
10 should be under seal, if any. The next step in the process is Google filing a timely motion to
11 seal. In expectation of that filing, the State respectfully makes two requests. *First*, that the
12 Court deny in full any motion to seal by Google pursuant to 5.4(g)(4), as the Complaint and
13 exhibits that the State is lodging here do not contain materials that meet the strict requirements
14 of 5.4(c)(2). *Second*, to the extent the Court orders any sealing, it should carefully limit the
15 amount sealed so that the “proposed restriction ... is no greater than necessary to preserve the
16 confidentiality of information subject to the overriding interest.” *See* Rule 5.4(c)(2)(C).

17 **II. BACKGROUND**

18 This case arises from an investigation under the Consumer Fraud Act, A.R.S. § 44-1521
19 *et seq.*, into deceptive and unfair acts and practices that relate to Google’s collection, use,
20 storage, and (lack of) deletion of its users’ location data. *See, e.g.*, Complaint ¶¶22-32.

21 On August 13, 2018, the Associated Press published *Google tracks your movements, like*
22 *it or not*, discussing Google’s Location History service, which enables users to view where they
23 have been. At the time, Google informed its users, “with Location History off, the places you
24 go are no longer stored.” But the article revealed that this statement was blatantly false—even
25 with Location History off, Google surreptitiously collects users’ location information through
26 another setting called Web & App Activity and uses that information to sell ads. The AG’s
27 investigation confirmed the findings of the AP article, and also uncovered widespread and
28 systematic use of deceptive and unfair acts and practices by Google to obtain users’ location

1 information—including as part of activating and setting up the user’s Android phone after
2 purchase; advertising its devices and services to users; selling ad placements to advertisers; and
3 serving ads to users as part of Google’s lucrative advertising business.

4 The governing statutory framework gives the Attorney General (“AG”) investigative
5 powers, A.R.S. § 44-1524, and provides that information or evidence provided during an
6 investigation “shall be confidential and shall not be made public unless in the judgment of the
7 attorney general the ends of justice and the public interest will be served by the publication
8 thereof, provided that the names of the interested parties shall not be made public.” A.R.S. § 44-
9 1525. During the investigation, the parties executed a Confidentiality Agreement. April 12,
10 2019 Agreement. (Ex. A). That Agreement acknowledges the framework of A.R.S. § 44-1525,
11 and also allows Google to “mark as ‘Confidential’ any materials or information it produces or
12 otherwise discloses to the AGO that Google reasonably believes contains sensitive information
13 (‘Designated Materials’).” (*Id.* ¶ 3). Google marked “Confidential” the vast majority of
14 information and materials provided during the investigation, regardless of whether they actually
15 contain “sensitive information.” The State has never agreed with Google’s designations.

16 The Agreement recognizes that the State may use Designated Materials in connection
17 with litigation arising from the investigation. The Agreement also allows the State to file
18 Designated Materials in the public record, so long as it “either file[s] the Designated Materials
19 under seal or afford[s] Google at least 10 days advanced notice, in either case consistent with the
20 applicable rules, regulations, and/or orders of the relevant tribunal.” (*Id.* ¶ 9). Importantly, “the
21 AGO reserve[d] the right to oppose any request for sealing, to ask the court to unseal Designated
22 Materials, and/or to challenge any confidentiality designations by Google, in each case in whole
23 or in part.” (*Id.*). Google bears “the burden of defending its designations.” (*Id.*).

24 On May 27, 2020, the State filed a Complaint against Google for violations of the
25 Consumer Fraud Act. The Complaint details extensive unfair and deceptive acts and practices
26 by Google, with citations to documents and testimony obtained during the AG’s investigation.
27 The Complaint also describes Google’s efforts to delay and impede the investigation. The State
28 spent considerable time drafting the Complaint in a manner to exclude materials it believed

1 would meet the requirements of Rule 5.4(c)(2) for filing under seal. But to permit the parties to
2 follow the Rule 5.4(g) process, the State redacted any material Google had designated
3 “Confidential” during the investigation, and also allegations relying upon such information.

4 On the same day (May 27), the State provided notice to Google as follows: “[I]t is the
5 judgment of the Attorney General that, consistent with Arizona Rule of Civil Procedure 5.4, the
6 ends of justice and the public interest will be served by making these materials public, *see*
7 A.R.S. § 44-1525.” The State further provided 10 days’ notice to Google, pursuant to ¶9 of the
8 Confidentiality Agreement, that the State intends to file the entire unredacted Complaint
9 (including exhibits) in the public record. On July 15, 2020, Google confirmed that it seeks to
10 seal “all information that is redacted in the version of the Complaint filed publicly on May 27,
11 2020,” including a vast majority of the exhibits. (Ex. D). The only exceptions were seven
12 exhibits that Google has agreed could be filed publicly—subject to heavy redactions. The State
13 is filing these redacted exhibits publicly.

14 During the meet-and-confer process (which spanned six weeks and included many hours
15 of telephone calls and extensive written correspondence), Google offered no real justification for
16 sealing any of the information and materials that it seeks to seal, much less all of it. The State
17 disagrees with Google’s attempt to seal any portion of the Complaint or exhibits and now
18 submits this Notice so that Google can defend its proposed sealing and redactions to the Court.

19 **III. ARGUMENT**

20 **A. The Requirements in Rule 5.4 Apply to the State’s Complaint and Exhibits.**

21 Under Rule 5.4(c)(2), the Court may seal a “document” only if it expressly finds (i) “an
22 overriding interest exists that supports filing the document under seal and overcomes the right of
23 public access to it,” (ii) a “substantial probability exists” that the party seeking to file under seal
24 would be prejudiced without the sealing of materials, (iii) “the proposed restriction on public
25 access to the document is no greater than necessary to preserve the confidentiality of the
26 information subject to the overriding interest,” and (iv) “no reasonable, less restrictive
27 alternative exists to preserve the confidentiality of the information subject to the overriding
28 interest.” Rule 5.4(b)(1) broadly defines a “document” as “any filing, exhibit, record, or other

documentary material to be filed or lodged with the court.” The Complaint and exhibits clearly fall within the definition of a “document,” and thus Google must satisfy the four requirements in Rule 5.4(c)(2) if any portion of the State’s Complaint or exhibits are to be sealed.

B. The Public Also has a Constitutional Right to Access the State’s Complaint and Exhibits.

Rule 5.4(c)(2)’s “substantive standards are drawn from federal and Arizona case law, and reflect the constitutional presumption favoring the public’s right of access to court proceedings.” Rule 5.4, comment 3; *see also* Ariz. R. Supreme Ct. 123(c)(1) (“Historically, this state has always favored open government and an informed citizenry. In the tradition, the records in all courts and administrative offices of the Judicial Department of the State of Arizona are presumed to be open to any member of the public . . .”). The constitutional right of public access is strongly presumed for “civil proceedings and associated records and documents,” including the case-initiating complaint. *Courthouse News Serv. v. Planet*, 750 F.3d 776, 786 (9th Cir. 2014). The public’s right of access under the Arizona Constitution is even broader than under the U.S. Constitution. *Mtn. States Tel. & Tel. v. ACC*, 150 Ariz. 350, 355 (1989).

Not only does the express language of Rule 5.4(b)(1) include complaints as a “document” triggering its requirements, but the public has a constitutional right to immediately access the Complaint upon filing. *Courthouse News Serv. v. Planet*, 947 F.3d 581, 591–94 (9th Cir. 2020) (“*Planet III*”). Immediate public access “‘plays a particularly significant role’ in the public’s ability to ably scrutinize ‘the judicial process and the government as a whole.’” *Id.* at 592; *see also Bernstein v. Bernstein Litowitz Berger & Grossmann LLP*, 814 F.3d 132, 139 (2d Cir. 2016) (“easily conclud[ing]” that “presumption of access” applies to complaint); *TriQuint Semiconductor, Inc. v. Avago Techs.*, 2010 WL 2474387, at *1 (D. Ariz. June 11, 2010) (“motions to seal the complaint must meet the compelling reasons standard”); *Reyna v. Arris Int’l, PLC*, No. 17-CV-01834-LHK, 2018 WL 1400513, at *2 (N.D. Cal. Mar. 20, 2018) (“courts have held that the compelling reasons standard applies to the sealing of a complaint precisely because the complaint forms the foundation of the lawsuit”). In *Bernstein*, the district court denied a *joint* motion to seal a complaint that had been quickly dismissed, rejecting the

1 parties' contention that the information should be sealed because of "confidential client
2 information." *Bernstein*, 814 F.3d at 136. The Second Circuit affirmed: "pleadings—even in
3 settled cases—are Judicial records subject to a presumption of public access." *Id.* at 140.

4 The same goes for the Complaint's exhibits. Not only does Rule 5.4(b)(1) define
5 "document" to include an "exhibit," but the constitutional right of public access also applies to
6 exhibits attached to a complaint. *FTC v. AbbVie Prods.*, 713 F.3d 54, 63 (11th Cir. 2013)
7 (public has a presumptive right to access complaint, including exhibits). Arizona courts view
8 exhibits as part of the complaint "for all purposes." *Kyles v. Contractors/Eng'rs Supply, Inc.*,
9 190 Ariz. 403, 406–07 (App. 1997). For example, on a motion to dismiss, "[a] complaint's
10 exhibits . . . are not 'outside the pleading.'" *Coleman v. City of Mesa*, 230 Ariz. 352, 356
11 (2012). Indeed, Google has already filed a motion to dismiss, which cites individual exhibits
12 (*see, e.g.*, Mot. at 4:11, 5:1, 9:21, 9:25) and even purports to characterize the entire "1,200 pages
13 of exhibits" (*id.* at 10:22–11:2). Like the complaint itself, the exhibits are "judicial records" and
14 presumptively public.

15 **C. The Public's Constitutional Right to Access Is Extremely Strong Here.**

16 "When the litigation involves matters of significant public concern," the public's right of
17 access to court records "may be asserted more forcefully." *Unknown Parties v. Johnson*, No.
18 CV-15-00250-TUC-DCB, 2016 WL 8199309, at *4 (D. Ariz. 2016); *see also In re Coordinated*
19 *Pretrial Proceedings in Petroleum Prods. Antitrust Litig.*, 101 F.R.D. 34, 38–39 (C.D. Cal.
20 1984) (finding significant public concern where collusion to raise retail oil prices "affected the
21 lives of all Americans"); *Lockyer v. Safeway*, 355 F.Supp.2d 1111, 1124 (C.D. Cal. 2005)
22 (unsealing records showing evidence of Sherman Act violations by grocery stores); *Apple, Inc.*
23 *v. Samsung Elecs. Co.*, No. 12-CV-00630-LHK, 2012 WL 2936432, at *2 (N.D. Cal. July 18,
24 2012) (denying motion to seal where a "plethora of media and general public scrutiny of" court
25 proceedings showed significant public interest and created a "strong presumption of public
26 access"); *Lucy Chi v. Univ. of S. Cal.*, No. 2:18-cv-04258-SVW-GJS, 2019 WL 3315282, at *7
27 (C.D. Cal. May 21, 2019) (no compelling interest in light of "extensive media coverage" and
28 where public access would "further the public narrative" about important societal issues).

1 Here, the serious allegations raised in the Complaint against Google affect millions of
2 Arizonans (as well as 120 million Americans) who are Android users (as of 2018)¹—plus many
3 other Arizonans who give Google their location information through other means, such as
4 Google apps. The State brought this action in light of Google’s illegal business practices
5 concerning its collection, use, storage, and deletion of its users’ highly sensitive location
6 information. (*See* Compl. ¶¶ 1–7). The location data collected is a critical part of Google’s
7 advertising business, which generates \$135 billion *yearly*. (*See id.* ¶¶ 3–5).

8 The public has a significant interest in these proceedings, especially given that their data
9 is obtained through violations of user privacy and consent. That major news outlets reported on
10 the Complaint mere hours after it was filed, only reinforces this fact that this is a matter of major
11 public concern.² Indeed, it is not just the underlying facts but also the very fact that the AG has
12 taken action that is a matter of public concern, particularly given the robust public discussion
13 about regulation of technology companies (and actions by tech companies in light of this
14 potential government regulation and enforcement). The Complaint *itself* continues to be cited
15 by major news outlets as part of this public discussion and debate. *See, e.g., Google makes*
16 *auto-deleting data the default for new accounts*, CNet.com (June 24, 2020) (specifically noting
17 that this major change in Google’s practices “comes as Google already faces severe criticism
18 over its data collection policies from lawmakers and state officials. Last month, the search giant
19 was hit by a consumer fraud lawsuit filed by Arizona Attorney General Mark Brnovich, alleging
20 the search giant deceives its users in order to collect location data from their phones. Brnovich’s
21 complaint accuses Google of leading people to believe they disabled settings for gathering that
22 type of information, when the settings were still turned on.”).³ Information in the Complaint and
23 exhibits is critical to that on-going public discourse. *See Planet III*, 947 F.3d at 589.

24
25 ¹ *See* <https://www.statista.com/statistics/232786/forecast-of-android-users-in-the-us>.

26 ² *See, e.g.,* <https://www.washingtonpost.com/technology/2020/05/27/google-android-privacy-lawsuit/>;
27 <https://www.reuters.com/article/us-google-arizona-lawsuit/u-s-state-of-arizona-files-consumer-fraud-lawsuit-against-google-idUSKBN2333CP>.

28 ³ *See* <https://www.cnet.com/news/google-makes-auto-deleting-data-the-default-for-new-accounts/>

1 Furthermore, “the State has a strong interest in informing its citizens about this suit that
2 was brought on their behalf.” *Lockyer*, 355 F.Supp.2d at 1125–26. The CFA is a remedial
3 mechanism “designed to root out and eliminate unlawful practices in merchant-consumer
4 transactions.” *Powers v. Guaranty RV Inc.*, 229 Ariz. 555, 561 (2012). Thus, “the public’s
5 interest in access to a proceeding involving the State’s allegations of *harm to the public* weighs
6 especially heavily in favor of access.” *Lockyer*, 355 F.Supp.2d at 1124 (emphasis in original).
7 The AG firmly believes that the information should be fully available to the public.

8 **D. Google Cannot Meet the Requirements of Rule 5.4(c)(2) for Sealing.**

9 Google cannot show that the unredacted Complaint and exhibits should be sealed.
10 Google’s unilateral designations do not establish that the materials are confidential, nor are they
11 a basis for sealing information so designated. Per the Confidentiality Agreement, the AGO can
12 challenge designations and oppose any efforts to seal, and Google bears the burden of defending
13 its designations. (Ex. A ¶ 9). A confidentiality agreement by itself does not warrant sealing a
14 document filed with the court. *TriQuint Semiconductor, Inc. v. Avago Techs. Ltd.*, No. CV 09-
15 1531-PHX-JAT, 2010 WL 2474387, at *1 (D. Ariz. June 11, 2010). Even for materials
16 produced subject to a protective order—which is not the case here—the producing party’s
17 designation is insufficient to establish that the materials are in fact “confidential,” much less an
18 interest that overcomes the right of public access. *Kamakana v. City & Cty. of Honolulu*, 447
19 F.3d 1172, 1183 (9th Cir. 2006) (protective order insufficient for sealing).

20 Google also cannot satisfy any of the requirements contained in Rule 5.4(c). Google
21 cannot substantiate “an overriding interest” for the materials it seeks to seal, much less one that
22 overcomes “the right of public access to it,” as required by Rule 5.4(c)(2)(A). On the contrary,
23 much of the information that Google seeks to seal is publicly available, discernible from public
24 materials, or simply “internal” Google information (available to thousands of employees) that is
25 not particularly sensitive. Nor has Google substantiated any particular prejudice—at least not
26 during the month-and-a-half meet-and-confer process—that it would suffer “without the sealing
27 of materials.” Rule 5.4(c)(2)(B). Instead, Google simply wants to prevent the public from
28 seeing the details corroborating the AG’s findings. That is not a basis for sealing the materials.

1 Equally problematic is the vast scope of Google’s proposed redactions and request for
2 sealing. Google’s proposed restriction on public access must be “no greater than necessary to
3 preserve the confidentiality of the information subject to the overriding interest,” and Google
4 must show that “no reasonable, less restrictive alternative exists to preserve the confidentiality
5 of the information subject to the overriding interest.” Rule 5.4(c)(2)(C), (D). Notably, courts
6 often deny a motion to seal altogether when the parties seek to redact entire swaths of
7 information that are not narrowly tailored. *See, e.g., D’Agnese v. Novartis Pharm. Corp.*, No.
8 CV 12-0749-PHX-JAT, 2012 WL 3744717, at *2 (D. Ariz. Aug. 27, 2012) (no sealing
9 warranted—even where the documents contained “internal company communications”—where
10 defendant failed to “identify and redact only information that it claims is confidential”); *Am.*
11 *Traffic Solutions, Inc. v. Redflex Traffic Sys.*, No. No. CV-08-02051-PHX-FJM, 2010 WL
12 481408, at *2 (D. Ariz. Feb. 8, 2010) (denying motion to seal where “[t]he parties make no
13 attempt to describe the specific portions of documents that they believe meet [the compelling
14 reasons] standard”); *Apple Inc. v. Samsung Elecs. Co.*, No. 11-CV-01846 LHK (PSG), 2012 WL
15 4120541, at *2 (N.D. Cal. Sept. 18, 2012) (denying motions to seal under the more lenient
16 “good cause” standard where redactions were not narrowly tailored).

17 During the investigation, Google designated as “confidential” nearly every document
18 produced, every page of every examination and every word in every written discovery response.
19 In the Complaint, Google likewise wants to redact anything and everything that derives from the
20 investigation. For example, Google seeks to redact entire portions of the Complaint, the entirety
21 of nearly all exhibits, and all quotations or information derived from any testimony, document or
22 other information provided during the investigation. Google also seeks to redact most of the
23 specifics concerning its wrongdoing in the Complaint. (*E.g.*, Compl. § IV). Google even insists
24 on redacting names of witnesses who were examined—even though Google routinely releases
25 public statements in the press attributable to these same employees. Thus, Google’s proposed
26 sealing and redactions would significantly undermine “the public’s ability to ably scrutinize”
27 this matter of great public interest, *Planet III*, 947 F.3d at 592, even as its PR team has accused
28 the State of “mischaracteriz[ing]” its services.

1 For the court’s convenience, the State has divided the provisionally redacted information
2 into categories or “buckets” based on the nature of that information: (i) information that is
3 publicly available or ascertainable, (ii) information that—although not necessarily public—is
4 not confidential, and (iii) information that concerns the State’s underlying investigation of
5 Google. The State spent hours meeting and conferring with Google, line-by-line, to confirm the
6 portions of the Complaint that fit into each “bucket”; Google never agreed or disagreed. At the
7 conclusion of this six-week effort, Google purported to categorize the exhibits into five new
8 categories (Ex. D at 2), but Google never explained what materials fit into any category.

9 **1. Publicly Available Information Cannot Be Sealed.**

10 Much of the information Google seeks to seal is either publicly available or readily
11 ascertainable. (*See* Ex. F at 1–4). *Orca Commc’ns Unlimited, LLC v. Noder*, 233 Ariz. 411, 417
12 (App. 2013) (“Information easily or readily available to the public remains public knowledge
13 and not protectable as confidential information even if a member of the public may have to
14 expend substantial time to gather it and comprehend its significance.”), *aff’d and depublished in*
15 *part on other grounds*, 236 Ariz. 180 (2014). The State opposes Google’s request.

16 This bucket mostly consists of information relating to Google’s various user-facing
17 products, features, settings and public information about Google and its policies. Google
18 purports to make this information available to the public including through Google’s public-
19 facing help pages, privacy policies, and the open source Android Operating System, so it is
20 unclear on what basis Google seeks to seal the information. During the parties’ discussions,
21 Google failed to articulate any basis for sealing this information, apart from the fact that the
22 information is contained in documents or testimony that Google unilaterally marked as
23 “confidential.” That is not a proper basis for sealing court records. *PCT Int’l Inc. v. Holland*
24 *Electronics LLC*, No. CV-12-01797-PHX-JAT, 2014 WL 6471419 at *3 (D. Ariz. Nov. 18,
25 2014) (“Because PCT has publicly disclosed [the information] PCT has not shown that
26 these documents should be filed under seal.”).

27 Google also fails to substantiate any basis for sealing the names, much less *titles*, of
28 witnesses. Most of these are individuals designated as corporate representatives, and all of them

1 worked on matters “at the heart of [the] case.” *Johnson*, No. CV-15-00250-TUC-DCB, 2016
2 WL 8199309, at *5 (finding no compelling reason to redact names despite privacy and
3 relevancy objections). Many of these individuals—including those identified in paragraphs 52,
4 62, 71 and 93—are often named and quoted in the press. Google cannot explain, much less
5 substantiate, why any of these individuals would be subject to harassment. *See State of Arizona*
6 *ex. rel. Brnovich v. Kapoor*, No. CV2019-010695, Complaint, ¶ 49 (Ariz. Super. Ct. July 17,
7 2019) (naming a defendant’s employee); *see also Seattle Times Co. v. Rhinehart*, 467 U.S. 20,
8 26 (1984) (sealing names only after affidavits describing threats of physical harm and defaming
9 statements were submitted); *Apple*, No. 11-CV-01846 LHK (PSG), 2012 WL 4120541, at *2
10 (denying motion to seal under the more lenient “good cause” standard “descriptions of exhibits
11 and names of deposed Apple employees”).

12 Google also invokes the language about “interested parties” in A.R.S. § 44-1525 as a
13 basis for redacting names, (Ex. D at 2), but that provision has nothing to do with sealing
14 information in a judicial document. Nor does it purport to override the constitutional protections
15 discussed here. Witnesses are not “interested parties.” The statutory language creates a narrow
16 exception to the general public records law so as to protect the integrity of the AG’s consumer
17 fraud investigations, which is why the AG has statutory authority to make materials public. *See*
18 *Carlson v. Pima County*, 141 Ariz. 487, 490 (1984). Before 1980, the statute provided that
19 “[n]o information or evidence provided the attorney general by a person pursuant to this article
20 shall be admitted in evidence, or used in any manner whatsoever, in any criminal prosecution.”
21 Laws 1980, Ch. 76, § 4. That year, the Legislature removed that limitation (*id.*); since then,
22 there has never been a limitation on how the AG can use materials produced during an
23 investigation in later civil proceedings, including by relying on them to make assertions in a
24 publicly available complaint.

25 **2. Internal Information That Is Not Confidential Cannot Be Sealed.**

26 The second bucket of information Google seeks to seal includes information that is not
27 confidential, even if it is not necessarily “public.” This includes (i) internal communications
28 commenting on Google’s products and services, (ii) information concerning Google’s internal

1 treatment of location data, (iii) Google’s communications with and information regarding third
2 parties, (iv) the names and definitions of internal Google platforms and services, and (v) the
3 names of Google witnesses examined in this investigation and appearing in the exhibits. (Ex. F
4 at 5–7). The State opposes Google’s request to seal this information.

5 As an initial matter, Google cannot substantiate any basis for sealing internal
6 communications, information concerning Google’s internal treatment of location data, and
7 communications with third parties (subcategories (i) through (iii)). In meet-and-confer
8 discussions, Google has simply pointed out that the information is “non-public.” But that is not
9 a proper basis for sealing court records. *Bernstein*, 814 F.3d at 136; *Ingram v. Pac. Gas & Elec.*
10 *Co.*, No. 12-CV-02777-JST, 2013 WL 5340697, at *3 (N.D. Cal. Sept. 24, 2013) (“PG & E’s
11 argument that the guidelines constitute a trade secret conflates trade secrets with ordinary
12 secrets. Information does not have value to a competitor merely because the competitor does not
13 have access to it.”) (internal quotation marks omitted). Indeed, “general assertions that the
14 information is confidential or a trade secret” or “conclusory statements” that disclosure would
15 cause competitive harm is not sufficient to provide an overriding interest to seal otherwise
16 public materials.⁴ *Allstate Ins. Co. v. Balle*, No. 2:10-CV-02205-APG-NJ, 2014 WL 1300924,
17 at *1 (D. Nev. March 27, 2014) (denying motion to seal) (internal quotation marks omitted).
18 Despite the State giving Google ample opportunity during the meet and confer process, Google
19 cannot show that any particular information in the Complaint is a trade secret, much less that
20 disclosure would cause Google financial or other harm. And Google has never explained why it
21 would be prejudiced from the disclosure of this information. Rule 5.4(c)(2)(B).

22 Nor has Google shown that its interest—whatever it may be—overrides the presumption
23 of public access. On the contrary, consumers have a strong interest in learning how their own
24

25 ⁴ In fact, in many instances, this information is already available to the public. *See, e.g.*
26 <https://www.linkedin.com/in/darshan-thaker-b46aa847/> (referring to “HULK (Holistic User-
27 Location Knowledge)”;
28 <https://patentimages.storage.googleapis.com/c8/69/e6/2809a5d75cc2af/US20130254309A1.pdf>
at 5 (referring to “IPGeo services” used to “determine approximated geographical location” via
IP address).

