No. 17-961

IN THE
Supreme Court of the United States

THEODORE H. FRANK, ET AL.,
Petitioners,

v.

PALOMA GAOS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, ET AL.,
Respondents.

On Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

CLASS RESPONDENTS' SUPPLEMENTAL BRIEF ON ARTICLE III STANDING

KASSRA P. NASSIRI
Counsel of Record
NASSIRI & JUNG LLP
47 Kearny St.
Suite 700
San Francisco, CA 94108
(415) 762-3100
kass@njfirm.com

JEFFREY A. LAMKEN
MICHAEL G. PATTILLO, JR.
JAMES A. BARTA
WILLIAM J. COOPER
MOLOLAMKEN LLP
The Watergate, Suite 660
600 New Hampshire Ave., N.W.
Washington, D.C. 20037
(202) 556-2000
jlamken@mololamken.com

Counsel for Class Respondents

(Additional Counsel Listed on Inside Cover)

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D.C. 20002

MICHAEL ASCHENBRENER
KAMBERLAW, LLC
201 Milwaukee St.
Suite 200
Denver, CO 80206
(303) 222-0281
masch@kamberlaw.com

JORDAN A. RICE
MOLOLAMKEN LLP
300 N. LaSalle St.
Chicago, IL 60654
(312) 450-6700

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

Page(s)

IN THE

Supreme Court of the United States

NO. 17-961

THEODORE H. FRANK, ET AL.,

Petitioners,

v.

PALOMA GAOS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, ET AL.,

Respondents.

On Writ of Certiorari
to the United States Court of Appeals
for the Ninth Circuit

CLASS RESPONDENTS' SUPPLEMENTAL BRIEF ON ARTICLE III STANDING

The requirement that plaintiffs have "standing" limits the judicial power to "'cases and controversies of the sort traditionally amenable to, and resolved by, the judicial process.'" *Vt. Agency of Nat. Res.* v. *United States ex rel. Stevens*, 529 U.S. 765, 774 (2000). This case represents such a controversy: A dispute arising from the unauthorized disclosure of communications. Such unauthorized disclosures are themselves injurious. This Nation's courts have long heard cases arising from privacy breaches without proof of "specific harm" beyond the breach itself. *Doe* v. *Chao*, 540 U.S. 614, 621 (2004). English and American courts have entertained actions

arising from unauthorized disclosure of communications in particular—like the Stored Communications Act ("SCA") violations here—for over 275 years, even enjoining disclosures or awarding the wrongdoer's profits, again without claimed injury beyond the disclosure itself. See, *e.g.*, *Folsom* v. *Marsh*, 9 F. Cas. 342, 346 (C.C.D. Mass. 1841). The Consolidated Complaint ("Complaint"), moreover, alleges that Google's disclosures breached contractual obligations. More than 180 years ago, this Court recognized that plaintiffs can sue—recovering nominal damages—for breach of contract, even if no loss results. See *Wilcox* v. *Ex'rs of Plummer*, 29 U.S. (4 Pet.) 172, 181-182 (1830). The notion that some further injury is required defies tradition and longstanding precedent.

That said, neither the court of appeals nor the district court below addressed whether the Complaint's allegations establish standing under the standard articulated in *Spokeo, Inc.* v. *Robins*, 136 S. Ct. 1540 (2016)—for the SCA claim *or* the "other four causes of action" asserted. Oral Arg. Tr. 67. This Court ordinarily is "'a court of final review and not first view.'" *Adarand Constructors, Inc.* v. *Mineta*, 534 U.S. 103, 110 (2001) (per curiam). We have found only one court-of-appeals decision applying *Spokeo*'s framework to SCA claims. See *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 272-274 (3d Cir. 2016); p. 17 n.4, *infra*. Nor has there been an opportunity in this Court for full *amicus* participation, despite helpful *amicus* input on similar matters (including *Spokeo* and *First American Financial Corp.* v. *Edwards*, 567 U.S. 756 (2012) (per curiam)). Class Respondents accordingly remain of the view that the Court should refrain from resolving standing here, even if it precludes the Court from addressing the question presented. That question, if important, will recur. A deci-

sion of this Court on standing, by contrast, would be conclusive on important issues—potentially with unanticipated adverse consequences—before most courts of appeals have even been heard.