1 data is surreptitiously collected and used by Google. *See FTC v. Amazon.com, Inc.*, No. C14-
2 1038-JCC, 2016 WL 3382532, at *2 (W.D. Wash. June 20, 2016). (*See also supra* § III.C
3 (citing cases involving matters of significant public concern)). Given the wrongdoing alleged in
4 this case—and given Google’s public response—both the U.S. and Arizona constitutions protect
5 the public’s right to evaluate “what [Google] officials knew and when, how they designed and
6 targeted their product, consumers’ response, and [Google]’s policy changes.” *Amazon.com,*
7 *Inc.*, No. C14-1038-JCC, 2016 WL 3382532, at *2 (finding strong public interest in access to
8 court records). If all that weren’t enough, Google cannot even show that its proposed wholesale
9 sealing of this information “is no greater than necessary” or that it is the least restrictive means
10 to preserve any overriding interest (Rule 5.4(c)(2)(C) and (D)).

11 This is not the first time Google has attempted to seal information based only on
12 generalized assertions of harm. In *Dunbar v. Google, Inc.*, Google sought to seal portions of the
13 plaintiff’s motion for leave to file a third amended complaint. No. 5:12-cv-003305-LHK, 2012
14 WL 6202719, at *1 (N.D. Cal. Dec. 12, 2012). The information in that motion, according to
15 Google, needed to be sealed because they described confidential technical aspects of how
16 Google scans for, uses, and stores data, “including for the delivery of personalized
17 advertising”—similar to the facts at issue here—and “that disclosing this information would
18 allow Google’s competitors to ‘examin[e] the mechanisms that Google designed for its own
19 proprietary use,’ thereby providing Google’s competitors with ‘an unfair advantage in designing
20 their own systems.’” *Id.* at *3. But the court was not persuaded by these generalized reasons,
21 even under the more lenient “good cause” standard of Fed. R. Civ. P. 26(c), because Google
22 failed to make a particularized showing as to each document it sought to seal by, for example,
23 explaining the specific unfair advantage competitors would earn if exposed to each piece of
24 information. *Id.* at *3–4; *see also id.* at *7 (denying motion to seal deposition excerpts).

25 **3. Information Concerning Arizona’s Investigation Cannot Be Sealed.**

26 The State also opposes Google’s attempt to seal nearly all of Section IV of the
27 Complaint, which describes the AG’s pre-Complaint investigation. (*See* Ex. F at 8). Google’s
28 attempt to hide its wrongdoing from the public only demonstrates that Google’s actions have

1 been willful and intentional. *See* A.R.S. § 44-1531(B); *see also State ex rel. Corbin v. United*
2 *Energy Corp. of Am.*, 151 Ariz. 45, 51–52 (App. 1986). Google contends that these materials
3 must be sealed because the investigation itself was “confidential.” (Ex. D at 2). But that bald
4 assertion does not overcome the strong presumption of public access, particularly where they are
5 directly relevant to the State’s underlying cause of action.

6 Again, such investigations are confidential to protect the integrity of the AG’s consumer
7 fraud investigations, as well as the identity of complainants and victims (*see supra* § III.D.2)—
8 concerns which are no longer present here. *See also Kamakana*, 447 F.3d at 1183 (reliance on
9 protective order not sufficient to seal documents). The AG is vested with authority to publicly
10 disclose his investigation if “in the judgment of the attorney general the ends of justice and the
11 public interest will be served by the publication thereof, provided that the names of the
12 interested parties shall not be made public.” A.R.S. § 44-1525. Given that this is a matter of
13 great public interest and concern, the AG believes that the entirety of Section IV should be
14 publicly available.

15 **E. Google Cannot Meet The Requirements of Rule 5.4 for Sealing Nearly All**
16 **Exhibits in Their Entirety.**

17 Google’s bases for sealing the exhibits filed with the Complaint are (i) that they were
18 included among Google’s blanket confidentiality designations in the underlying investigation,
19 and (ii) they “are the kind of documents that courts routinely maintain under seal.” (Ex. D at 2).
20 As explained, the Confidentiality Agreement does not prevent the State from filing them
21 publicly. In any case, Google has the burden to explain, *for each piece of information*, the
22 specific “overriding interest,” how it would be prejudiced by disclosure, how its proposed
23 restriction (wholesale sealing) is no greater than necessary, and how no reasonable, less
24 restrictive alternative (such as targeted redactions) exists. Rule 5.4(c)(2); *Dunbar*, No. 5:12-cv-
25 003305-LHK, 2012 WL 6202719, at *1 (generalized assertions of harm not sufficient); *Allstate*,
26 No. 2:10-CV-02205-APG-NJ, 2014 WL 1300924, at *1 (same); *Am. Traffic Solutions*, No. CV-
27 08-02051-PHX-FJM, 2010 WL 481408, at *2 (denying motion to seal for failure to “describe
28 the specific portions of documents” meeting the “compelling reasons” standard). Despite

1 repeatedly requesting Google provide this information during the meet and confer process,
2 Google failed to do so. Indeed, the State has long asked Google to sort the exhibits it seeks to
3 seal into categories or “buckets” for the Court’s ease of review. Google failed to do even that.
4 Days before the State filed this Notice, Google finally proposed buckets, but it did not populate
5 them with the exhibits or explain with specificity why each (or even any) of the exhibits met the
6 standard described in Rule 5.4(c)(2). (*See* Ex. D at 2). Because Google cannot meet the
7 stringent requirements of Rule 5.4(c)(2) with respect to the State’s exhibits, the Court should
8 permit them to be publicly filed.

9 **F. Google Has Waived Any Assertions of Confidentiality.**

10 Google’s proposed sealing is particularly problematic given Google’s own public
11 statements regarding the subject matter of this case and its public filings in this case. Google
12 itself expends significant resources monitoring this media attention, including the August 2018
13 AP article that instituted the AG’s investigation. (*See* Compl. ¶¶ 54–57). Google has also
14 invited this public discussion over its location data practices. In response to this lawsuit, Google
15 claimed that the State “mischaracterized [its] services.”⁵ And that “[it] look[s] forward to
16 setting the record straight.” *Id.* Google cannot publicly accuse the State of mischaracterizing
17 the Designated Materials while at the same time preventing the public from reviewing those
18 materials. *Cf. Mendoza v. McDonald’s Corp.*, 222 Ariz. 139, 155 (App. 2009) (attorney-client
19 privilege waived where used as both sword and shield).

20 More fundamentally, Google has now filed a motion to dismiss—on the public docket—
21 that expressly seeks a ruling with respect to the sufficiency of the Complaint, including the
22 exhibits. Google publicly challenges (and often describes) the very allegations that it seeks to
23 seal. For example, Google publicly mischaracterizes the State’s allegations concerning
24 Google’s interactions with OEMs (*see* Mot. at 14 (suggesting that the State is supposedly trying
25 to assert claims on behalf of OEMS)), while trying to seal the detailed allegations and
26

27 ⁵ [https://www.theverge.com/2020/5/27/21272625/arizona-ag-sues-google-location-tracking-](https://www.theverge.com/2020/5/27/21272625/arizona-ag-sues-google-location-tracking-android-allegations)
28 [android-allegations](https://www.theverge.com/2020/5/27/21272625/arizona-ag-sues-google-location-tracking-android-allegations).

1 supporting documents showing how Google coopted OEMs into Google’s scheme for deceiving
2 consumers. (*E.g.*, Compl. ¶¶ 114-128, 142, 161j). Similarly, Google publicly contends that the
3 Complaint fails to allege intent (Motion at 13), yet Google redacts large swaths of the Complaint
4 and exhibits that show Google acted knowingly and deliberately (*e.g.*, Compl. ¶¶ 26, 30, 43-47,
5 49, 61, 65–70, 75, 77, 81–86, 88-89, 94, 99–104, 107, 109, 114–28, 131, 134–36). Google
6 likewise redacts all allegations concerning its delay and impeding of the AG’s investigation (*Id.*
7 ¶¶ 138–54), which further evidences Google’s willfulness.

8 In other instances, Google publicly describes much of the same information that it wants
9 to seal in the Complaint. For example, Google wants to seal nearly all allegations concerning
10 ads personalization, including the fact that Google still serves location-based ads when users opt
11 out. (*E.g.*, Compl. ¶¶ 9e, 98–104, 161p, 161q). Even so, Google discloses the same information
12 in its own motion, while citing the paragraphs that are redacted. (Mot. at 13:3-5). Similarly,
13 Google purports to characterize allegations relating to the Location Master and System Updates,
14 while citing to paragraphs 91, 105-09 and 161f of the Complaint, which Google has fully or
15 substantially redacted. (Mot. at 12:20-23). Google insists its services are not a “sale,” (*id.* at 8),
16 but Google wants to seal the seemingly non-confidential testimony explaining what
17 consideration is exchanged (*e.g.*, Compl. 8:23-25). Painting with broad strokes, Google
18 contends that the Complaint fails to sets forth any violations (Mot. at 1:16–17) or purports to
19 identify allegations that are lacking in the entire “45-page complaint with over 1,200 pages of
20 exhibits” (*id.* at 10:23–24), most of which Google wants to seal. Google cannot litigate its
21 motion to dismiss on the public record, while trying seal the Complaint and exhibits that are the
22 subject of Google’s motion.

23 **G. Google’s Other Likely Arguments Fail.**

24 In the face of the extensive legal authority cited above, Google still insists “there is no
25 public interest in disclosure of discovery materials in connection with a non-dispositive motion.”
26 (Ex. D at 1). Google mostly cites cases concerning *unfiled* discovery, which the Supreme Court
27 held “are not public components of a civil trial.” *Seattle Times*, 467 U.S. at 33; *see also Foltz v.*
28 *State Farm Mut. Auto. Ins. Co.*, 331 F.3d 1122, 1135 (9th Cir. 2003) (noting exception for

1 sealed discovery submitted with nondispositive motion). Here, Google is trying to seal the
2 Complaint—not unfiled discovery—and therefore the presumption of public access has
3 attached. *See Lewis R. Pyle Mem'l Hosp.*, 149 Ariz. at 197 (“Even though information may be
4 discoverable per Rule 26(b)(1), such information is not ordinarily public information **until**
5 **introduced into evidence or filed with the clerk of the court.**”) (emphasis added); *Ctr. for Auto*
6 *Safety*, 809 F.3d at 99 (holding that the exception is limited to pleadings that are only
7 “tangentially related to the underlying cause of action”).

8 Arizona courts, like federal courts, explicitly distinguish between unfiled discovery and
9 materials filed with the Court. *See* Ariz. R. Civ. P. 5.1(c)(2)(B) (providing that discovery “may
10 not be filed” unless relevant to a determination of an issue before the court); *see also Bond v.*
11 *Utreras*, 585 F.3d 1061, 1075–76 (7th Cir. 2009) (“The rights of the public kick in when
12 material produced during discovery is filed with the court.”). As explained, both Arizona and
13 Ninth Circuit authority confirms the public’s presumptive right of access to a Complaint.⁶

14 Google also insists other courts routinely seal the kinds of documents that it seeks to seal
15 here, (Ex. D at 2), but the cases it cites largely undermine its claim. In *In re Google Inc. Gmail*
16 *Litig.*, No. 13-MD-02430-LHK, 2014 WL 10537440, at *2, *5 (N.D. Cal. Aug. 6, 2014), the
17 court largely **denied** a request to seal information “critical to public understanding of the cause
18 of action in this case” and otherwise public, and only permitted narrowly tailored redactions on a
19 particularized, document-by-document basis. Similarly, in *Apple Inc. v. Samsung Elecs., Co.*,
20 727 F.3d 1214, 1226 (Fed. Cir. 2013), the court only sealed “limited portions” of proprietary
21 financial documents that were not introduced into evidence, not considered by the jury, and not
22 “essential to the public’s understanding of the jury’s damages award,” and only because the
23

24 ⁶ Google cites *Mercury Interactive Corp. v. Klein*, which declines public access where “the
25 Complaint’s exhibits did not become a basis for adjudication” when a demurrer for lack of
26 standing is sustained. 70 Cal. Rptr. 3d 88, 121 (Ct. App. 2007) (demurrer did not deal “with the
27 underlying factual claims” and “exhibits were not submitted as a basis for adjudication”). Since
28 then, the Ninth Circuit has rejected the notion “that the public character of judicial records
depends on whether the proceedings have progressed to a stage requiring a judge to act on the
papers.” *Planet III*, 947 F.3d at 591–92. And unlike in *Mercury*, Google’s motion to dismiss
challenges the State’s factual claims and puts at issue what is or is not alleged in the Complaint.

1 parties already agreed to “make public all of the information contained in these documents that
2 was actually cited by the parties or the district court.” Here, Google’s proposed sealing is a far
3 cry from what the courts allowed in *Apple* or *Gmail*. Google also cites cases from other
4 jurisdictions applying a different standard from what the Ninth Circuit and Arizona courts
5 require⁷ or where—unlike the present case—the public’s interest in accessing to the complaint
6 was “minimal.”⁸ Also, most of the Google’s authorities involved sealed materials produced
7 subject to a protective order. Here, there is no court order precluding the State from publicly
8 filing the materials. Rather, the materials produced were subject to a Confidentiality Agreement
9 and a statutory scheme—both of which recognize the AG’s discretion to use the materials in
10 connection with litigation and make them public.

11 IV. CONCLUSION

12 The Court should reject Google’s efforts to seal large swaths of the Complaint and
13 exhibits, which are presumptively public. Google cannot articulate a compelling interest for
14 sealing this information, much less one that overrides the public’s strong interest in the facts
15 surrounding this case. Neither can Google establish prejudice beyond embarrassment. Finally,
16 Google’s proposed restriction on public access—wholesale sealing of a vast majority of the
17 exhibits and much of the Complaint—is far greater than necessary.

18
19 Dated: July 17, 2020

MARK BRNOVICH
ATTORNEY GENERAL
By: /s/ Brunn W. Roysden III
Joseph A. Kanefield
Brunn W. Roysden III
Oramel H. Skinner
Michael S. Catlett
Christopher Slood
Assistant Attorneys General

25
26 ⁷ *A.L. v. Walt Disney Parks & Resorts US, Inc.*, No. 614CV1544ORL22GJK, 2020 WL
27 1138254, at *1 (M.D. Fla. Mar. 9, 2020) (applying “good cause,” not “compelling interest”);
28 *Jochims v. Isuzu Motors, Ltd.*, 151 F.R.D. 338, 341 n.7 (S.D. Iowa 1993) (sealing trial exhibits
because “compelling showing” standard is “inconsistent with the Eighth Circuit’s view”).
⁸ *IDT Corp. v. eBay*, 709 F.3d 1220, 1224 (8th Cir. 2013).

1 Guy Ruttenberg (CA Bar No. 207937)
2 (pro hac vice application forthcoming)
3 Michael Eshaghian (CA Bar No. 300869)
4 (pro hac vice application forthcoming)
5 RUTTENBERG IP LAW, A
6 PROFESSIONAL CORPORATION
7 1801 Century Park East, Suite 1920
8 Los Angeles, California 90067
9 Telephone: (310) 627-2270
10 guy@ruttenbergiplaw.com
11 mike@ruttenbergiplaw.com

David H. Thompson (DC Bar No. 450503)
(pro hac vice application forthcoming)
Peter A. Patterson (DC Bar No. 998668)
(pro hac vice application forthcoming)
COOPER & KIRK PLLC
1523 New Hampshire Ave NW
Washington, DC 20036
Telephone: (202) 220-9600
dthompson@cooperkirk.com
ppaterson@cooperkirk.com

Attorneys for Plaintiff State of Arizona ex rel. Mark Brnovich, Attorney General

GOOD FAITH CONSULTATION CERTIFICATE

Pursuant to Rule of Civil Procedure 5.4(g)(3), I certify that the parties engaged in good-faith consultation under Rule 7.1(h).

/s/ Guy Ruttenberg

1 COPY of the foregoing Notice, as well as
2 Exhibits A, D, and E to this Notice FILED
with the Court this 17th day of July, 2020.

3 COPY of Exhibits B, C, and F to this Notice
4 LODGED in a sealed envelope with the Clerk
5 of Court pursuant to Rule 5.4(e)(1)(A), (2)
this 17th day of July, 2020.

6
7 COURTESY COPY of the foregoing Notice;
8 Exhibits A, D, and E to this Notice; and, in a
9 sealed envelope, Exhibits B, C, and F to this Notice
HAND DELIVERED pursuant to Rule 5.4(e)(1)(B)
this 17th day of July, 2020 to:

10 Chambers of Judge Thomason
11 101 W. Jefferson St.
12 Phoenix, AZ 85003

13 COPY of the foregoing Notice and Exhibits
14 HAND DELIVERED this 17th day of July, 2020 to:

15 J Cabou
16 PERKINS COIE LLP
17 2901 N. Central Ave., Suite 2000
18 Phoenix, AZ 85012
Counsel for Defendant Google LLC

19
20 /s/ Brunn W. Roysden III
21
22
23
24
25
26
27
28

Exhibit A

**IN THE MATTER OF THE INVESTIGATION BY THE ARIZONA ATTORNEY
GENERAL RELATING TO GOOGLE LLC AND STORAGE OF CONSUMER
LOCATION DATA, TRACKING OF CONSUMER LOCATION, AND OTHER
CONSUMER TRACKING, PHX-INV-2018-0025**

CONFIDENTIALITY AGREEMENT

1. The purpose of this Confidentiality Agreement ("Agreement") is to address the confidentiality concerns raised by Google LLC ("Google") concerning the handling of information to be produced by Google to the Arizona Attorney General's Office (the "AGO")¹ during its investigation under the Arizona Consumer Fraud Act, A.R.S. § 44-1521 *et seq.*, relating to storage of consumer location data, tracking of consumer location, and other consumer tracking, PHX-INV-2018-0025 (the "Investigation"). The AGO and Google (collectively, the "Parties"), by and through undersigned counsel, agree to the following.
2. The parties recognize that Arizona law provides as follows. Under A.R.S. § 44-1525, "[a]ll information or evidence provided to the attorney general shall be confidential and shall not be made public unless in the judgment of the attorney general the ends of justice and the public interest will be served by the publication thereof, provided that the names of the interested parties shall not be made public." Moreover, under A.R.S. § 44-401(4), "'[t]rade secret' means information, including a formula, pattern, compilation, program, device, method, technique or process, that both: (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and] (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."
3. **Marking materials as "Confidential."** In addition to the generally applicable provisions of law described in paragraph 2, Google shall have the right to mark as "Confidential" any materials or other information it produces or otherwise discloses to the AGO in the course of the Investigation that Google reasonably believes contains sensitive information ("Designated Materials"). As used in this Agreement, "sensitive information" means any document, data, or other information that Google reasonably believes both:
 - (i) contains confidential, non-public commercial or financial information with present economic value to Google; contains confidential consumer information; or contains, under applicable United States or state law, a trade secret; and

¹ As used herein, AGO refers to the Arizona Attorney General and all assistant attorneys general and staff.

- (ii) needs to be marked as "Confidential" under this Agreement in a good faith exercise of Google's business judgment to protect Google's legitimate interest in the confidentiality of such information or consumer privacy.

Except as otherwise provided in paragraph 5, below, the AGO agrees to use Designated Materials only in connection with the Investigation and any litigation that may arise therefrom between Google and the AGO or the State of Arizona (collectively, "Investigation and Any Related Litigation"). Nothing in this Agreement prohibits the AGO from contacting consumers or others identified in Designated Materials in connection with the Investigation and Any Related Litigation. The AGO also agrees not to disclose any Designated Materials to any party or the public, except as specifically provided by the Agreement.

4. **Public records and other requests to the AGO.** In the event that the AGO receives any third-party request or demand for any Designated Materials and the AGO concludes the information requested must be produced under the Arizona Public Records Law, A.R.S. § 39-121 *et seq.*, or any other law or legal process compelling the production of such Designated Materials to any person, the AGO agrees to provide Google with at least ten (10) days advance notice before complying with such a request and/or voluntarily providing information designated as "Confidential." Such notice shall be made by electronic mail to Google's counsel in the Investigation and by first class mail, postage prepaid, to Google LLC, 1600 Amphitheatre Pkwy, Mountain View, CA 94043, or to such other address as Google or its attorneys may designate by written notice to the AGO.
5. **Disclosure related to the Investigation And Any Related Litigation and to government agencies.** Unless otherwise ordered by a court of competent jurisdiction with jurisdiction over the Parties, or permitted in writing by Google, the AGO and, as to 5(b), (d)-(h) AGO and its Outside Counsel Personnel, may disclose Designated Materials only:
 - (a) to any employee of the AGO to whom it is reasonably necessary to disclose the Designated Materials in connection with the Investigation And Any Related Litigation or another AGO investigation, civil or criminal, in which the Designated Materials are reasonably calculated to be relevant, and who agrees to be bound to this Agreement;
 - (b) to any United States or state judicial or administrative court or tribunal of competent jurisdiction, including to any relevant staff of the court or tribunal, in connection with any proceeding that arises from the Investigation and Any Related Litigation, subject to Paragraph 9, below;
 - (c) upon the request of a state or federal agency ("Other Government Agency") as part of an investigation or prosecution within the scope of its powers and in which the

AGO determines such Designated Materials are reasonably calculated to be relevant, only after such Other Government Agency agrees, on behalf of itself and its staff, to be bound to this Agreement, subject to paragraph 6, below;

- (d) to any outside counsel assisting the AGO in this investigation, including Cooper & Kirk, PLLC ("Cooper & Kirk") and Ruttenberg IP Law, a Professional Corporation ("Ruttenberg IP"), as well as their attorneys and staff assigned to the Investigation And Any Related Litigation (collectively, "Outside Counsel Personnel"), exclusively for use in this Investigation and Any Related Litigation and subject to paragraph 6, below;
- (e) to any potential expert witness including any consulting expert and any employees, contractors, or counsel of any expert (collectively, "Expert Witness Personnel") retained by the AGO or its outside counsel in connection with the Investigation And Any Related Litigation, subject to paragraphs 6 and 7, below;
- (f) during any examination, deposition, or other proceeding, to any examinee under oath, deponent, or other sworn witness and their counsel ("Third-Party Testifying Witness"), to the extent such witness is providing testimony related to the Investigation And Any Related Litigation, subject to paragraph 6, below, unless such witness has access, under other provisions of this Agreement, including paragraph 5(g) herein, to the Designated Materials to be shown that witness;
- (g) during any examination, deposition, or other proceeding, to any examinee under oath, deponent, or other sworn witness and their counsel, where such witness presently or previously received or has the right of access to particular Designated Materials or similar such materials in the course of their present or former employment at Google (or its predecessor or affiliates), including but not limited to any such witness who is a creator or recipient of particular Designated Materials; where such witness is designated as a corporate representative of Google (or its predecessor or affiliates); or where such witness is a present or former director or officer of Google (or its predecessor or affiliates); and
- (h) to any personnel involved in litigation support services in connection with the Investigation And Any Related Litigation, including any mediator, court reporter, videographer, graphics or design services, photocopy or document imaging services, document collection or hosting services, database services, document review services or similar vendors (collectively, "Litigation Support Vendor").

6. **Requirement of prior acknowledgement and notice to Google.** The AGO will require any Other Government Agency, Outside Counsel Personnel, Expert Witness Personnel, or Third-Party Testifying Witness designated to receive Designated Materials to first sign a

written agreement substantially in the form of Exhibit A hereto that such person has received a copy of this Agreement, agrees to be bound by its terms, and agrees not to further disseminate the Designated Materials without the prior consent of the AGO and Google. In the case of an agency or entity serving as any of the foregoing, the AGO will require a representative to agree on behalf of the agency or entity and its staff, and will not require each staff member to sign. The representative must further agree to inform other associated personnel of their obligations to comply with this requirement. The AGO will retain copies of such acknowledgements and produce them to Google if Google has specific reason to believe Designated Materials have been disclosed in violation of this Agreement. Furthermore, at least 5 days prior to disclosing any Designated Materials pursuant to 5(c), 5(d) (other than disclosure by AGO to Outside Counsel Personnel already identified by AGO to Google), or 5(f), the AGO or Outside Counsel Personnel shall notify Google of its intent to make such disclosure, of the person(s) to whom the proposed disclosure is to be made, and of the contents of the proposed disclosure.

7. **Additional requirements for disclosure to Expert Witness Personnel.** Any Expert Witness Personnel must not have any present or future, planned employment or contractor relationship (whether paid or unpaid) with (1) Oracle Corporation or any of its affiliates, or (2) any entity that the proposed Expert Witness Personnel reasonably knows to be a business competitor of Google's smart phone or search business. Further, any Expert Witness Personnel must further agree to only use Designated Materials in connection with the Investigation And Any Related Litigation and to destroy all such materials they retain possession of at the conclusion of the Investigation And Any Related Litigation, provided that they may, at their discretion, retain a copy of any of their final reports and deposition or trial testimony transcripts in the Investigation And Any Related Litigation. If the limitations in this paragraph pose a material limitation on the AGO's ability to obtain qualified expert witnesses for the Investigation And Any Related Litigation, then the parties will meet and confer in good faith regarding alternative limitations on potential experts to protect Google's legitimate business interests.
8. **Meeting and conferring regarding a "Confidential" marking.** Outside of litigation (which is described in paragraph 9, below) the Parties agree to meet and confer in good faith regarding markings as follows. If the AGO believes that Google has erroneously marked materials or information as Designated Materials, *i.e.*, because such materials or information does not contain sensitive information, as defined above in paragraph 3, the parties agree to meet and confer in good faith regarding the marking. In addition, if the AGO believes that Google has marked materials or information as Designated Materials, and the sensitive information contained therein can be protected through redaction, the parties similarly agree to meet and confer in good faith regarding the redaction.
9. **Filing documents under seal.** The Parties recognize and acknowledge that, if the Investigation proceeds to litigation or another form of dispute resolution proceeding, the

relevant tribunal is likely to have its own rules, regulations, and/or orders for handling and filing materials that are purportedly confidential. Google acknowledges that, if it seeks to seal or otherwise to withhold from the public record any Designated Materials in any proceedings, Google will need to comply with the applicable rules, regulations, and/or orders of the relevant tribunal. Similarly, to the extent the AGO seeks to file in such a tribunal any Designated Materials, the AGO agrees to either file the Designated Materials under seal or afford Google at least 10 days advanced notice, in either case consistent with the applicable rules, regulations, and/or orders of the relevant tribunal. Further, in all cases, the AGO reserves the right to oppose any request for sealing, to ask the court to unseal Designated Materials, and/or to challenge any confidentiality designations by Google, in each case in whole or in part. Further, in the event of any such dispute, Google shall bear the burden of defending its designations of material as Designated Material.

10. **Inadvertent disclosure.** If any person bound by this Agreement learns that, by inadvertence or otherwise, it has disclosed Designated Materials to any person or in any circumstance not authorized under this Agreement, the person must promptly (a) notify Google and the AGO of the unauthorized disclosures, (b) use its best efforts to retrieve all unauthorized copies of the Designated Materials, (c) inform the persons to whom the unauthorized disclosures were made of all the terms of this Agreement, and (d) request that such persons return the disclosed Designated Materials to the AGO.
11. **Process after termination of Investigation And Any Related Litigation.** Even after conclusion of the Investigation And Any Related Litigation, the confidentiality obligations imposed by this Agreement shall remain in effect until Google agrees otherwise in writing or a court order otherwise directs. In agreeing to be bound by this Agreement, the AGO and Outside Counsel Personnel all agree to return or destroy the Designated Materials except if the return or destruction is inconsistent with its legal obligations.
12. **Choice of law and enforcement.** This Agreement is governed by the laws of the State of Arizona and shall be enforced in the courts of the State of Arizona. Nothing in this agreement creates or otherwise confers any rights or causes of action in any third party.
13. To the extent any provision of this Agreement conflicts with any applicable laws or regulations, the applicable laws and/or regulations shall govern. Further, to the extent this Investigation leads to litigation, the rules, procedures, and orders of the relevant court shall govern. Should this Investigation proceed to litigation, any Protective Order entered by a court with competent jurisdiction shall supersede this Agreement with respect to that litigation.

Agreed to and accepted this 12th day of April, 2019, by:

PERKINS COIE LLP

By: 

Jean-Jacques (J) Cabou
Counsel for Google LLC

ARIZONA ATTORNEY GENERAL'S OFFICE

By: 

Brunn (Beau) W. Roysden III
Assistant Attorney General

EXHIBIT A TO CONFIDENTIALITY AGREEMENT

By signing this Exhibit A to the Confidentiality Agreement In The Matter Of The Investigation By The Arizona Attorney General Relating To Google LLC And Storage Of Consumer Location Data, Tracking Of Consumer Location, And Other Consumer Tracking, Phx-Inv-2018-0025, I certify and agree that I have read the Confidentiality Agreement ("Agreement") in its entirety, and that I fully understand the obligations under the Agreement, including this Exhibit A.

I further hereby agree that _____ will be bound by the terms of the Confidentiality Agreement and this Exhibit A.

I further agree that _____ will not disseminate any information received pursuant to the Confidentiality Agreement without the prior written consent of the Arizona Attorney General's Office and Google LLC.

By: _____

Date: _____

Printed Name

Title: _____

Agency/Entity

Exhibit D

July 15, 2020

SENT BY E-MAIL

Guy Ruttenberg
Ruttenberg IP Law
1801 Century Park East, Suite 1920
Los Angeles, CA 90067
E-mail: guy@ruttenbergiplaw.com

Re: *The State of Arizona ex rel. Brnovich v. Google LLC* – Case No. CV2020-006219
Confidentiality of the Complaint

Dear Guy:

We understand that the Attorney General (the “AG”) will soon file a notice with the Court, announcing his intent to publicly reveal information that Google shared with the AG as part of a confidential investigative process and pursuant to a written confidentiality agreement between the parties. The AG has asked for Google’s position, which has already been the subject of a meet and confer. While Google will set forth its position with greater specificity in its motion to seal, below we reiterate Google’s overarching position.

First, there is no public interest in disclosure of discovery materials in connection with a non-dispositive motion. The AG has taken the position that just because he wants to attach confidential documents to his Complaint, a company’s confidential information instantly becomes a matter of public interest. That is incorrect. There is no compelling interest in disclosure of information gained in discovery unless such information becomes part of a trial or summary judgment. *See Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 33 (1984) (“[D]iscovered, but not yet admitted, information [is] not ... a traditionally public source of information.”); *see also Mercury Interactive Corp. v. Klein*, 70 Cal. Rptr. 3d 88, 97 (Cal. Ct. App. 2007) (no presumption of public access to discovery documents attached to a complaint because no public right of access to discovery materials); *Lewis R. Pyle Mem’l Hosp. v. Super. Ct.*, 149 Ariz. 193, 197 (1986) (applying *Seattle Times* and holding “pretrial depositions are no public right of access to discovery materials”); *Lewis R. Pyle Mem’l Hosp. v. Super. Ct.*, 149 Ariz. 193, 197 (1986) (applying *Seattle Times* and holding “pretrial depositions are not public proceedings”). That is especially true here, where Google relied on the AG’s agreement to maintain confidentiality, and

where the copious documents attached to the AG's complaint are not at all necessary for the AG to plead his claims, or for the Court to analyze the pending motion to dismiss the Complaint, which Google will soon file. *See, e.g., Foltz v. State Farm Mut. Auto. Ins. Co.*, 331 F.3d 1122, 1135 (9th Cir. 2003) (even accounting for the "strong presumption of access to court records," when "a party attaches a sealed discovery document to a *nondispositive* motion, the usual presumption of the public's right of access is rebutted" (citation omitted)).

Second, most if not all of the confidential documents the AG now seeks to publish are the kind of documents that courts routinely maintain under seal. Generally, the exhibits the AG seeks to publish can be categorized in one or more of the following five protected categories: (1) product design, engineering, performance, and improvement presentations and reviews; (2) product design and development deliberations and emails; (3) internal studies or projections; (4) customer or user data; and (5) other business strategy business deliberations. For good and obvious reasons, such information is protected from public disclosure.¹

Third, the AG improperly seeks to publicize through his pleading various other things that have no bearing on his claim for relief and in which there is no legitimate public interest. For instance, allegations about how Google cooperated with the course of the AG's confidential investigation, which is confidential by statute (A.R.S. 44-1525), have nothing to do with the AG's claim about Google's business practices. That investigation is over. The Complaint itself recognizes that such information is neither a "Factual Allegation" nor a part of the "Claim for Relief" by throwing these impertinent allegations into an entirely separate section of the Complaint. To the extent these allegations remain in any pleading the AG seeks to file, they should remain sealed. *See* A.R.S. 44-1525.

Fourth, there is no good reason to make public the names and personal identifying information ("PII") of Google employees who testified in the AG's confidential investigation and whose names appear in various documents. *See* Ariz. R. Civ. P. 26(c)(1) (permitting the entry of a protective order to protect witnesses from "annoyance, embarrassment, oppression or undue burden"). Indeed, there is clear reason not to: A.R.S. § 44-1525 provides that, even when

¹ *See e.g., Jochims v. Isuzu Motors, Ltd.*, 151 F.R.D. 338, 341 (S.D. Iowa 1993) (sealing "test reports relating to the design and development" of the product at issue as well as "internal engineering standards" and "confidential information regarding advertising expenditures" because they are "the kind of technical and commercial information commonly subject to confidentiality orders"); *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2014 WL 10537440, at *4 (N.D. Cal. Aug. 6, 2014) (sealing documents that relate (1) to "specific descriptions of how Gmail operates," the disclosure of "which could cause competitive harm to Google" or (2) to "how users' interactions with the Gmail system affects how messages are transmitted," the disclosure of which "could lead to a breach in the security of the Gmail system"); *Microsoft Corp. v. Motorola, Inc.*, No. C10-1823JLR, 2012 WL 5476846, at *2 (W.D. Wash. Nov. 12, 2012) (sealing "confidential source code, settlement negotiations, and product specifications"); *A.L. v. Walt Disney Parks & Resorts US, Inc.*, No. 614CV1544ORL22GJK, 2020 WL 1138254, at *1 (M.D. Fla. Mar. 9, 2020) (sealing "internal study results," "communications strategies," and "business operations" because the sealed documents contain "confidential and proprietary information"); *See Apple Inc. v. Samsung Elecs. Co.*, 727 F.3d 1214, 1225 (Fed. Cir. 2013) (sealing "detailed product-specific financial information" and "profit, cost, and margin data" that "could give suppliers an advantage in contract negotiations, which they could use to extract price increases for components").

the Attorney General believes that it serves the “public interest” to publicize certain things about a Consumer Fraud Act investigation, “the names of the interested parties shall not be made public.” *Id.* Courts routinely recognize that the protection of personal information, such as the names of deponents and employee names and email addresses, constitutes an “overriding interest” sufficient to keep such information sealed. *See, e.g., Hadley v. Kellogg Sales Co.*, No. 16-CV-04955-LHK, 2018 WL 7814785, at *3 (N.D. Cal. Sept. 5, 2018) (sealing documents that contain “sensitive personal information”); *Skurkis v. Montelongo*, No. 16-CV-0972 YGR, 2016 WL 4719271, at *6 (N.D. Cal. Sept. 9, 2016) (instructing a party to refer to the other party’s employees’ names in its complaint “in a manner that identifies them without revealing their names”).

Finally, you indicated that you intend to publicly file with your Notice any material Google is not currently seeking to maintain under seal. Although we disagree that the Rule requires this, as promised, attached as **Exhibit A** hereto are the exhibits Google agrees may be publicly filed along with your Notice (some in redacted form). As requested in your July 14 letter, Google’s position is that all other exhibits to the Complaint should currently remain under seal for the reasons explained above. With respect to the Complaint, Google’s position is that all information that is redacted in the version of the complaint filed publicly on May 27, 2020 should currently remain under seal for the reasons explained above.

Sincerely,

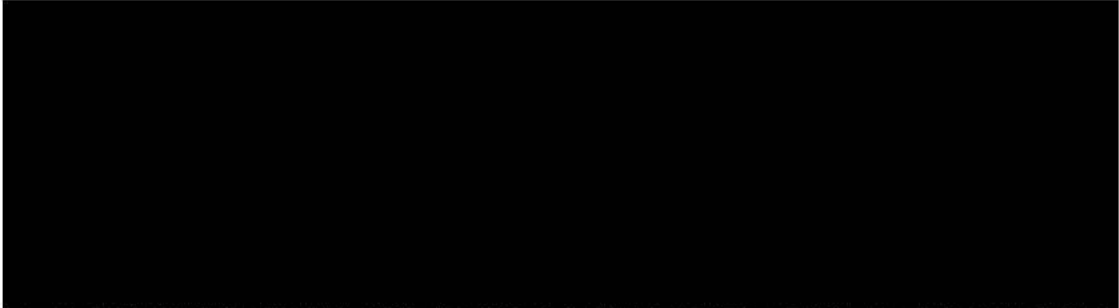


Benedict Y. Hur


BYH:bk

Exhibit E

Exhibit 18

- 
- AP Exclusive: Google tracks your movements; like it or not - 3 Updates
 - Caesars Palace not-so-Praetorian guards intimidate DEF CON goers, seize soldering irons - 1 Update
 - That New Android Update Broke a Key Perk of the Pixel XL - 3 Updates
 - Musk Mulls Taking Tesla Private, Valuing Company at \$82 Billion - 6 Updates
 - "Google plans censored search engine for China" - The Intercept - 3 Updates
 - [NY Times Op-Ed] A Better Way to Ban Alex Jones - 3 Updates
 - Axios: "How tech fuels authoritarians" - 1 Update

AP Exclusive: Google tracks your movements, like it or not



<https://apnews.com/828aefab64d4411bac257a07c1af0ecb>

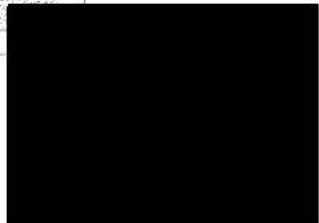
SAN FRANCISCO (AP) — Google wants to know where you go so badly that it records your movements even when you explicitly tell it not to.

An Associated Press investigation found that many Google services on Android devices and iPhones store your location data even if you've used privacy settings that say they will prevent it from doing so.

Computer-science researchers at Princeton confirmed these findings at the AP's request.

For the most part, Google is upfront about asking permission to use your location information. An app like Google Maps will remind you to allow access to location if you use it for navigating. If you agree to let it record your location over time, Google Maps will display that history for you in a "timeline" that maps out your daily movements.

Storing your minute-by-minute travels carries privacy risks and has been used by police to determine the location of suspects — such as a warrant that police in Raleigh, North Carolina, served on Google last year to find



devices near a murder scene. So the company will let you "pause" a setting called Location History.

Google says that will prevent the company from remembering where you've been. Google's support page on the subject states: "You can turn off Location History at any time. With Location History off, the places you go are no longer stored."

That isn't true. Even with Location History paused, some Google apps automatically store time-stamped location data without asking.

For example, Google stores a snapshot of where you are when you merely open its Maps app. Automatic daily weather updates on Android phones pinpoint roughly where you are. And some searches that have nothing to do with location, like "chocolate chip cookies," or "kids science kits," pinpoint your precise latitude and longitude — accurate to the square foot — and save it to your Google account.

The privacy issue affects some two billion users of devices that run Google's Android operating software and hundreds of millions of worldwide iPhone users who rely on Google for maps or search.

Storing location data in violation of a user's preferences is wrong, said Jonathan Mayer, a Princeton computer scientist and former chief technologist for the Federal Communications Commission's enforcement bureau. A researcher from Mayer's lab confirmed the AP's findings on multiple Android devices; the AP conducted its own tests on several iPhones that found the same behavior.

"If you're going to allow users to turn off something called 'Location History,' then all the places where you maintain location history should be turned off," Mayer said. "That seems like a pretty straightforward position to have."

Google says it is being perfectly clear.

"There are a number of different ways that Google may use location to improve people's experience, including: Location History, Web and App Activity, and through device-level Location Services," a Google spokesperson said in a statement to the AP. "We provide clear descriptions of these tools, and robust controls so people can turn them on or off, and delete their histories at any time."

To stop Google from saving these location markers, the company says, users can turn off another setting, one that does not specifically reference location information. Called "Web and App Activity" and enabled by default,

that setting stores a variety of information from Google apps and websites to your Google account.

When paused, it will prevent activity on any device from being saved to your account. But leaving "Web & App Activity" on and turning "Location History" off only prevents Google from adding your movements to the "timeline," its visualization of your daily travels. It does not stop Google's collection of other location markers.

You can delete these location markers by hand, but it's a painstaking process since you have to select them individually, unless you want to delete all of your stored activity.

You can see the stored location markers on a page in your Google account at myactivity.google.com, although they're typically scattered under several different headers, many of which are unrelated to location.

To demonstrate how powerful these other markers can be, the AP created a visual map of the movements of Princeton postdoctoral researcher Gunes Acar, who carried an Android phone with Location history off, and shared a record of his Google account.

The map includes Acar's train commute on two trips to New York and visits to The High Line park, Chelsea Market, Hell's Kitchen, Central Park and Harlem. To protect his privacy, The AP didn't plot the most telling and frequent marker — his home address.

Huge tech companies are under increasing scrutiny over their data practices, following a series of privacy scandals at Facebook and new data-privacy rules recently adopted by the European Union. Last year, the business news site Quartz found that Google was tracking Android users by collecting the addresses of nearby cellphone towers even if all location services were off. Google changed the practice and insisted it never recorded the data anyway.

Critics say Google's insistence on tracking its users' locations stems from its drive to boost advertising revenue.

"They build advertising information out of data," said Peter Lenz, the senior geospatial analyst at Dstillery, a rival advertising technology company. "More data for them presumably means more profit."

The AP learned of the issue from K. Shankari, a graduate researcher at UC Berkeley who studies the commuting patterns of volunteers in order to help urban planners. She noticed that her Android phone prompted her to rate a shopping trip to Kohl's, even though she had turned Location History off.

"So how did Google Maps know where I was?" she asked in a blog post .

The AP wasn't able to recreate Shankari's experience exactly. But its attempts to do so revealed Google's tracking. The findings disturbed her.

"I am not opposed to background location tracking in principle," she said. "It just really bothers me that it is not explicitly stated."

Google offers a more accurate description of how Location History actually works in a place you'd only see if you turn it off — a popup that appears when you "pause" Location History on your Google account webpage . There the company notes that "some location data may be saved as part of your activity on other Google services, like Search and Maps."

Google offers additional information in a popup that appears if you re-activate the "Web & App Activity" setting — an uncommon action for many users, since this setting is on by default. That popup states that, when active, the setting "saves the things you do on Google sites, apps, and services ... and associated information, like location."

Warnings when you're about to turn Location History off via Android and iPhone device settings are more difficult to interpret. On Android, the popup explains that "places you go with your devices will stop being added to your Location History map." On the iPhone, it simply reads, "None of your Google apps will be able to store location data in Location History."

The iPhone text is technically true if potentially misleading. With Location History off, Google Maps and other apps store your whereabouts in a section of your account called "My Activity," not "Location History."

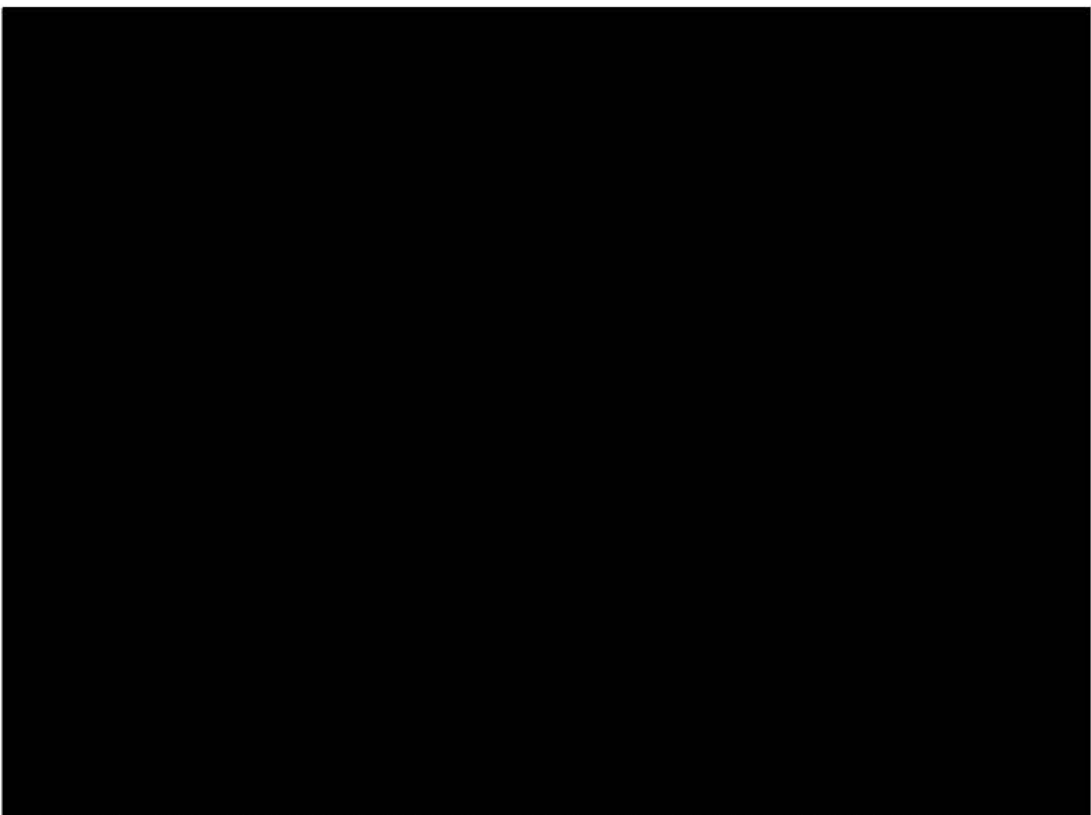
Since 2014, Google has let advertisers track the effectiveness of online ads at driving foot traffic , a feature that Google has said relies on user location histories.

The company is pushing further into such location-aware tracking to drive ad revenue, which rose 20 percent last year to \$95.4 billion. At a Google Marketing Live summit in July, Google executives unveiled a new tool called "local campaigns" that dynamically uses ads to boost in-person store visits. It says it can measure how well a campaign drove foot traffic with data pulled from Google users' location histories.


Google also says location records stored in My Activity are used to target ads. Ad buyers can target ads to specific locations — say, a mile radius around a particular landmark — and typically have to pay more to reach this narrower audience.

While disabling "Web & App Activity" will stop Google from storing location markers, it also prevents Google from storing information generated by searches and other activity. That can limit the effectiveness of the Google Assistant, the company's digital concierge.

Sean O'Brien, a Yale Privacy Lab researcher with whom the AP shared its findings, said it is "disingenuous" for Google to continuously record these locations even when users disable Location History. "To me, it's something people should know," he said.



Caesars Palace not-so-Praetorian guards intimidate DEF CON goers, seize soldering irons



<https://arstechnica.com/tech-policy/2018/08/security-theater-meets-def-con-as-room-searches-spark-controversy/>

Caesars Palace not-so-Praetorian guards intimidate DEF CON goers, seize soldering irons Hotel policies drafted after last October's mass shooting arrive just in time for DEF CON.

Sean Gallagher <<https://arstechnica.com/author/sean-gallagher/>> -
8/13/2018, 3:40 PM

In the wake of the mass shooting in Las Vegas in October of 2017, hotels in the city started drafting more aggressive policies regarding security. Just as Caesars Entertainment was rolling out its new security policies, the company ran head on into DEF CON—an event with privacy tightly linked to its culture.

The resulting clash of worlds—especially at Caesars Palace, the hotel where much of DEF CON was held—left some attendees feeling violated, harassed, or abused, and that exploded onto Twitter this past weekend.

Caesars began rolling out a new security policy in February <https://www.playusa.com/caesars-do-not-disturb/> that mandated room searches when staff had not had access to rooms for over 24 hours. Caesars has been mostly tolerant of the idiosyncratic behavior of the DEF CON community, but it's not clear that the company prepared security staff for dealing with the sorts of things they would find in the rooms of DEF CON attendees. Soldering irons and other gear were seized, and some attendees reported being intimidated by security staff.

https://twitter.com/really_awolf

Andrew Wolf @really_awolf

https://twitter.com/really_awolf

https://twitter.com/really_awolf/status/1028062678881693697

WARNING HACKERS

Caesars staff are performing "random" security checks of rooms. If you opt out of room cleaning and used defcon discount they will check your room and WILL confiscate soldering irons + more!

Not a drill! Spread the word!#defcon

<https://twitter.com/hashtag/defcon?src=hash> #badgelife

<https://twitter.com/hashtag/badgelife?src=hash> #dc26

<https://twitter.com/hashtag/dc26?src=hash> #DEFCON26

<https://twitter.com/hashtag/DEFCON26?src=hash>

4:36 PM - Aug 10, 2018

https://twitter.com/really_awolf/status/1028062678881693697

And since the searches came without any warning other than a knock, they led, in some cases, to frightening encounters for attendees who were in those rooms. Katie Moussouris—a bug bounty and vulnerability disclosure program pioneer at Microsoft, an advocate for security researchers, and now the founder and CEO of Luta Security—was confronted by two male members of hotel security as she returned to her room. When she went into the room to call the desk to verify who they were, they banged on the door and screamed at her to immediately open it.