ARGUMENT

Article III standing requires a plaintiff to demonstrate, among other things, an "injury in fact" that is "'concrete and particularized.'" *Spokeo,* 136 S. Ct. at 1547-1548 (quoting *Lujan* v. *Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). In *Spokeo*, this Court confirmed that "intangible harm" can be injury-in-fact where it bears a "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* at 1549. Congress, moreover, can "'define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before.'" *Ibid.* Risks of harm can suffice as well. *Ibid.* But violation of a statute is not necessarily by itself sufficient. Courts instead must consider both "history" and Congress's "judgment" in deciding whether a violation constitutes a constitutionally sufficient injury-in-fact. *Ibid.*

In this case, that history—the traditional practices of English and American courts—should be "well nigh conclusive." *Vt. Agency*, 529 U.S. at 777. The SCA forbids the unauthorized disclosure of "communications." 18 U.S.C. §2702(a)-(b). For centuries, unauthorized disclosure itself has been sufficient injury to sustain an action in court, without proof of further harm. Courts thus have awarded injunctions against disclosure, as well as the wrongdoer's profits—relief that the Complaint demands and the SCA authorizes. Although no extension of traditional principles is required, Congress resolved any doubt through the cause of action it created in the SCA,

which affords relief without regard to actual harm beyond the disclosure itself. See § 2707(a)-(c). The other causes of action asserted, including breach of contract and unjust enrichment, have similar pedigrees. Those breaches are likewise sufficient to support Article III standing.[1]

Because this case was resolved "at the pleading stage," standing is evaluated based on the complaint. *Spokeo*, 136 S. Ct. at 1547; see *Lujan*, 504 U.S. at 561. The operative Complaint is therefore reproduced as an Appendix (App., *infra*, 1a-60a). We address the asserted causes of action, and their historical antecedents, in turn.[2]

---

[1] Under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), federal courts have jurisdiction over class actions with $5 million in controversy if there is minimal diversity—*i.e.*, if any named plaintiff and defendant are diverse. The Complaint alleges every required element under CAFA: It states that Google's citizenship is different from the citizenship of named plaintiffs, App., *infra*, 3a-4a (¶¶ 8-11); and it seeks disgorgement of profits estimated in the tens of billions, App., *infra*, 5a-6a (¶ 17), 55a-56a (¶¶ 152, 158); see Pet. App. 40 ($8.5 million settlement). Although the Complaint does not cite CAFA, no citation is required when a court "readily can recognize the existence of a federal question or diversity of citizenship and the requisite amount in controversy." 5 C. Wright & A. Miller, *Federal Practice and Procedure* § 1214 (3d ed.). If preferable, the pleadings can be amended under 28 U.S.C. § 1653 now or on remand.

[2] Although we analyze claims individually, history demonstrates that a plaintiff generally need not allege additional harm "to enforce only his personal rights against another private party." *Spokeo*, 136 S. Ct. at 1551 (Thomas, J., concurring). "In a suit for the violation of a private right, courts historically presumed that the plaintiff suffered a *de facto* injury merely from having his personal, legal rights invaded." *Ibid.*; see *Entick* v. *Carrington* (1765) 95 Eng. Rep. 807, 817 (KB); *Ashby* v. *White* (1703) 92 Eng. Rep. 126, 137 (KB); 3 W. Blackstone, *Commentaries on the Laws of England* 23 (1768).