<https://twitter.com/k8em0>

Katie Moussouris *✓* @k8em0

<https://twitter.com/k8em0>

<https://twitter.com/k8em0/status/1028375035285630976>

Current status: two members of hotel security banging on my door after I asked to go into my room and verify them with hotel security. I'm on speaker phone with hotel security, asking for a supervisor to come verify.

I'm terrified. What the hell is this @CaesarsPalace
<<https://twitter.com/CaesarsPalace>> #DEFCON
<<https://twitter.com/hashtag/DEFCON?src=hash>>
1:18 PM - Aug 11, 2018
<<https://twitter.com/k8em0/status/1028375035285630976>>

In another case, a hotel employee—likely hotel security—entered the room of a woman attending DEF CON without knocking:

<<https://twitter.com/maddiestone>>
Maddie Stone @maddiestone
<<https://twitter.com/maddiestone>>
<<https://twitter.com/maddiestone/status/1028498769732460544>>

This evening, a man in a light blue collared shirt with a walkie talkie, entered my room with a key without knocking while I was getting dressed. He left when I started screaming. @CaesarsPalace

<<https://twitter.com/CaesarsPalace>> is investigating whether it was a hotel employee. @defcon <<https://twitter.com/defcon>> has also been alerted.
9:29 PM - Aug 11, 2018

<<https://twitter.com/maddiestone/status/1028498769732460544>>

Beau Woods, cyber policy activist and co-founder of I Am The Cavalry, hacked the "Do Not Disturb" sign in an attempt to stave off searches:

<<https://twitter.com/beauwoods>>
<<https://twitter.com/beauwoods>>
<<https://twitter.com/beauwoods>> <<https://twitter.com/beauwoods>>
<<https://twitter.com/beauwoods>> View image on Twitter
<https://twitter.com/beauwoods/status/1028387331927986176/photo/1?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1028387331927986176&ref_url=https%3A%2F%2Farstechnica.com%2Ftech-policy%2F2018%2F08%2Fsecurity-theater-meets-def-con-as-room-searches-spark-controversy%2F>

Beau Woods @beauwoods
<<https://twitter.com/beauwoods>>
<<https://twitter.com/beauwoods/status/1028387331927986176>>

For those trying to figure out how to avoid the hotel room (in)security checks, I've used this setup and so far no intrusions in two days.

2:07 PM - Aug 11, 2018
<<https://twitter.com/beauwoods/status/1028387331927986176>>

Ars attempted to reach Caesars for comment but received no response. After Ars reached out to DEFCON, the organizers posted this statement:

We understand that attendees want a statement from DEF CON about the Caesars room search policy. We are actively engaged with the hotel, seeking

answers and a clear policy document we can share with you. Please know that we hear your concerns and we've shared them with Caesars. We expect a venue where our attendees are secure in their persons and effects and a security policy that is codified, predictable, and verifiable. Thank you for your patience while we work this out.

There is a long history of legal precedent

<https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1048&context=circuit_review>

surrounding the expectation of privacy in hotel rooms—overnight hotel guests are recognized to have an expectation of privacy under the Fourth Amendment. But things become murkier when the search is conducted by the property owner. Still, Moussouris' concern was for her physical safety more than her privacy; despite the new security policies, Caesars doesn't control access to its elevators by room key, and there is largely uncontrolled public access to the hotel's towers.

<<https://twitter.com/k8em0>>

Katie Moussouris *✓* @k8em0

<<https://twitter.com/k8em0>>

<<https://twitter.com/k8em0/status/1029059581136105472>>

Last view of the crime scene that was my invaded hotel room and violated space, courtesy of @CaesarsPalace <<https://twitter.com/CaesarsPalace>> who still have not told me anything, offered me anything (except to move my room - like that really would prevent their security team screaming at me again). My last #DEFCON <<https://twitter.com/hashtag/DEFCON?src=hash>> 10:38 AM - Aug 13, 2018

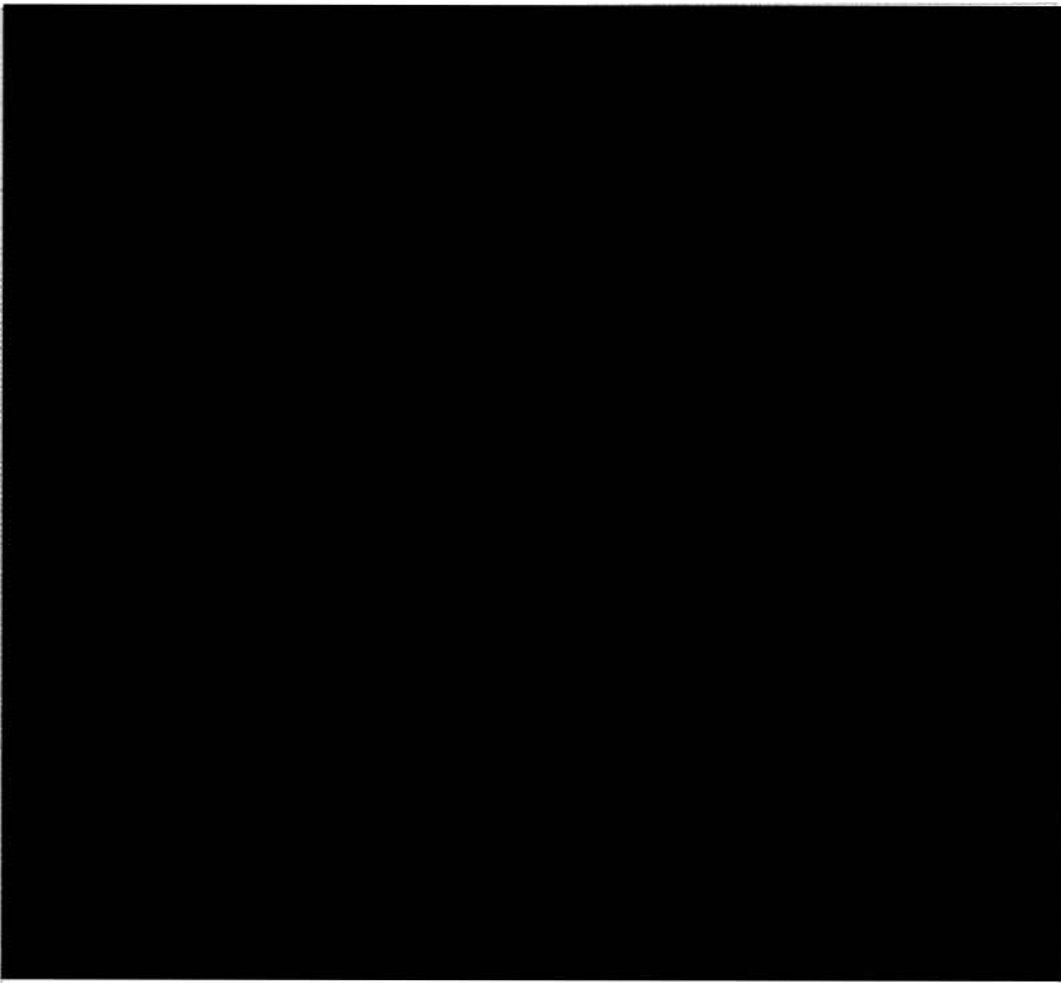
<<https://twitter.com/k8em0/status/1029059581136105472>>

DEF CON won't be at Caesar's Palace next year—but not because of these incidents. The conference has a multi-year contract with Caesars Entertainment to host DEF CON, and Caesars' convention center will be undergoing renovations in 2019. Moussouris said this was her last DEF CON.

[Back to top](#)


That New Android Update Broke a Key Perk of the Pixel XL

<https://gizmodo.com/that-new-android-update-broke-a-key-perk-of-the-pixel-x-1828300671>



[Back to top](#)

Musk Mulls Taking Tesla Private, Valuing Company at \$82 Billion



<https://www.tesla.com/blog/update-taking-tesla-private>

Update on Taking Tesla Private

Elon Musk August 13, 2018

As I announced <<https://www.tesla.com/blog/taking-tesla-private>> last

Tuesday, I'm considering taking Tesla private because I believe it could be good for our shareholders, enable Tesla to operate at its best, and advance our mission of accelerating the transition to sustainable energy. As I continue to consider this, I want to answer some of the questions that have been asked since last Tuesday.

What has happened so far?

On August 2nd, I notified the Tesla board that, in my personal capacity, I wanted to take Tesla private at \$420 per share. This was a 20% premium over the ~\$350 then current share price (which already reflected a ~16% increase in the price since just prior to announcing Q2 earnings on August 1st). My proposal was based on using a structure where any existing shareholder who wished to remain as a shareholder in a private Tesla could do so, with the \$420 per share buyout used only for shareholders that preferred that option.

After an initial meeting of the board's outside directors to discuss my proposal (I did not participate, nor did Kimbal), a full board meeting was held. During that meeting, I told the board about the funding discussions that had taken place (more on that below) and I explained why this could be in Tesla's long-term interest.

At the end of that meeting, it was agreed that as a next step, I would reach out to some of Tesla's largest shareholders. Our largest investors have been extremely supportive of Tesla over the years, and understanding whether they had the ability and desire to remain as shareholders in a private Tesla is of critical importance to me. They are the ones who believed in Tesla when no one else did and they are the ones who most believe in our future. I told the board that I would report back after I had these discussions.

Why did I make a public announcement?

The only way I could have meaningful discussions with our largest shareholders was to be completely forthcoming with them about my desire to take the company private. However, it wouldn't be right to share information about going private with just our largest investors without sharing the same information with all investors at the same time. As a result, it was clear to me that the right thing to do was announce my intentions publicly. To be clear, when I made the public announcement, just as with this blog post and all other discussions I have had on this topic, I am speaking for myself as a potential bidder for Tesla.

Why did I say "funding secured"?

Going back almost two years, the Saudi Arabian sovereign wealth fund has approached me multiple times about taking Tesla private. They first met with me at the beginning of 2017 to express this interest because of the important need to diversify away from oil. They then held several

additional meetings with me over the next year to reiterate this interest and to try to move forward with a going private transaction. Obviously, the Saudi sovereign fund has more than enough capital needed to execute on such a transaction.

Recently, after the Saudi fund bought almost 5% of Tesla stock through the public markets, they reached out to ask for another meeting. That meeting took place on July 31st. During the meeting, the Managing Director of the fund expressed regret that I had not moved forward previously on a going private transaction with them, and he strongly expressed his support for funding a going private transaction for Tesla at this time. I understood from him that no other decision makers were needed and that they were eager to proceed.

I left the July 31st meeting with no question that a deal with the Saudi sovereign fund could be closed, and that it was just a matter of getting the process moving. This is why I referred to "funding secured" in the August 7th announcement.

Following the August 7th announcement, I have continued to communicate with the Managing Director of the Saudi fund. He has expressed support for proceeding subject to financial and other due diligence and their internal review process for obtaining approvals. He has also asked for additional details on how the company would be taken private, including any required percentages and any regulatory requirements.

Another critical point to emphasize is that before anyone is asked to decide on going private, full details of the plan will be provided, including the proposed nature and source of the funding to be used. However, it would be premature to do so now. I continue to have discussions with the Saudi fund, and I also am having discussions with a number of other investors, which is something that I always planned to do since I would like for Tesla to continue to have a broad investor base. It is appropriate to complete those discussions before presenting a detailed proposal to an independent board committee.

It is also worth clarifying that most of the capital required for going private would be funded by equity rather than debt, meaning that this would not be like a standard leveraged buyout structure commonly used when companies are taken private. I do not think it would be wise to burden Tesla with significantly increased debt.

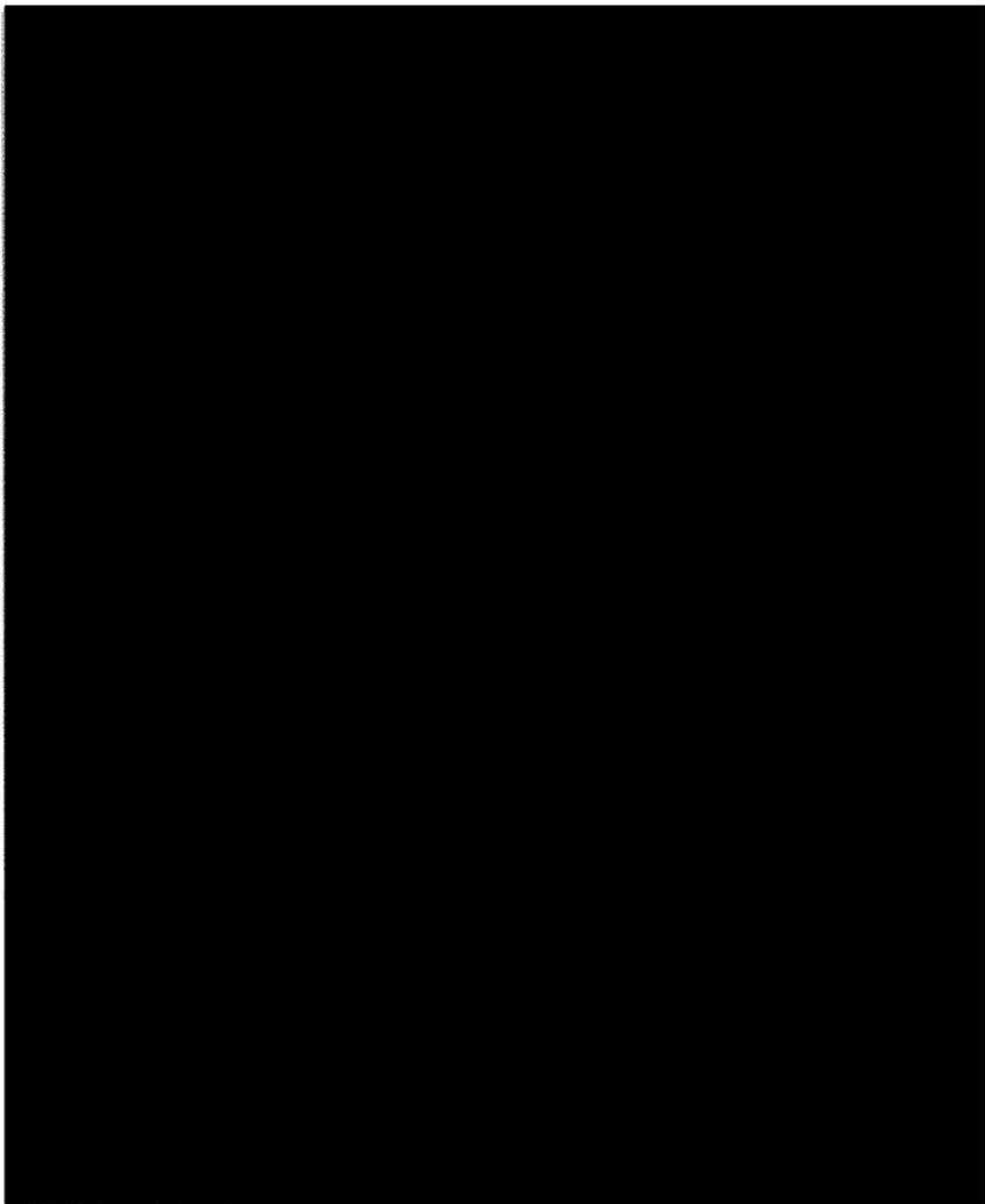
Therefore, reports that more than \$70B would be needed to take Tesla private dramatically overstate the actual capital raise needed. The \$420 buyout price would only be used for Tesla shareholders who do not remain with our company if it is private. My best estimate right now is that

approximately two-thirds of shares owned by all current investors would roll over into a private Tesla.

What are the next steps?

As mentioned earlier, I made the announcement last Tuesday because I felt it was the right and fair thing to do so that all investors had the same information at the same time. I will now continue to talk with investors, and I have engaged advisors to investigate a range of potential structures and options. Among other things, this will allow me to obtain a more precise understanding of how many of Tesla's existing public shareholders would remain shareholders if we became private.

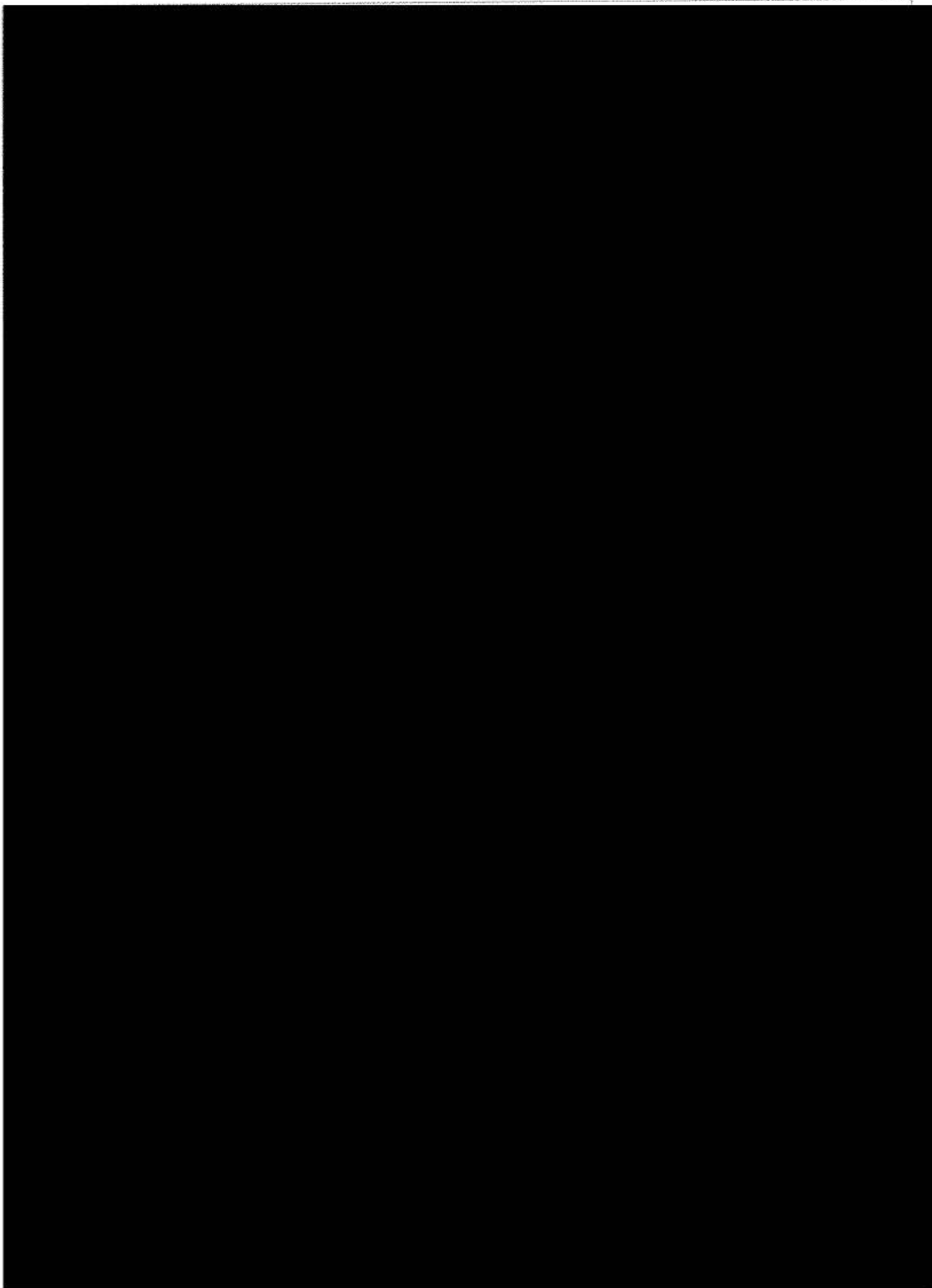
If and when a final proposal is presented, an appropriate evaluation process will be undertaken by a special committee of Tesla's board, which I understand is already in the process of being set up, together with the legal counsel it has selected. If the board process results in an approved plan, any required regulatory approvals will need to be obtained and the plan will be presented to Tesla shareholders for a vote.

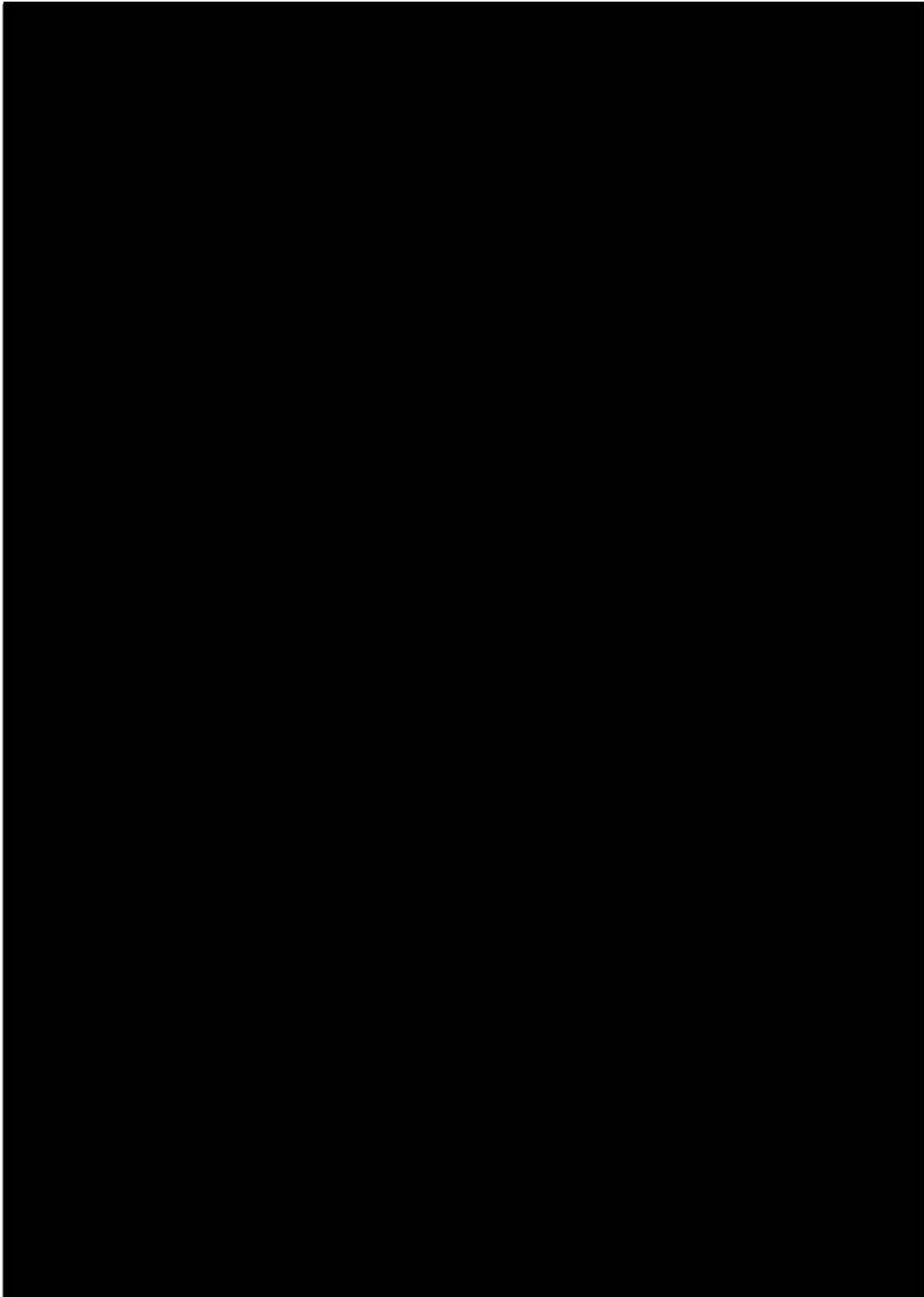


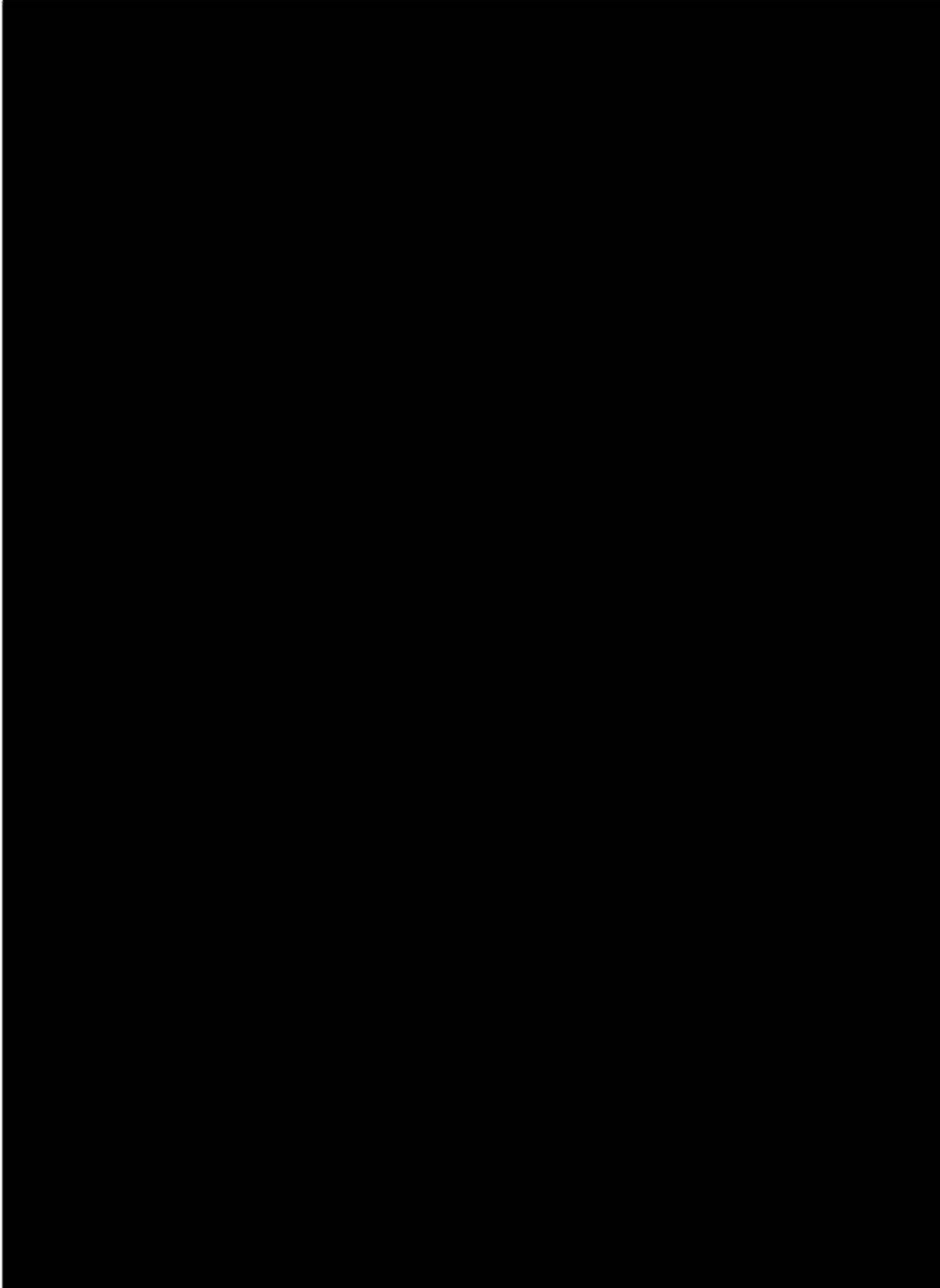
[Back to top](#)

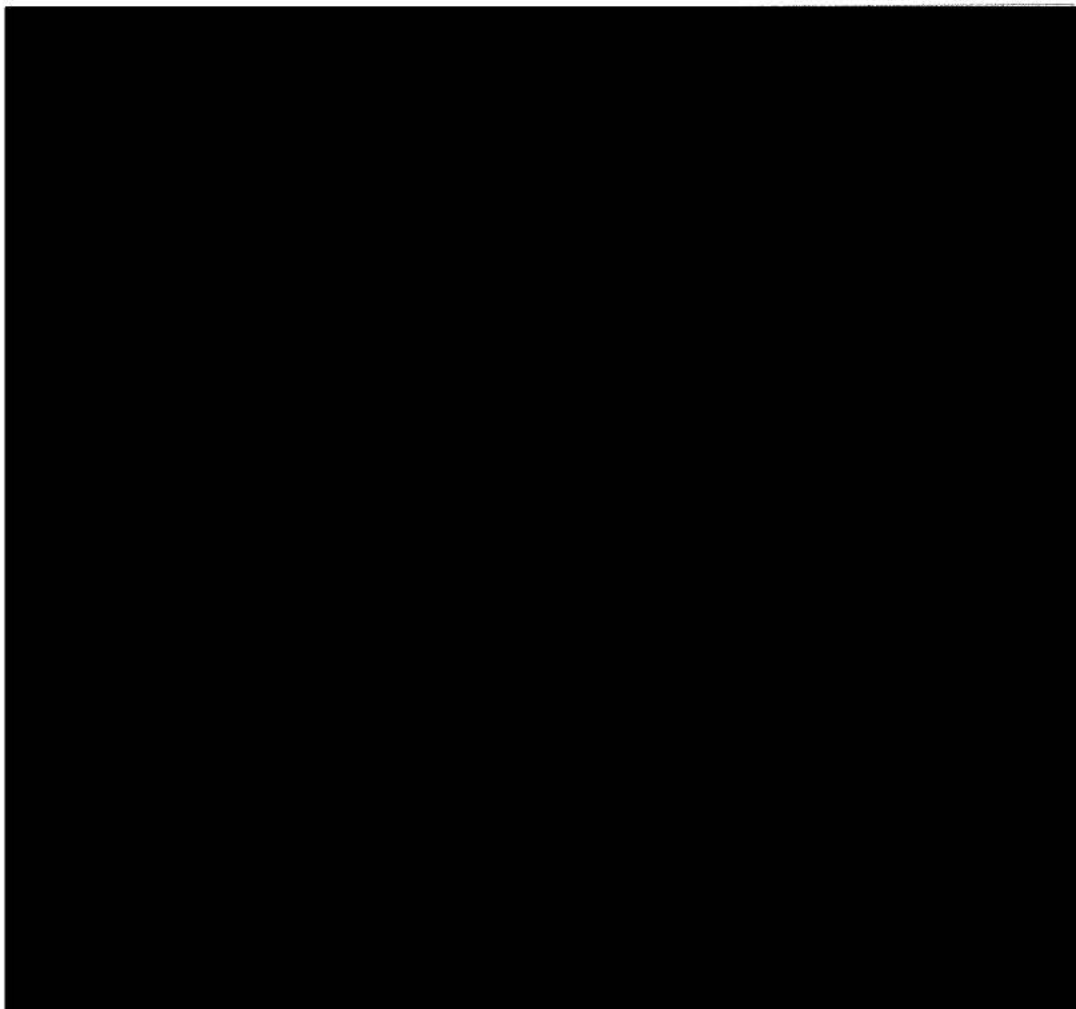
"Google plans censored search engine for China" - The Intercept





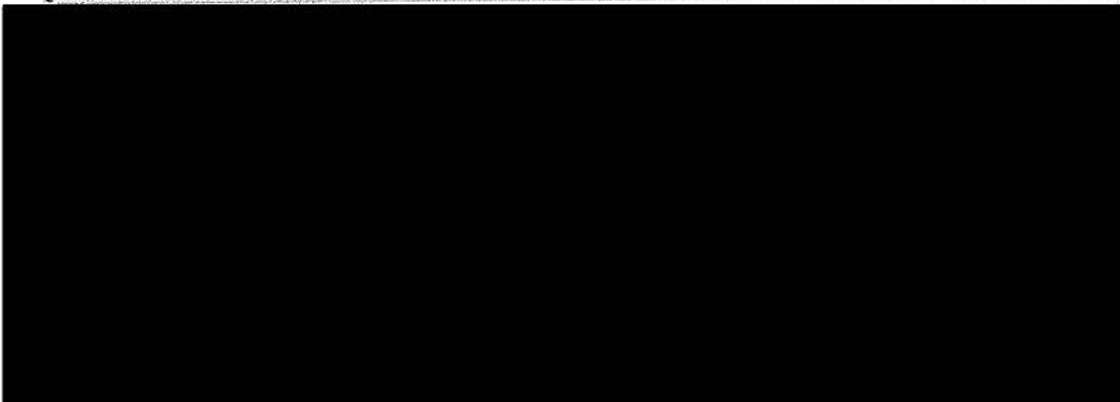


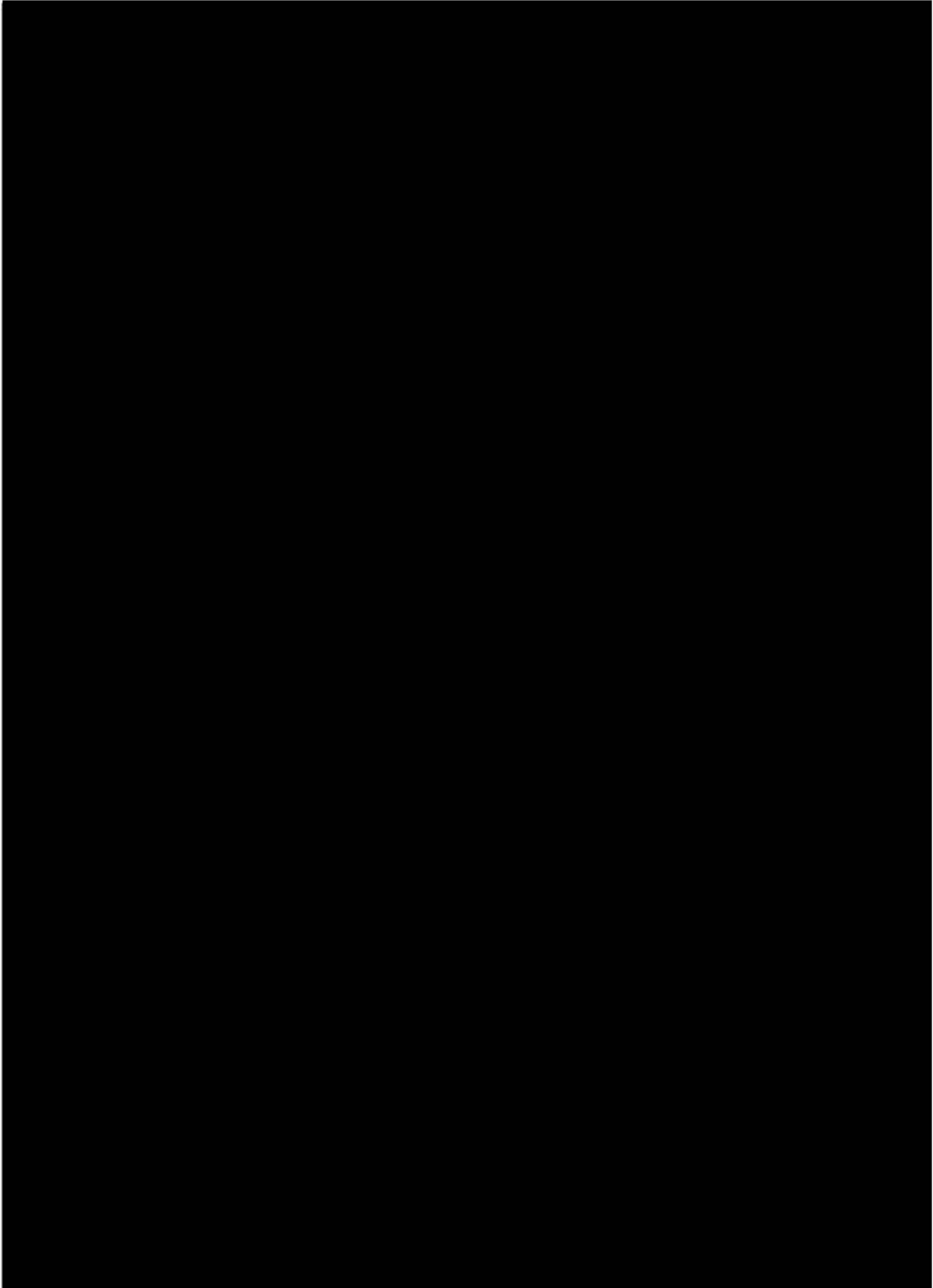


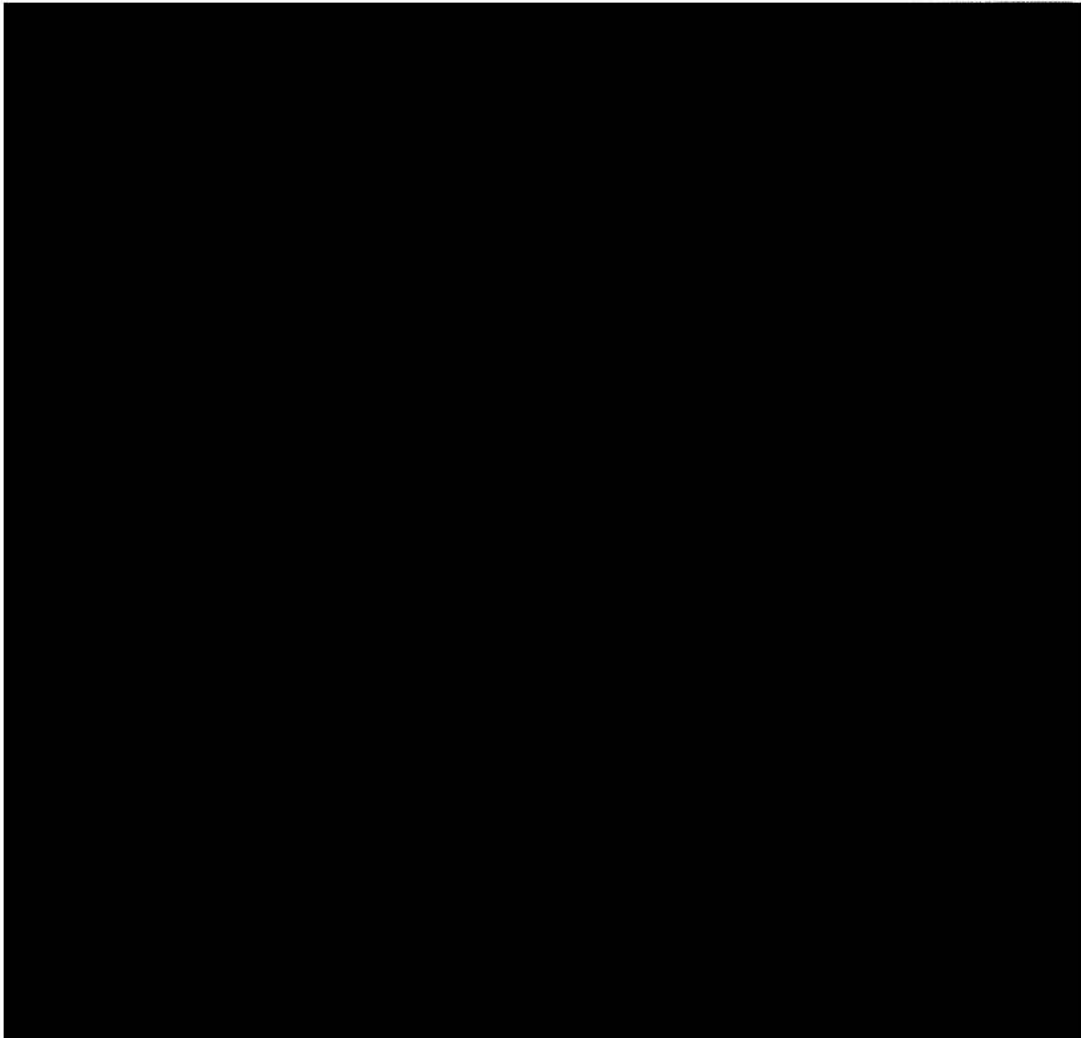


[Back to top](#)

[NY Times Op-Ed] A Better Way to Ban Alex Jones

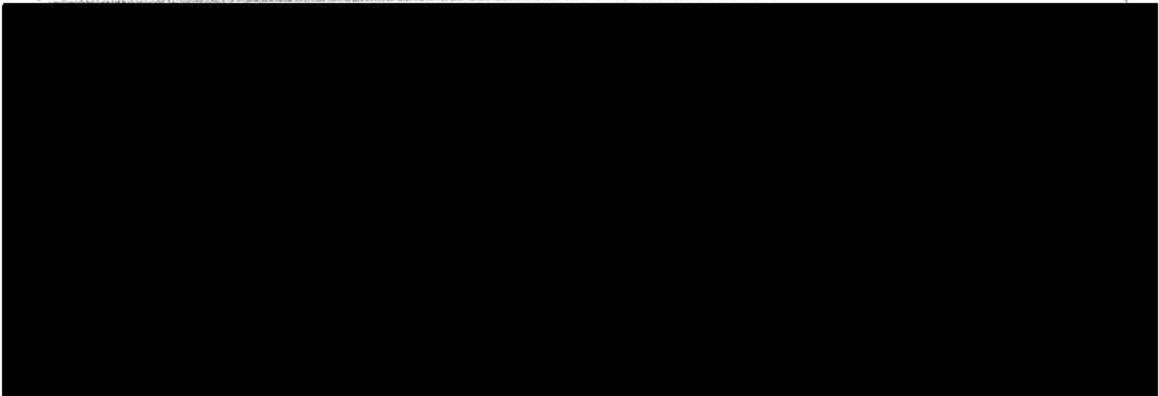






[Back to top](#)

Axios: "How tech fuels authoritarians"



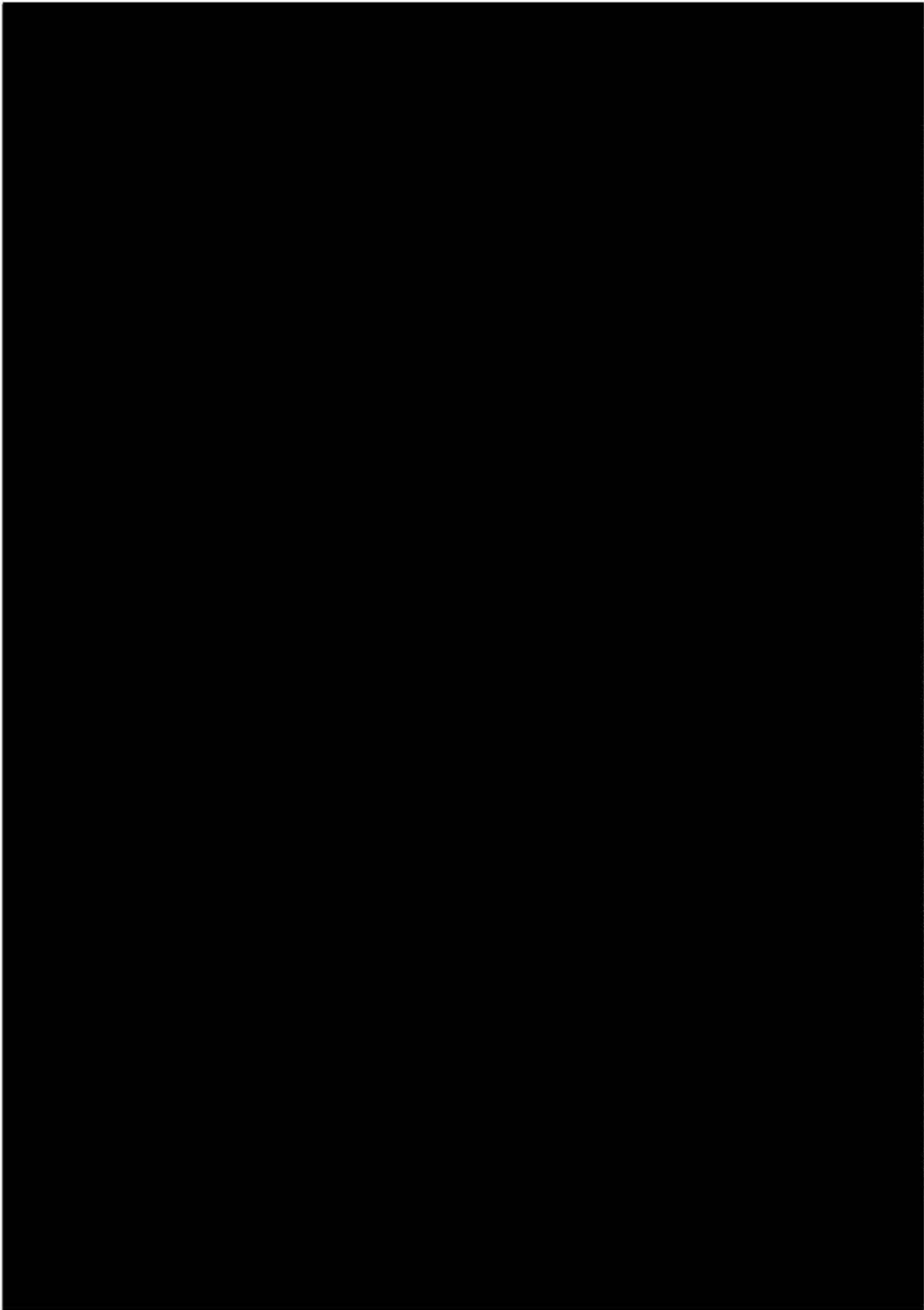




Exhibit 72

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective January 22, 2019

[Archived versions](#)

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for key terms. And if you have any questions about this Privacy Policy, you can [contact us](#).

INFORMATION GOOGLE COLLECTS



GOOG-GLAZ-00000715

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do things like maintain your language preferences across browsing sessions.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

Things you create or provide to us

When you create a Google Account, you provide us with personal information that includes your name and a password. You can also choose to add a phone number or payment information to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information – like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type, carrier name, crash reports, and which apps you've installed.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.

You can visit your Google Account to find and manage activity information that's saved in your account.

© 2017 Google LLC. All rights reserved. Google, the Google logo, Android, the Android logo, and other marks contained herein are trademarks of Google LLC in the U.S. and other countries. Other marks contained herein are trademarks of their respective owners.



[Go to Google Account](#)

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- [IP address](#)
- [Sensor data from your device](#)
- [Information about things near your device](#), such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, Security Checkup provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.



[Go to Ad Settings](#)

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites that use Google Analytics, Google and a Google Analytics customer may link information about your activity from that site with activity from other sites that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the [Privacy Checkup](#), which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our [Product Privacy Guide](#).



[Go to Privacy Checkup](#)

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your Google Account includes:

Privacy controls



Activity Controls

Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube watch history to get better video suggestions.

[Go to Activity Controls](#)



Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that [partner with Google](#) to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

[Go to Ad Settings](#)



About you

Control what others see about you across Google services.

[Go to About You](#)



Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

[Go to Shared Endorsements](#)

Information you share



Control whom you share information with through your account on Google+.

[Go to Information You Share](#)

Ways to review & update your information



My Activity

My Activity allows you to review and control data that's created when you use Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

[Go to My Activity](#)



Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

[Go to Dashboard](#)



Your personal information

Manage your contact information, such as your name, email, and phone number.

[Go to Personal Info](#)

When you're signed out, you can manage information associated with your browser or device, including:

- **Signed out search personalization:** Choose whether your search activity is used to offer you more relevant results and recommendations.
- **YouTube settings:** Pause and delete your YouTube Search History and your YouTube Watch History.
- **Ad Settings:** Manage your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



Export your data

You can also request to remove content from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#)
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account



Delete your information

And finally, Inactive Account Manager allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- **Browser settings:** For example, you can configure your browser to indicate when Google has set a [cookie](#) in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services [rely on cookies to function properly](#), for things like remembering your language preferences.
 - **Device-level settings:** Your device may have controls that determine what information we collect. For example, you can [modify location settings](#) on your Android device.
-

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing a song in Play, your name and photo appear next to your activity. We may also display this information in ads depending on your Shared endorsements setting.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you use Google Home to make a reservation through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services (like G Suite), your domain administrator and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password

- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help us with customer support.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our Transparency Report.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



Export your data

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#)
- Delete specific Google products, including your information associated with those products
- Delete your entire Google Account



Delete your information

In some cases, we retain data for limited periods when it needs to be kept for legitimate business or legal purposes. You can read about Google's data retention periods, including how long it takes us to delete your information.

We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain [servers around the world](#) and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US and Swiss-US Privacy Shield Frameworks.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection

authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites that may include Google services, be displayed to you in search results, or be linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to archived versions for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- Chrome & the Chrome Operating System
- Play Books

- Payments
- Fiber
- Google Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link, for Children under 13 (or applicable age in your country)

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- Your Google Account is home to many of the settings you can use to manage your account
- Privacy Checkup guides you through key privacy settings for your Google Account
- Google's safety center helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- Privacy & Terms provides more context regarding this Privacy Policy and our Terms of Service
- Technologies includes more information about:
 - How Google uses cookies
 - Technologies used for Advertising
 - How Google uses pattern recognition to recognize things like faces in photos
 - How Google uses information from sites or apps that use our services

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." [Learn more about Google ads and why you may see particular ads.](#)

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you contact most frequently.

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. [Learn more](#)

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. [Learn more](#)

devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. [Learn more](#)

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Hangouts, for making domestic and international calls
- Google Voice, for making calls, sending text messages, and managing voicemail
- Google Fi, for a phone plan

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. [Learn more](#)

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate.