I. NAMED PLAINTIFFS HAVE ARTICLE III STANDING TO ASSERT STORED COMMUNICATIONS ACT CLAIMS

The Complaint alleges that Google disclosed the class representatives' communications—search terms they transmitted to Google—to third parties without authorization in violation of the SCA. App., *infra*, 43a-47a (¶¶100-118), 50a-53a(¶¶130-141). It alleges that Google profited therefrom, "effectively selling" their "search queries." App., *infra*, 34a-35a (¶¶78-82), 52a (¶¶136, 138). The Complaint thus seeks an injunction, App., *infra*, 53a (¶141), 57a-59a (¶¶164-171); recovery of wrongful profits, App., *infra*, 53a (¶141), 59a; and all forms of damages authorized by law, *ibid.* Even apart from threatened harm, see pp. 18-19, *infra*, the alleged wrongful disclosure of individual communications supports standing here.

"[T]he law has long" recognized that actionable harm inheres in the invasion of certain legal rights, such as the right "'to obtain information' that Congress ha[s] decided to make public." *Spokeo*, 136 S. Ct. at 1549. The same rule applies to the right to prevent disclosure of private information. *Doe*, 540 U.S. at 621 & n.3. A "privacy tort victim" thus can recover damages without showing "specific harm[s]." *Id.* at 621. As explained below, centuries of law likewise establish that persons whose *communications* are disclosed without authorization "need not allege any *additional* harm beyond" the disclosure itself. *Spokeo*, 136 S. Ct. at 1549.

A. Founding-Era Courts Redressed Unauthorized Disclosures Without Requiring Further Harm

English and American courts have long held that the disclosure of communications without consent is actionable, either as an invasion of "property" or "a breach of private confidence or contract." *Folsom*, 9 F. Cas. at 346. No further showing of harm was required. Courts pre-

sumed the disclosure itself inflicted actionable—indeed irreparable—injury.

1. As early as 1741, English courts heard cases arising from the unauthorized disclosure of communications. See *Pope* v. *Curl* (1741) 26 Eng. Rep. 608, 608 (Ch.). English law recognized that "'every man has a right to keep his own sentiments' and 'a right to judge whether he will make them public.'" D. Seipp, *English Judicial Recognition of a Right to Privacy*, 3 Oxford J. Legal Stud. 325, 338 (1983). Writers of letters had a right to control their communications on "familiar subjects" no less than authors of literary works. *Pope*, 26 Eng. Rep. at 608. It was "ever so clear" that both had a "property" right in, and the right to control dissemination of, their writings. *Gee* v. *Pritchard* (1818) 36 Eng. Rep. 670, 674-675, 677 (Ch.).

English courts regularly restrained the unauthorized publication of letters without asking whether publication would "wound * * * feelings" or have "mischievous effects." *Gee*, 36 Eng. Rep. at 678; see *Thompson* v. *Stanhope* (1774) 27 Eng. Rep. 476, 477 (Ch.); *Pope*, 26 Eng. Rep. at 608. The purpose of disclosure was "immaterial." *Gee*, 36 Eng. Rep. at 675. Courts presumed that "the plaintiff suffered a *de facto* injury merely from having his personal, legal rights invaded." *Spokeo*, 136 S. Ct. at 1551 (Thomas, J., concurring).

The practice of enjoining disclosure without requiring any "mischievous effect[ ]" is telling. The longstanding rule is that conduct may be enjoined only if it will otherwise cause "irreparable injury." *Weinberger* v. *Romero-Barcelo*, 465 U.S. 305, 312 (1982). For English courts, unauthorized disclosure of a communication *automatically* provided *irreparable harm*. See R. Eden, *A Treatise on the Law of Injunctions* 190, 200-202 (1822).

2. Early American courts agreed, recognizing that "no doctrine" had been "more fully sustained." *Woolsey* v. *Judd*, 11 How. Pr. 49, 55-56 (N.Y. Super. Ct. 1855); see *Grigsby* v. *Breckinridge*, 65 Ky. 480, 485-486 (1867) (collecting authorities). "The earliest case in this country * * * arose in 1811," *Baker* v. *Libbie*, 97 N.E. 109, 110 (Mass. 1912), in the federal territorial court for the Territory of Orleans, which enjoined an attempt to print a letter with "the sole view of disclosing the writer's secrets and wounding his feelings," *Denis* v. *LeClerc*, 1 Mart. 297, 305-306 (Orleans T. Super. Ct. 1811). The court invoked English cases concerning letters published for "pecuniary benefit." *Id.* at 305. The law, it stated, abhors the "disclosure of the contents of a confidential communication"; the writer retains a "property" interest and the right to control disclosure. *Id.* at 299-302, 309-312.