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. [Learn more](#)
- A flight confirmation email you receive may be used to create a "check-in" button that appears in your Gmail

- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can [learn more here](#). You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can search and browse privately or turn off signed-out search personalization.

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. [Learn more](#)

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't

use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. [Learn more](#)

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The “last account activity” feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. [Learn more](#)

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

combine the information we collect

Some examples of how we combine the information we collect include:

- When you’re signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google

products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. [Learn more](#)

- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. [Learn more](#)
- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based your activity. [Learn more](#)
- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. [Learn more](#)

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

[Learn more about how Google uses data when you use our partners' sites or apps.](#)

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. [Learn more](#)

specific Google services

For example, you can delete your blog from Blogger or a Google Site you own from Google Sites. You can also delete reviews you've left on apps, games, and other content in the Play Store.

rely on cookies to function properly

For example, we use a cookie called 'lbc' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. [Learn more](#)

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. [Learn more in our Transparency Report.](#)

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. [Learn more](#)

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. [Learn more about these partners and how they use your information.](#)

servers around the world

For example, we operate data centers located around the world to help keep our products continuously available for users.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

appropriate safeguards

For example, we may anonymize data, or encrypt data to ensure it can't be linked to other information about you. [Learn more](#)

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

Customizing our services

For example, we may display a Google Doodle on the Search homepage to celebrate an event specific to your country.

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. [Learn more about the companies providing business services in the EU.](#)

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. [Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.](#)