In 1841, Justice Story enjoined the publication of a collection of George Washington's letters. *Folsom*, 9 F. Cas. 342. Absent "a most unequivocal dedication of private letters * * * either to the public, or to some private person," Justice Story explained, a writer retains "property" in their contents. *Id.* at 345-346. If someone attempts to publish letters, "a court of equity will prevent the publication by an injunction, as a breach of private confidence or contract, or of the rights of the author; and a fortiori if he attempt to publish them for profit." *Id.* at 346.

For that reason, by 1855, the New York Superior Court did not hesitate to enjoin the publication of a private letter. *Woolsey*, 11 How. Pr. at 53. The plaintiff did not aver the letter "ha[d] any value" or that publication would cause "any injury." *Ibid.*; see *id.* at 56, 77-78. Agreeing with Justice Story, the court ruled that the "unquestionable and unquestioned law" was that the wri-

ter could "forbid publication" of his communication, his "property," without his consent. *Id.* at 53, 55-56, 64-65. It was thus the court's "duty" to prevent injury to that "exclusive property" by enjoining publication. *Id.* at 57-58. That was consistent with the "general rule" that an injunction "can never" issue but to prevent "irreparable" harm. *Id.* at 54. If a writer is to have "an exclusive right of property," that right must "be protected" by "an injunction." *Id.* at 55.

By the mid-19th century, injunctions issued "upon the ground that the writer has a right of property in his letters, and that they can only be used by the receiver for the purposes for which they were written." *Bartlett* v. *Crittenden*, 2 F. Cas. 967, 970 (C.C.D. Ohio 1849). No further harm had to be shown. Courts "act[ed] alone upon the principle of protecting the rights of property, and not upon the grounds that such publications tend * * * to degrade or injure the author." *Roberts* v. *McKee*, 29 Ga. 161, 163 (1859). Injunctions issued on the "naked" allegation that publication was "made without the consent, and contrary to the wishes of the writer." *Woolsey*, 11 How. Pr. at 53.

3. Treatises agreed. Anti-disclosure injunctions were "founded, not on any notion, that the publication of letters would be painful to the feelings of the writer, but upon a civil right of property, which the Court is bound to respect." 2 J. Story, *Commentaries on Equity Jurisprudence, as Administered in England and America* § 945, at 219 (2d ed. 1839). That also safeguarded "essential" societal interests: If private letters were made the subject of "public display," a person would "write, even to his dearest friends, with the cold and formal severity, with which he would write to his wariest opponents, or his most implacable enemies." *Id.* § 946, at 220-221.

Plaintiffs did not need to show further harm. See Story, *supra*, §§ 945-948, at 219-222. As Eaton Drone explained in 1879, it was "recognized law" that courts would enjoin even a letter's recipient, as well as third parties, from making "any public use of its contents." E. Drone, *Treatise on the Law of Property in Intellectual Productions in Great Britain and the United States Embracing Copyright in Works of Literature and Art, and Playwright in Dramatic and Musical Compositions* 127-128 (1879). Although "[p]ublication" of letters "may cause broken friendship, wounded feelings," etc., it was "well settled" that "the right of the author to restrain unlicensed publication" is based on "the principle of property"—not "considerations of policy or social ethics." *Id.* at 128. "Whatever may be the nature of the letter, its merit, or its value," Drone wrote, "the law gives to the writer the right to determine what use * * * shall be made of its contents." *Id.* at 135.