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for "cars" looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -  
http://www.google.com/search?q=cars -  
Firefox 1.0.7; Windows NT 5.1 -  
740674ce2123e969
```

- 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.
- 25/Mar/2003 10:15:32 is the date and time of the query.
- http://www.google.com/search?q=cars is the requested URL, including the search query.
- Firefox 1.0.7; Windows NT 5.1 is the browser and operating system being used.

- 740674ce2123a969 is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

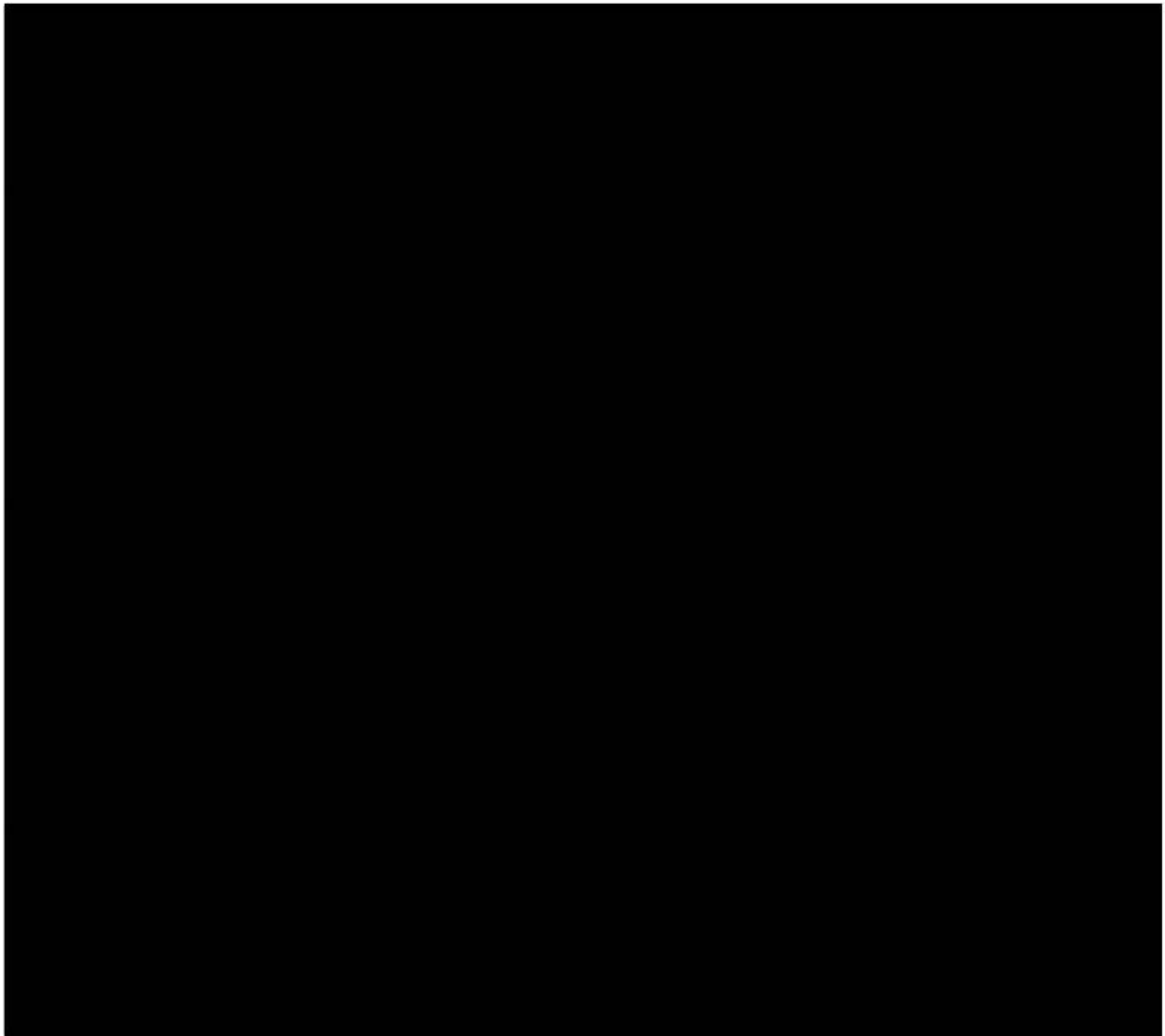
Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

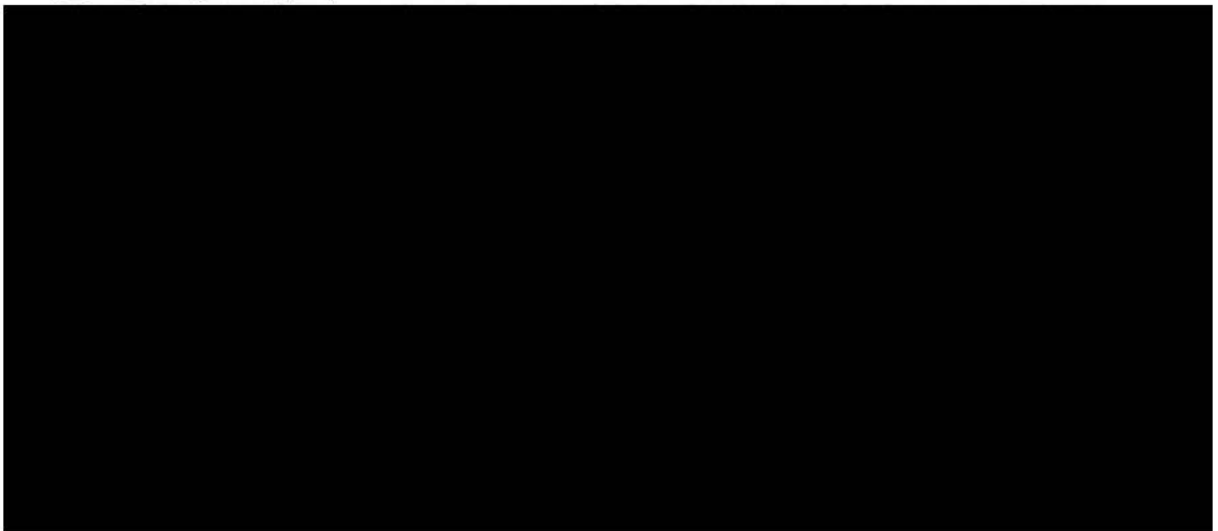
Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. [Learn more about how Google uses cookies.](#)

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be managed in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.

Exhibit 206



http://www.theregister.co.uk/2016/09/12/turn_off_location_services_go_ahead_says_google_well_still_track_you/



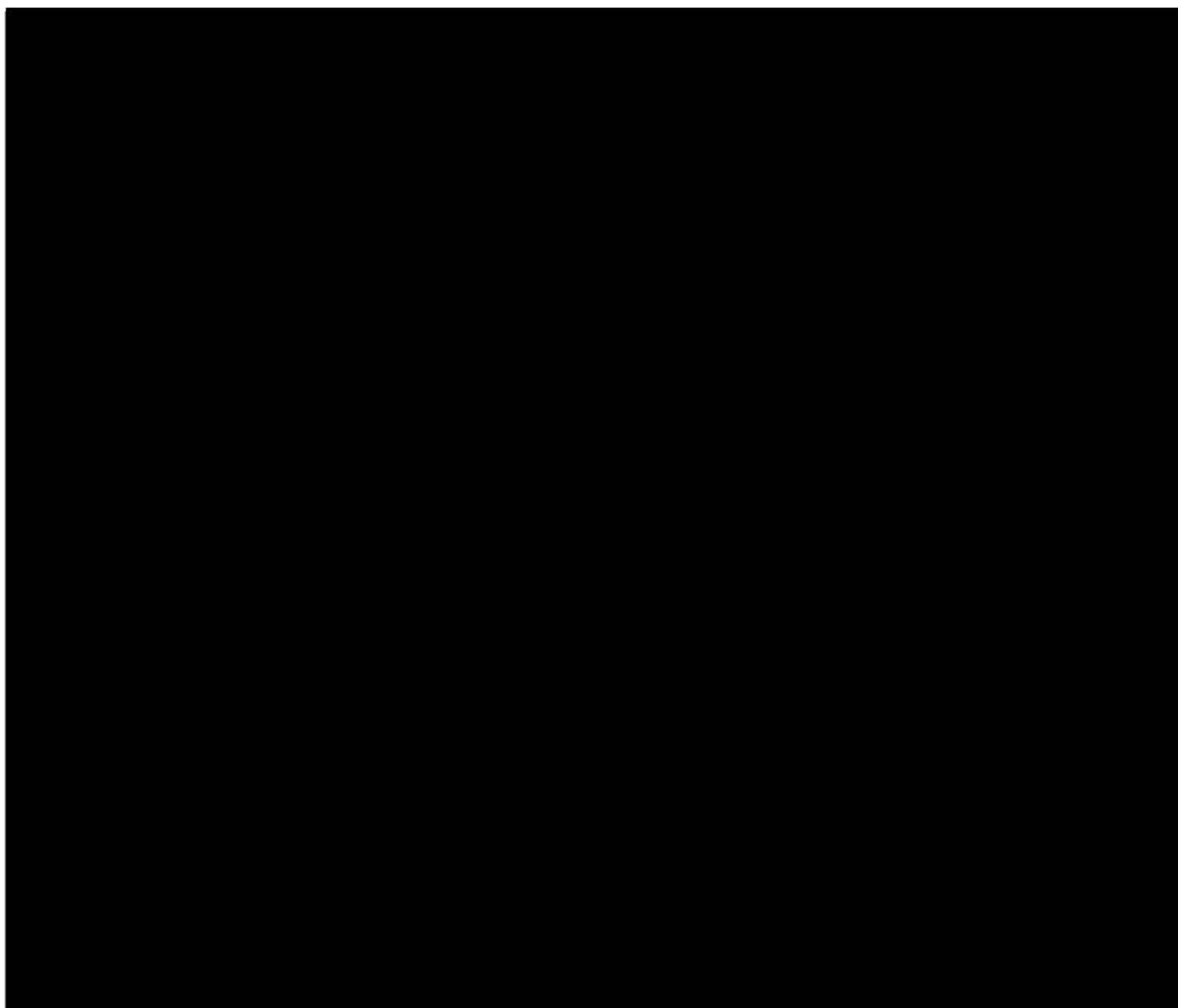
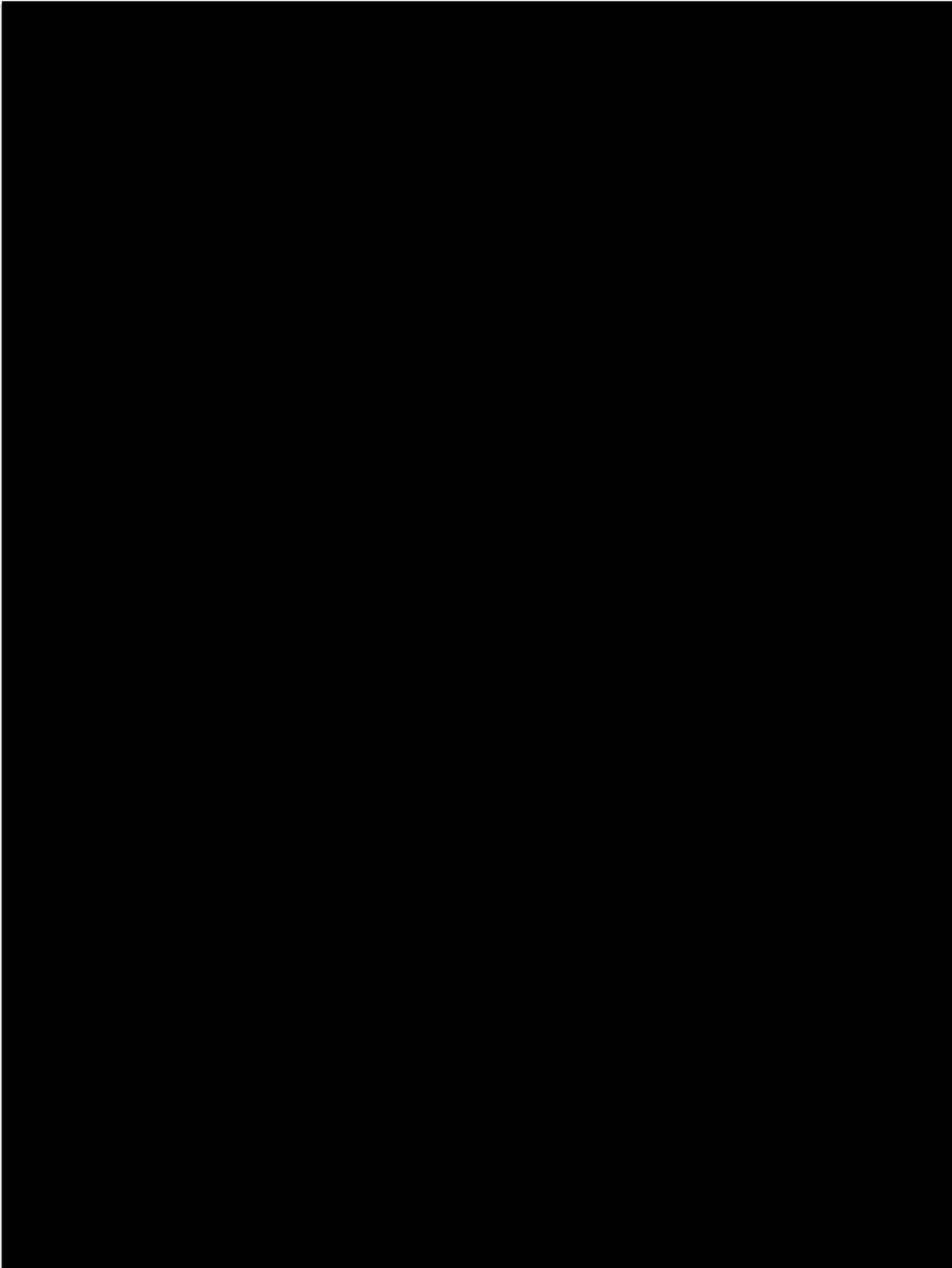
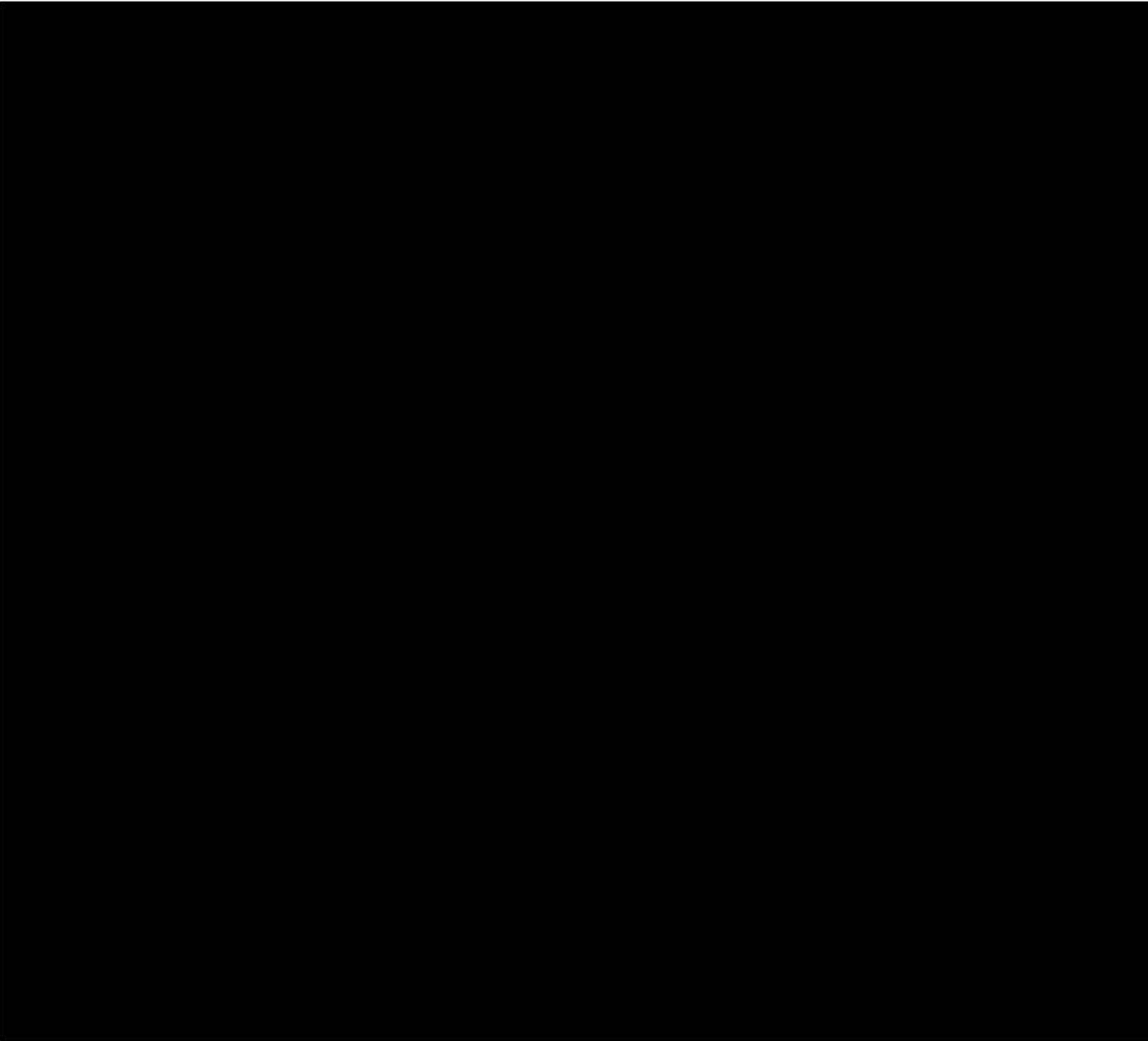


Exhibit 207





<https://apnews.com/828aefab64d4411bac257a07c1af0ecb>

SAN FRANCISCO (AP) — Google wants to know where you go so badly that it records your movements even when you explicitly tell it not to.

An Associated Press investigation found that many Google services on Android devices and iPhones store your location data even if you've used privacy settings that say they will prevent it from doing so.

Computer-science researchers at Princeton confirmed these findings at the AP's request.

For the most part, Google is upfront about asking permission to use your location information. An app like Google Maps will remind you to allow access to location if you use it for navigating. If you agree to let it record your location over time, Google Maps will display that history for you in a “timeline” that maps out your daily movements.

Storing your minute-by-minute travels carries privacy risks and has been used by police to determine the location of suspects — such as a warrant that police in Raleigh, North Carolina, served on Google last year to find devices near a murder scene. So the company will let you “pause” a setting called Location History.

Google says that will prevent the company from remembering where you’ve been. Google’s support page on the subject states: “You can turn off Location History at any time. With Location History off, the places you go are no longer stored.”

That isn’t true. Even with Location History paused, some Google apps automatically store time-stamped location data without asking.

For example, Google stores a snapshot of where you are when you merely open its Maps app. Automatic daily weather updates on Android phones pinpoint roughly where you are. And some searches that have nothing to do with location, like “chocolate chip cookies,” or “kids science kits,” pinpoint your precise latitude and longitude — accurate to the square foot — and save it to your Google account.

The privacy issue affects some two billion users of devices that run Google’s Android operating software and hundreds of millions of worldwide iPhone users who rely on Google for maps or search.

Storing location data in violation of a user’s preferences is wrong, said Jonathan Mayer, a Princeton computer scientist and former chief technologist for the Federal Communications Commission’s enforcement bureau. A researcher from Mayer’s lab confirmed the AP’s findings on multiple Android devices; the AP conducted its own tests on several iPhones that found the same behavior.

“If you’re going to allow users to turn off something called ‘Location History,’ then all the places where you maintain location history should be turned off,” Mayer said. “That seems like a pretty straightforward position to have.”

Google says it is being perfectly clear.

“There are a number of different ways that Google may use location to improve people’s experience, including: Location History, Web and App Activity, and through device-level Location Services,” a Google spokesperson said in a statement to the AP. “We provide clear descriptions of these tools, and robust controls so people can turn them on or off, and delete their histories at any time.”

To stop Google from saving these location markers, the company says, users can turn off

another setting, one that does not specifically reference location information. Called “Web and App Activity” and enabled by default, that setting stores a variety of information from Google apps and websites to your Google account.

When paused, it will prevent activity on any device from being saved to your account. But leaving “Web & App Activity” on and turning “Location History” off only prevents Google from adding your movements to the “timeline,” its visualization of your daily travels. It does not stop Google’s collection of other location markers.

You can delete these location markers by hand, but it’s a painstaking process since you have to select them individually, unless you want to delete all of your stored activity.

You can see the stored location markers on a page in your Google account at myactivity.google.com, although they’re typically scattered under several different headers, many of which are unrelated to location.

To demonstrate how powerful these other markers can be, the AP created a visual map of the movements of Princeton postdoctoral researcher Gunes Acar, who carried an Android phone with Location history off, and shared a record of his Google account.

The map includes Acar’s train commute on two trips to New York and visits to The High Line park, Chelsea Market, Hell’s Kitchen, Central Park and Harlem. To protect his privacy, The AP didn’t plot the most telling and frequent marker — his home address.

Huge tech companies are under increasing scrutiny over their data practices, following a series of privacy scandals at Facebook and new data-privacy rules recently adopted by the European Union. Last year, the business news site Quartz found that Google was tracking Android users by collecting the addresses of nearby cellphone towers even if all location services were off. Google changed the practice and insisted it never recorded the data anyway.

Critics say Google’s insistence on tracking its users’ locations stems from its drive to boost advertising revenue.

“They build advertising information out of data,” said Peter Lenz, the senior geospatial analyst at Dstillery, a rival advertising technology company. “More data for them presumably means more profit.”

The AP learned of the issue from K. Shankari, a graduate researcher at UC Berkeley who studies the commuting patterns of volunteers in order to help urban planners. She noticed that her Android phone prompted her to rate a shopping trip to Kohl’s, even though she had turned Location History off.

“So how did Google Maps know where I was?” she asked in a blog post .

The AP wasn’t able to recreate Shankari’s experience exactly. But its attempts to do so revealed Google’s tracking. The findings disturbed her.

“I am not opposed to background location tracking in principle,” she said. “It just really bothers me that it is not explicitly stated.”

Google offers a more accurate description of how Location History actually works in a place you’d only see if you turn it off — a popup that appears when you “pause” Location History on your Google account webpage . There the company notes that “some location data may be saved as part of your activity on other Google services, like Search and Maps.”

Google offers additional information in a popup that appears if you re-activate the “Web & App Activity” setting — an uncommon action for many users, since this setting is on by default. That popup states that, when active, the setting “saves the things you do on Google sites, apps, and services ... and associated information, like location.”

Warnings when you’re about to turn Location History off via Android and iPhone device settings are more difficult to interpret. On Android, the popup explains that “places you go with your devices will stop being added to your Location History map.” On the iPhone, it simply reads, “None of your Google apps will be able to store location data in Location History.”

The iPhone text is technically true if potentially misleading. With Location History off, Google Maps and other apps store your whereabouts in a section of your account called “My Activity,” not “Location History.”

Since 2014, Google has let advertisers track the effectiveness of online ads at driving foot traffic , a feature that Google has said relies on user location histories.

The company is pushing further into such location-aware tracking to drive ad revenue, which rose 20 percent last year to \$95.4 billion. At a Google Marketing Live summit in July, Google executives unveiled a new tool called “local campaigns” that dynamically uses ads to boost in-person store visits. It says it can measure how well a campaign drove foot traffic with data pulled from Google users’ location histories.

Google also says location records stored in My Activity are used to target ads. Ad buyers can target ads to specific locations — say, a mile radius around a particular landmark — and typically have to pay more to reach this narrower audience.

While disabling “Web & App Activity” will stop Google from storing location markers, it also prevents Google from storing information generated by searches and other activity. That can limit the effectiveness of the Google Assistant, the company’s digital concierge.

Sean O’Brien, a Yale Privacy Lab researcher with whom the AP shared its findings, said it is “disingenuous” for Google to continuously record these locations even when users disable Location History. “To me, it’s something people should know,” he said.

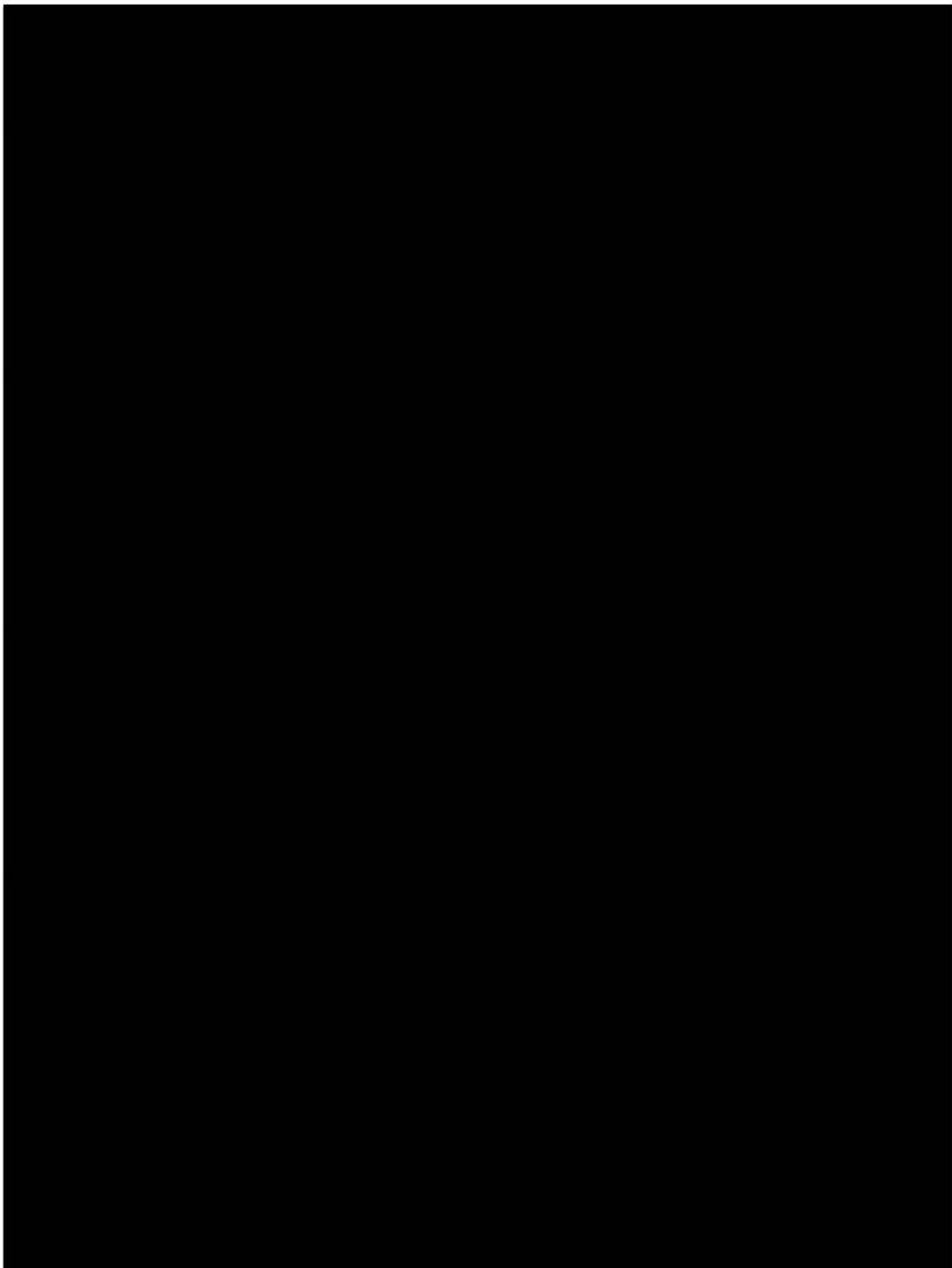
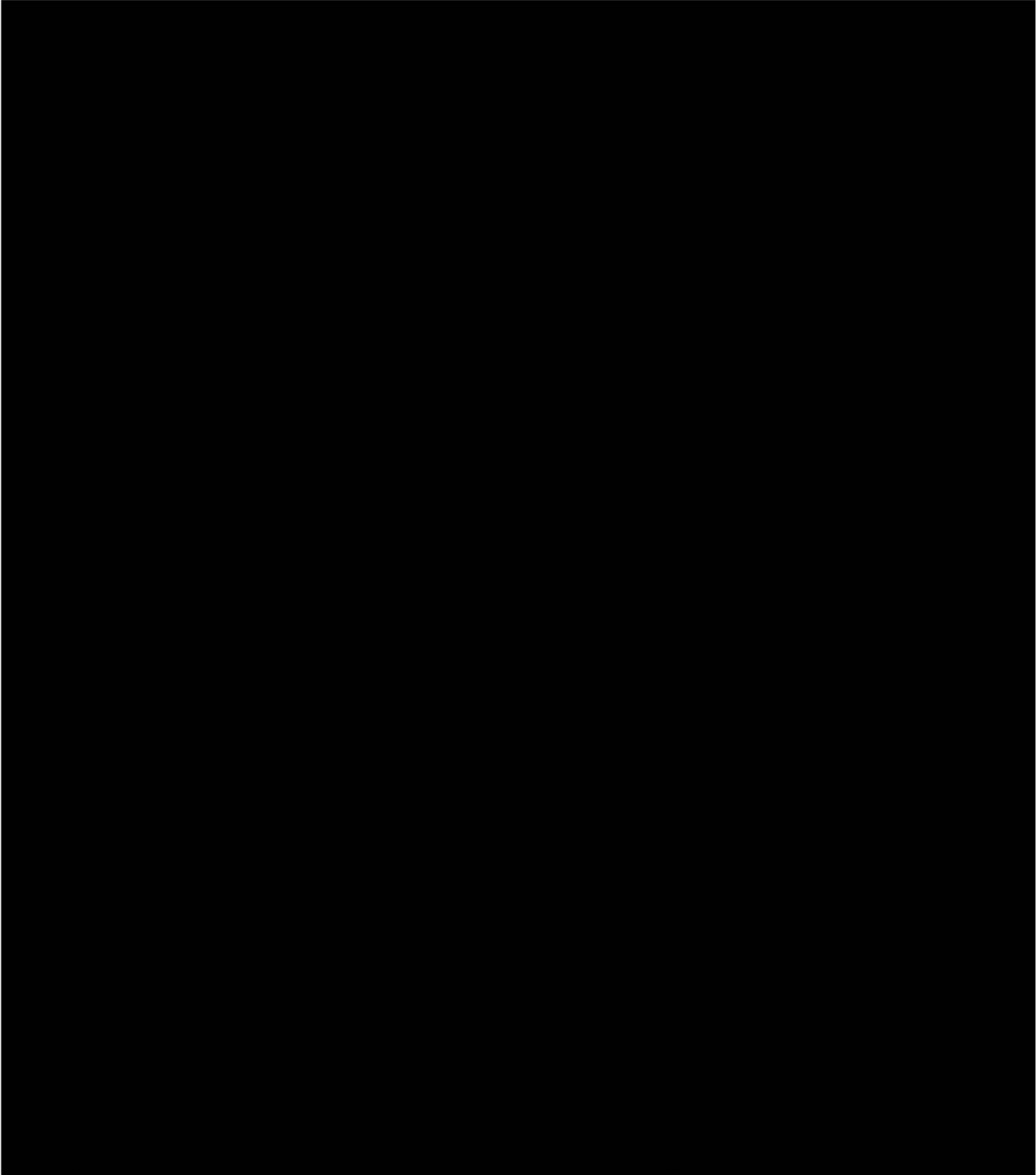




Exhibit 215



"Often, Google employees said, the company responds to a single warrant with location information on dozens or hundreds of devices."

"This year, one Google employee said, the company received as many as 180 requests in one week. Google declined to confirm precise numbers."

"The new orders, sometimes called 'geofence' warrants, specify an area and a time

period, and Google gathers information from Sensorvault about the devices that were there. It labels them with anonymous ID numbers, and detectives look at locations and movement patterns to see if any appear relevant to the crime. Once they narrow the field to a few devices they think belong to suspects or witnesses, Google reveals the users' names and other information."

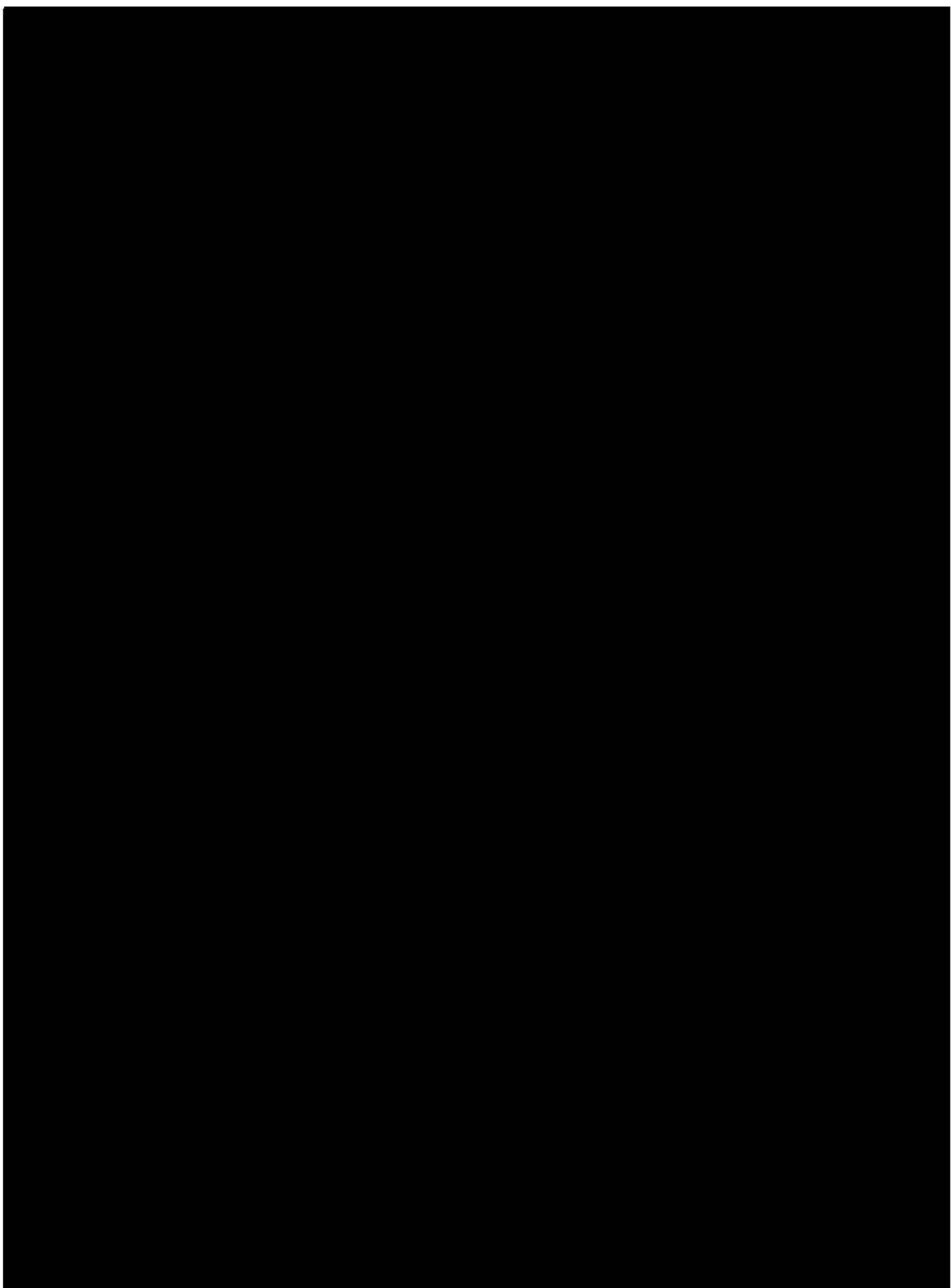
"The areas they targeted ranged from single buildings to multiple blocks, and most sought data over a few hours. In the Austin case, warrants covered several dozen houses around each bombing location, for times ranging from 12 hours to a week. It wasn't clear whether Google responded to all the requests, and multiple officials said they had seen the company push back on broad searches."

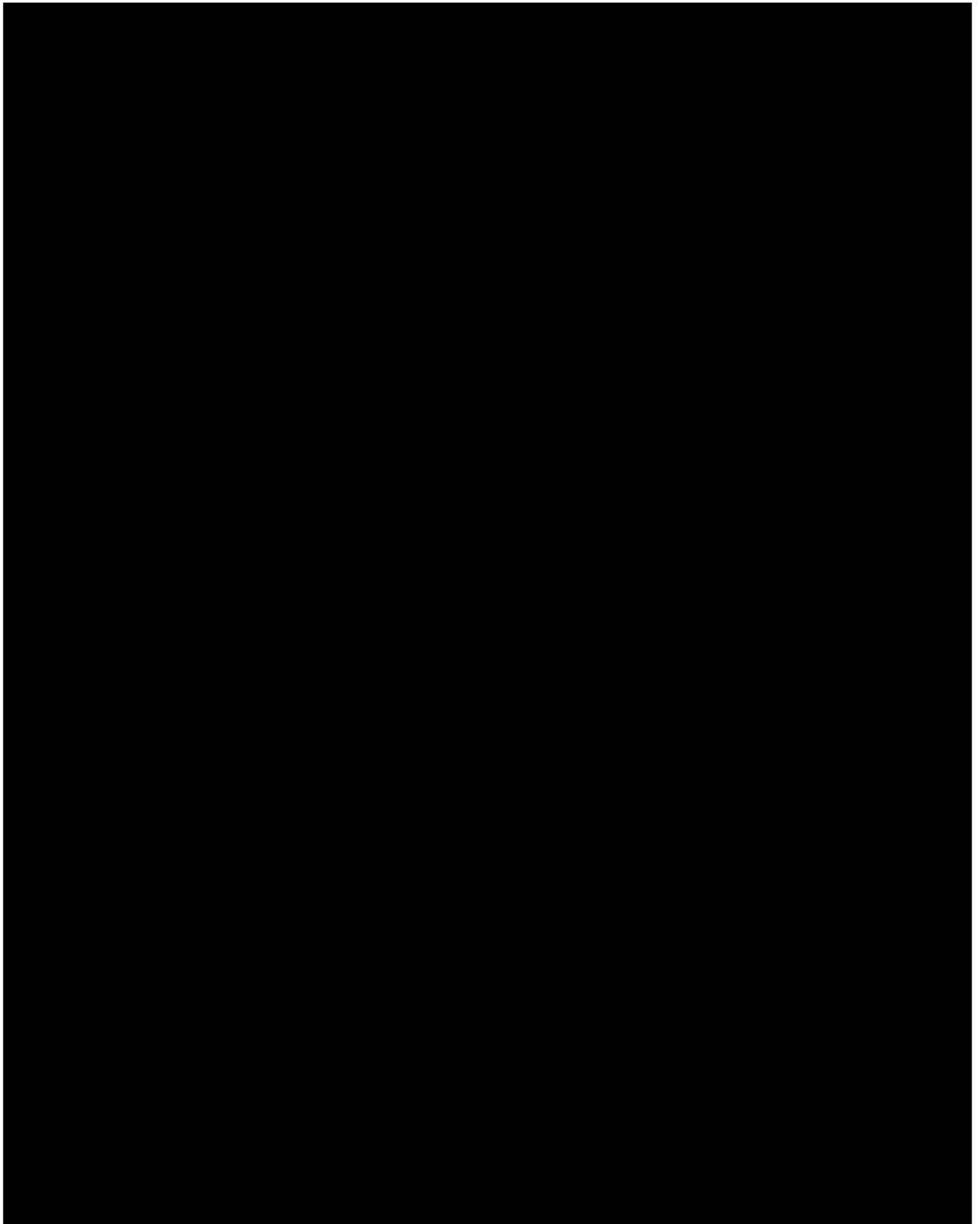
[REDACTED]

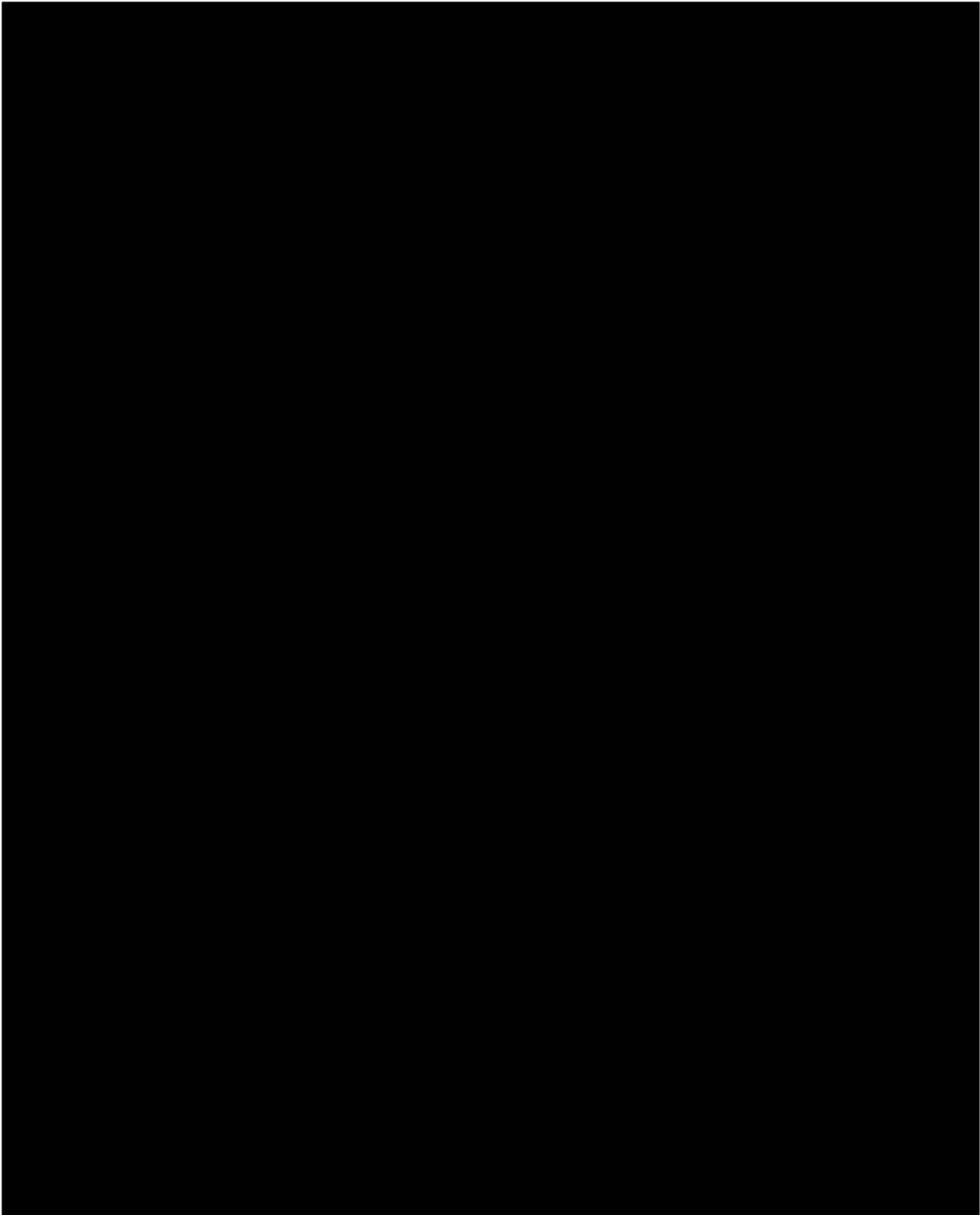
[REDACTED]

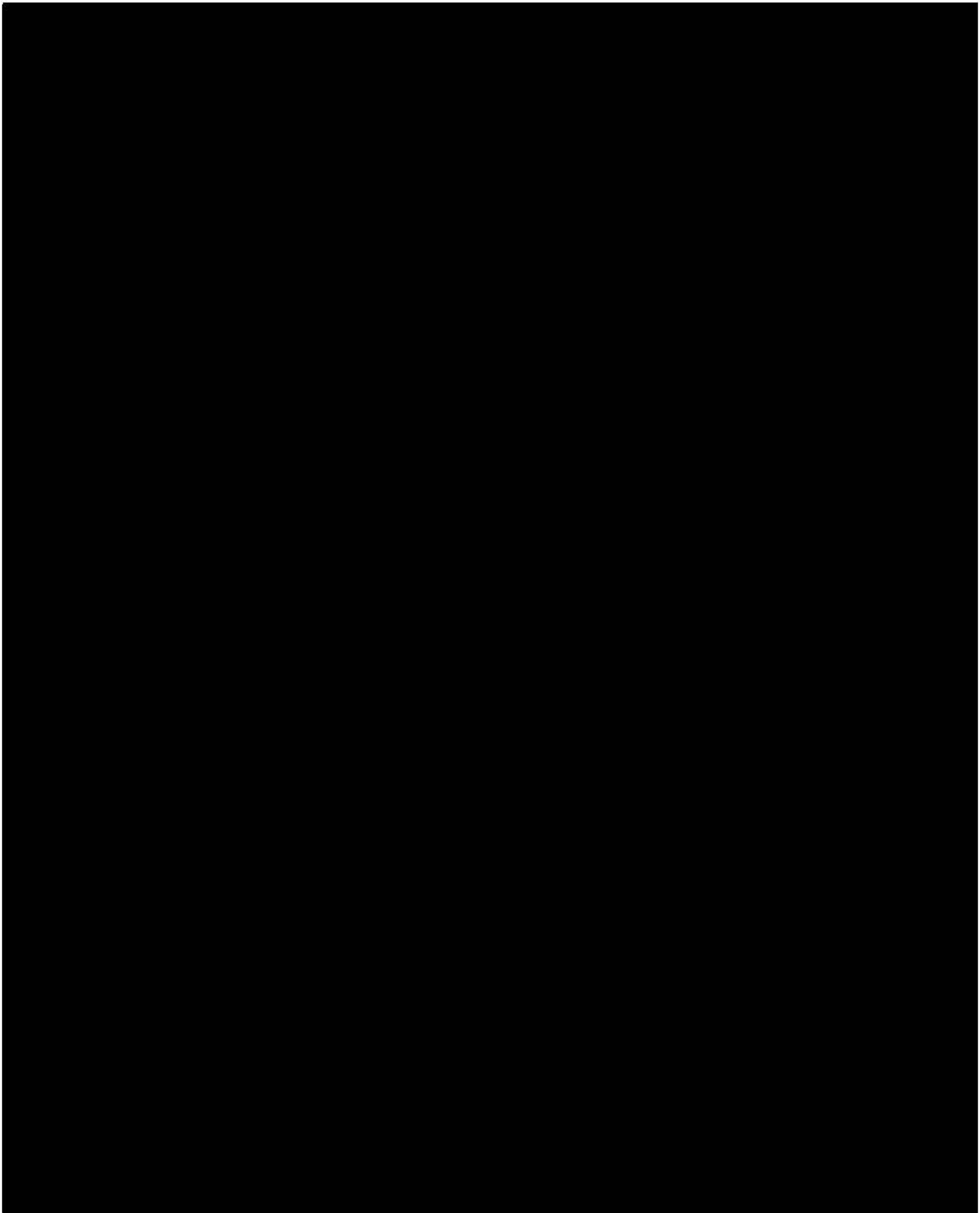
"In Minnesota, for example, the name of an innocent man was released to a local journalist after it became part of the police record. Investigators had his information because he was within 170 feet of a burglary. Reached by a reporter, the man said he was surprised about the release of his data and thought he might have appeared because he was a cabdriver. "I drive everywhere," he said."

[REDACTED]









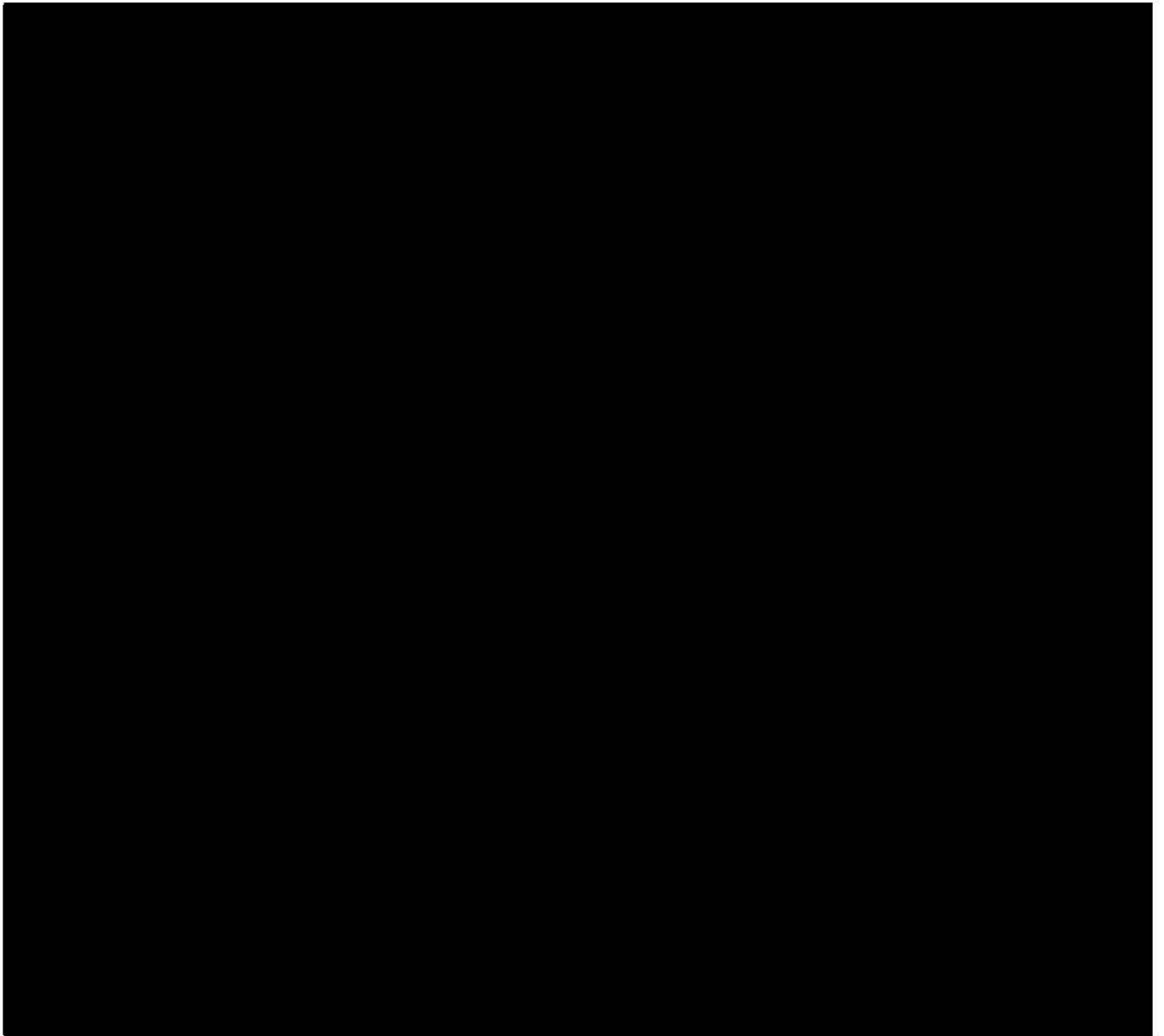
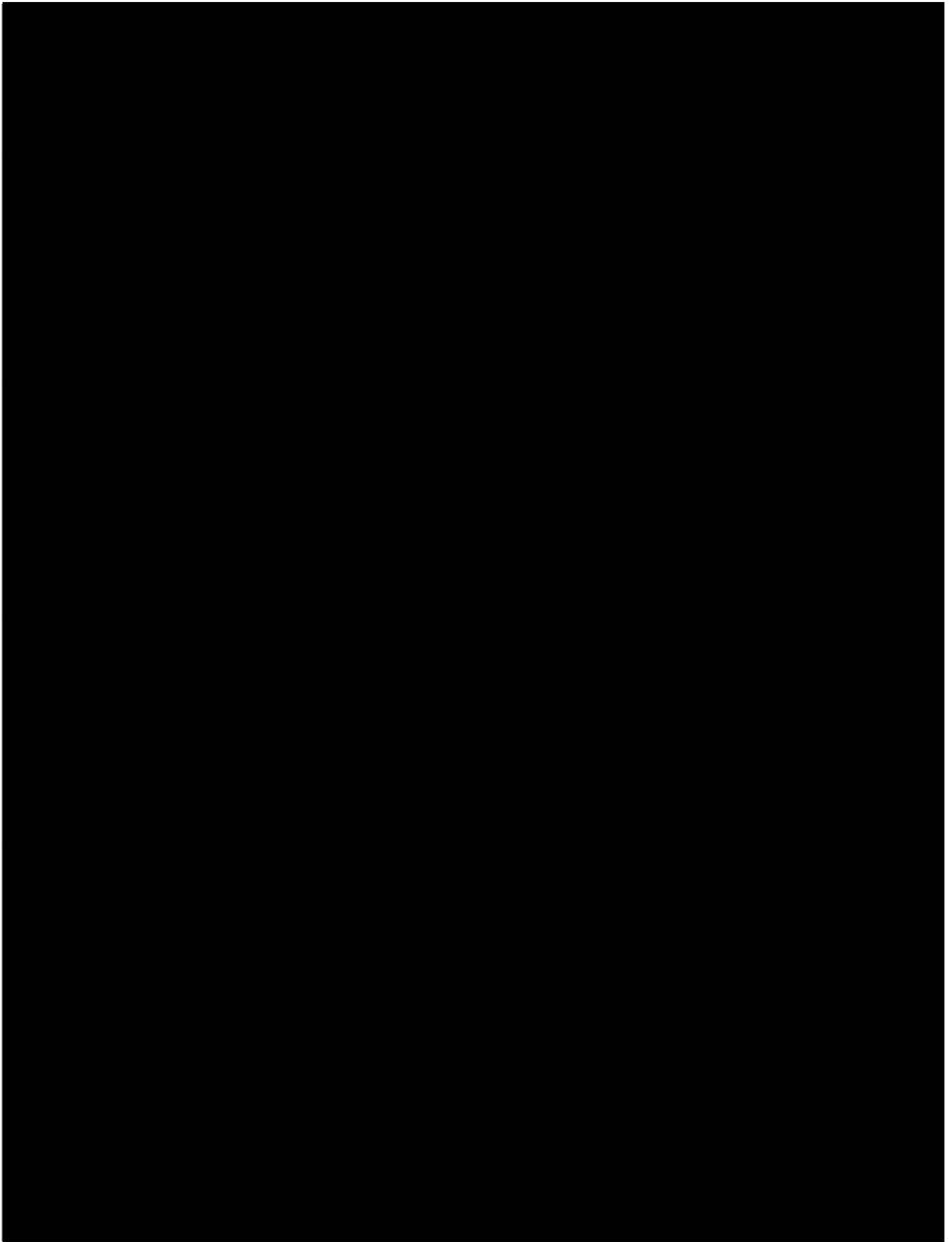
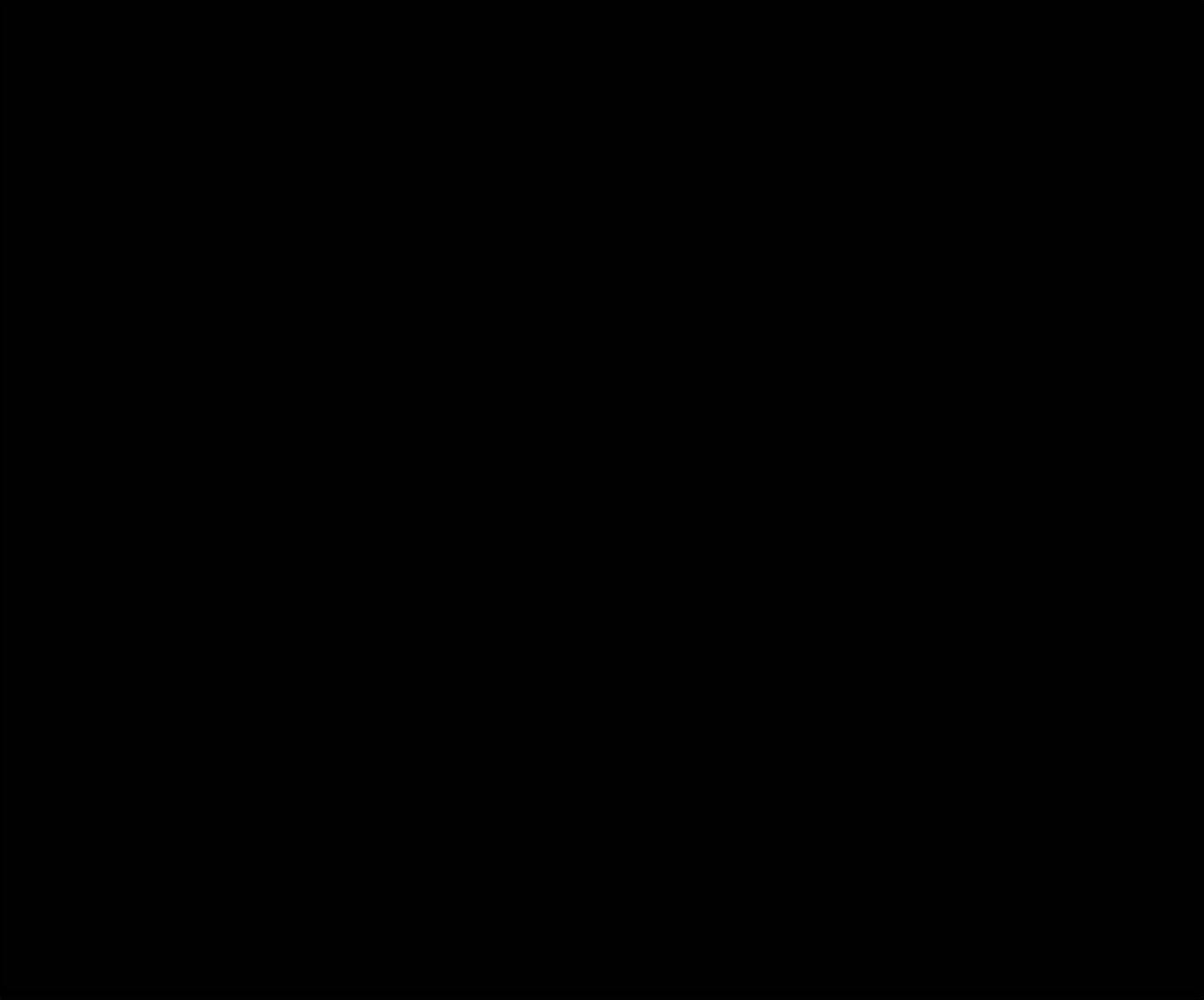


Exhibit 224





<https://apnews.com/828acfab64d4411bac257a07c1af0ecb>

SAN FRANCISCO (AP) — Google wants to know where you go so badly that it records your movements even when you explicitly tell it not to.

An Associated Press investigation found that many Google services on Android devices and iPhones store your location data even if you've used privacy settings that say they will prevent it from doing so.

Computer-science researchers at Princeton confirmed these findings at the AP's request.

For the most part, Google is upfront about asking permission to use your location information. An app like Google Maps will remind you to allow access to location if you use it for

navigating. If you agree to let it record your location over time, Google Maps will display that history for you in a “timeline” that maps out your daily movements.

Storing your minute-by-minute travels carries privacy risks and has been used by police to determine the location of suspects — such as a warrant that police in Raleigh, North Carolina, served on Google last year to find devices near a murder scene. So the company will let you “pause” a setting called Location History.

Google says that will prevent the company from remembering where you’ve been. Google’s support page on the subject states: “You can turn off Location History at any time. With Location History off, the places you go are no longer stored.”

That isn’t true. Even with Location History paused, some Google apps automatically store time-stamped location data without asking.

For example, Google stores a snapshot of where you are when you merely open its Maps app. Automatic daily weather updates on Android phones pinpoint roughly where you are. And some searches that have nothing to do with location, like “chocolate chip cookies,” or “kids science kits,” pinpoint your precise latitude and longitude — accurate to the square foot — and save it to your Google account.

The privacy issue affects some two billion users of devices that run Google’s Android operating software and hundreds of millions of worldwide iPhone users who rely on Google for maps or search.

Storing location data in violation of a user’s preferences is wrong, said Jonathan Mayer, a Princeton computer scientist and former chief technologist for the Federal Communications Commission’s enforcement bureau. A researcher from Mayer’s lab confirmed the AP’s findings on multiple Android devices; the AP conducted its own tests on several iPhones that found the same behavior.

“If you’re going to allow users to turn off something called ‘Location History,’ then all the places where you maintain location history should be turned off,” Mayer said. “That seems like a pretty straightforward position to have.”

Google says it is being perfectly clear.

“There are a number of different ways that Google may use location to improve people’s experience, including: Location History, Web and App Activity, and through device-level Location Services,” a Google spokesperson said in a statement to the AP. “We provide clear descriptions of these tools, and robust controls so people can turn them on or off, and delete their histories at any time.”

To stop Google from saving these location markers, the company says, users can turn off another setting, one that does not specifically reference location information. Called “Web and App Activity” and enabled by default, that setting stores a variety of information from Google apps and websites to your Google account.

When paused, it will prevent activity on any device from being saved to your account. But leaving “Web & App Activity” on and turning “Location History” off only prevents Google from adding your movements to the “timeline,” its visualization of your daily travels. It does not stop Google’s collection of other location markers.

You can delete these location markers by hand, but it’s a painstaking process since you have to select them individually, unless you want to delete all of your stored activity.

You can see the stored location markers on a page in your Google account at myactivity.google.com, although they’re typically scattered under several different headers, many of which are unrelated to location.

To demonstrate how powerful these other markers can be, the AP created a visual map of the movements of Princeton postdoctoral researcher Gunes Acar, who carried an Android phone with Location history off, and shared a record of his Google account.

The map includes Acar’s train commute on two trips to New York and visits to The High Line park, Chelsea Market, Hell’s Kitchen, Central Park and Harlem. To protect his privacy, The AP didn’t plot the most telling and frequent marker — his home address.

Huge tech companies are under increasing scrutiny over their data practices, following a series of privacy scandals at Facebook and new data-privacy rules recently adopted by the European Union. Last year, the business news site Quartz found that Google was tracking Android users by collecting the addresses of nearby cellphone towers even if all location services were off. Google changed the practice and insisted it never recorded the data anyway.

Critics say Google’s insistence on tracking its users’ locations stems from its drive to boost advertising revenue.

“They build advertising information out of data,” said Peter Lenz, the senior geospatial analyst at Dstillery, a rival advertising technology company. “More data for them presumably means more profit.”

The AP learned of the issue from K. Shankari, a graduate researcher at UC Berkeley who studies the commuting patterns of volunteers in order to help urban planners. She noticed that her Android phone prompted her to rate a shopping trip to Kohl’s, even though she had turned Location History off.

“So how did Google Maps know where I was?” she asked in a blog post.

The AP wasn’t able to recreate Shankari’s experience exactly. But its attempts to do so revealed Google’s tracking. The findings disturbed her.

“I am not opposed to background location tracking in principle,” she said. “It just really bothers me that it is not explicitly stated.”

Google offers a more accurate description of how Location History actually works in a place you'd only see if you turn it off — a popup that appears when you “pause” Location History on your Google account webpage . There the company notes that “some location data may be saved as part of your activity on other Google services, like Search and Maps.”

Google offers additional information in a popup that appears if you re-activate the “Web & App Activity” setting — an uncommon action for many users, since this setting is on by default. That popup states that, when active, the setting “saves the things you do on Google sites, apps, and services ... and associated information, like location.”

Warnings when you're about to turn Location History off via Android and iPhone device settings are more difficult to interpret. On Android, the popup explains that “places you go with your devices will stop being added to your Location History map.” On the iPhone, it simply reads, “None of your Google apps will be able to store location data in Location History.”

The iPhone text is technically true if potentially misleading. With Location History off, Google Maps and other apps store your whereabouts in a section of your account called “My Activity,” not “Location History.”

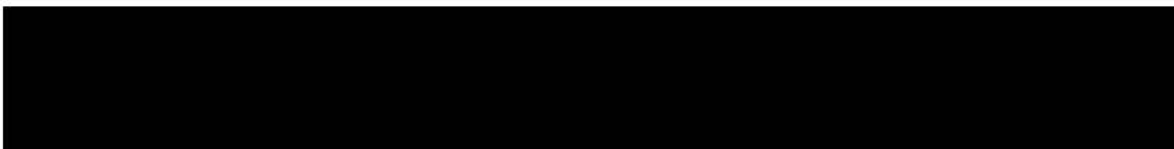
Since 2014, Google has let advertisers track the effectiveness of online ads at driving foot traffic , a feature that Google has said relies on user location histories.

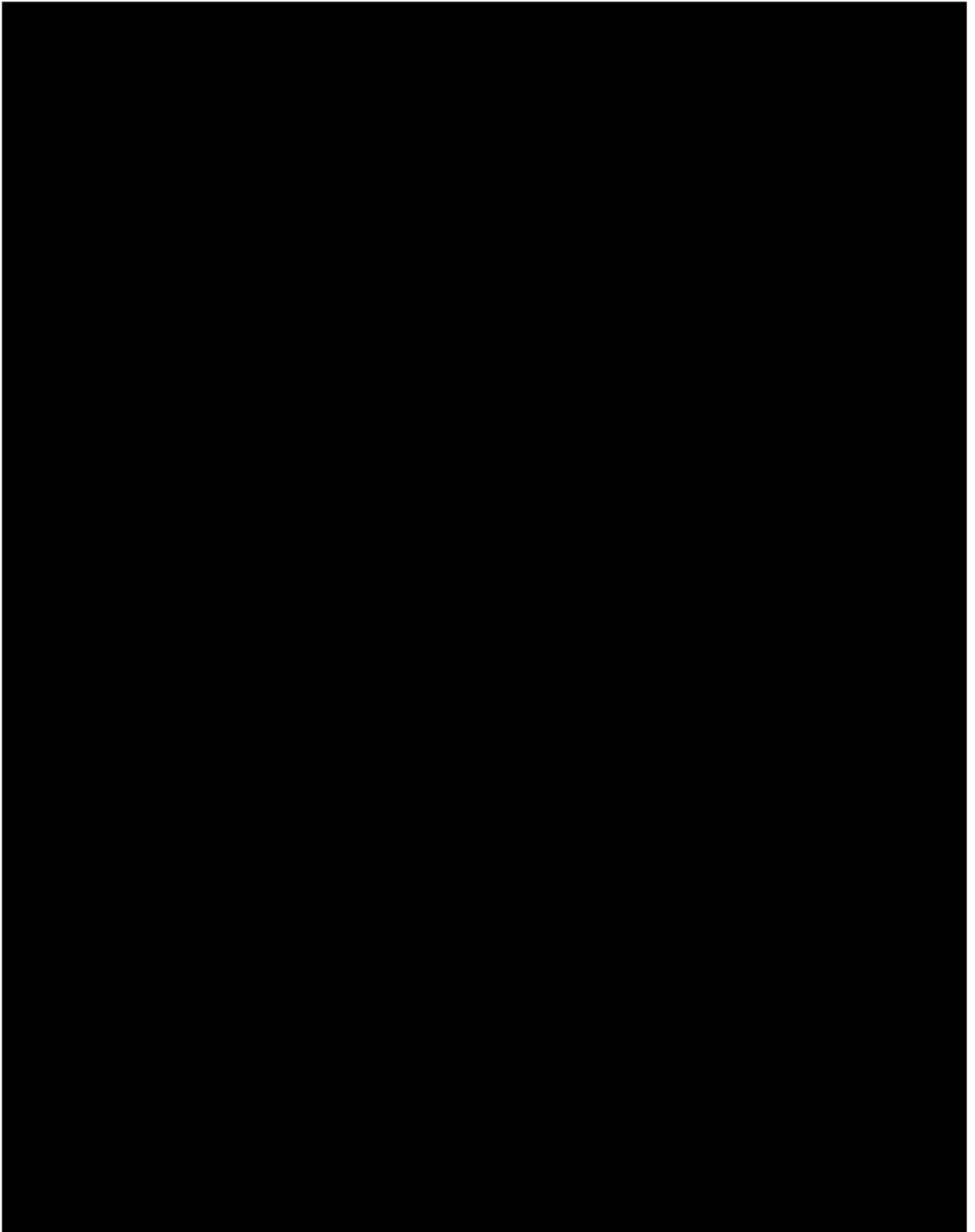
The company is pushing further into such location-aware tracking to drive ad revenue, which rose 20 percent last year to \$95.4 billion. At a Google Marketing Live summit in July, Google executives unveiled a new tool called “local campaigns” that dynamically uses ads to boost in-person store visits. It says it can measure how well a campaign drove foot traffic with data pulled from Google users' location histories.

Google also says location records stored in My Activity are used to target ads. Ad buyers can target ads to specific locations — say, a mile radius around a particular landmark — and typically have to pay more to reach this narrower audience.

While disabling “Web & App Activity” will stop Google from storing location markers, it also prevents Google from storing information generated by searches and other activity. That can limit the effectiveness of the Google Assistant, the company's digital concierge.

Sean O'Brien, a Yale Privacy Lab researcher with whom the AP shared its findings, said it is “disingenuous” for Google to continuously record these locations even when users disable Location History. “To me, it's something people should know,” he said.





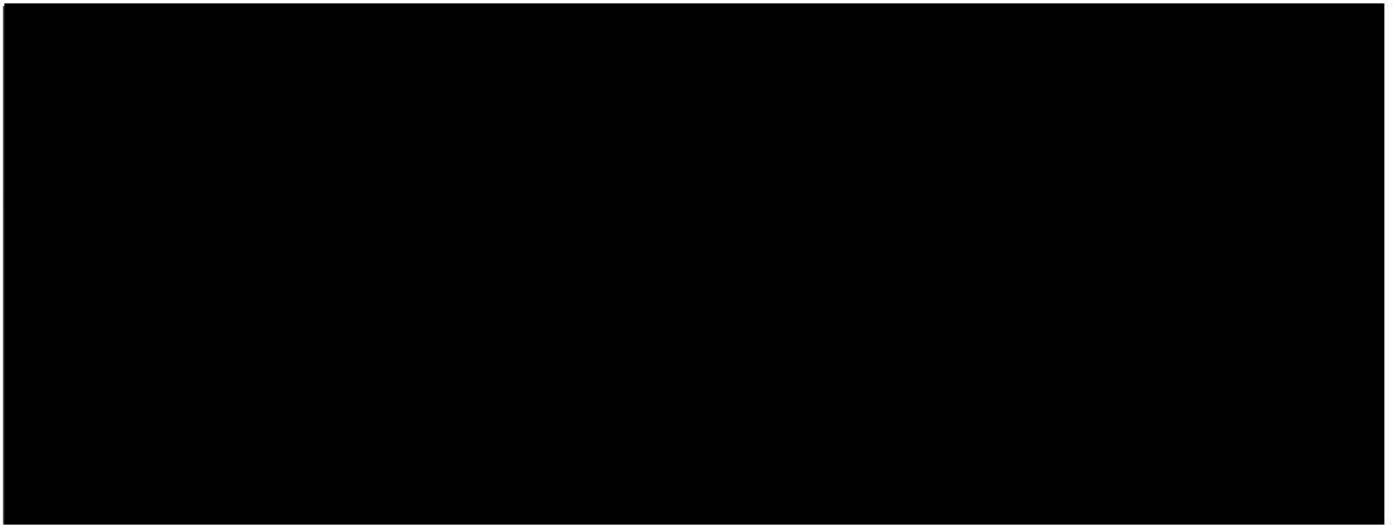


Exhibit 225

Set up Now cards?

To get Now cards, you need to have the following

Google Account settings turned on for

Your searches and browsing activity

Web & App Activity includes searches, Chrome history, and content you browse in apps

Information from your devices

Device Information includes contacts, calendars, apps, music, battery life, sensor readings

Places you go

Location History creates a private map of where you go with your logged-in devices

LEARN MORE

These settings allow Google to store and use information whenever you're signed in to a Google product (like Chrome or YouTube). By choosing "Yes, I'm in", Google will turn these settings on for you. If you choose "Cancel", your existing settings stay the same. You can manage your settings at any time in

CANCEL

YES, I'M IN