4. While injunctions were the "usual[]" remedy, T. Cooley, *Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* 358 (1880), other remedies were available without proof of further harm. For example, complainants were entitled to recover the wrongdoer's profits from wrongful disclosure. See Drone, *supra*, at 134. "The right to an account of profits" was "incident to the right to an injunction." *Stevens* v. *Gladding*, 58 (17 How.) U.S. 447, 455 (1855). Justice Story thus ordered "an account of the profits made by the defendants" from publishing President Washington's letters. *Folsom*, 9 F. Cas. at 349. That remedy serves not to compensate the plaintiff for injury, but "to prevent an unjust enrichment." *Sheldon* v. *Metro-Goldwyn Pictures Corp.*, 309 U.S. 390, 399 (1940).

There likewise was "no reasonable doubt" that damages were available for "unauthorized publication." Drone, *supra*, at 132. For intrusion into the exclusive right to publish (or to use an invention), the general rule was that "[e]very violation of a right imports some damage, and if none other be proved, the law allows a nominal damage." *Whittemore* v. *Cutter*, 29 F. Cas. 1120, 1121 (C.C.D. Mass. 1813) (Story, Circuit Justice). Thus, the first Congress authorized the award of a fixed sum for any violation of the copyright statute. Copyright Act of 1790, ch. 15, § 2, 1 Stat. 124, 125. That statutory-damages award afforded "the owner of a copyright some recompense for injury done him, in a case where the rules of law render difficult or impossible proof of damages." *Douglas* v. *Cunningham*, 294 U.S. 207, 209 (1935).

B. Communications Have Long Been Protected as Confidences Without Proof of Further Harm

English courts extended the legal protections afforded to letters to myriad communications—from lectures, to recipes, to etchings, to manuscripts. See, *e.g.*, *Prince Albert* v. *Strange* (1849) 41 Eng. Rep. 1171, 1178 (Ch.) (etching); *Abernethy* v. *Hutchinson* (1825) 47 Eng. Rep. 1313, 1317-1318 (Ch.) (lectures); *Yovatt* v. *Winyard* (1820) 37 Eng. Rep. 425, 426 (Ch.) (medical recipes); *Duke of Queensberry* v. *Shebbeare* (1758) 28 Eng. Rep. 924, 925 (Ch.) (unpublished manuscript). Those decisions rested on the same "property" interest. *Morison* v. *Moat* (1851) 68 Eng. Rep. 492, 498 (Ch.). But they also invoked interests founded on contract, confidence, and trust. See *ibid.*

In 1825, the Court of Chancery ruled that a student who attended a lecture had an "implied contract" or "trust" obligation not to publish his lecture notes for profit. *Abernethy*, 47 Eng. Rep. at 1316-1318. A person

who acquired a customer's etchings through private employment similarly had a "contract" or "trust" obligation not to betray the customer's "confidence" by sharing them. *Prince Albert*, 41 Eng. Rep. at 1178. No inquiry into harm was required: A "breach of trust, confidence, or contract, would of itself entitle the Plaintiff to an injunction." *Ibid.*; see *Morison*, 68 Eng. Rep. at 500-501.

American courts followed that tradition. See, *e.g.*, *Clague* v. *City Bank*, 8 La. 48, 50 (1835) (customer affairs); *Peabody* v. *Norfolk*, 98 Mass. 452, 459-460 (1868) (manufacturing processes); *Corliss* v. *E.W. Walker Co.*, 57 F. 434, 435-436 (C.C.D. Mass. 1893) (painting and photograph). Even *the recipient's* use of a communication, courts observed, "must be deemed strictly limited * * * to the very occasions expressed or implied." *Bartlett*, 2 F. Cas. at 970. Relief was available "in all cases, where the publication would be a violation of a trust or confidence, founded in contract, or implied from circumstances." 2 Story, *supra*, § 949, at 222 (footnote omitted); see 2 J. High, *Treatise on the Law of Injunctions* § 1013, at 650 (2d ed. 1880). "[I]n breach of confidence cases, the harm" occurred "when the plaintiff's trust in the breaching party" was "violated." *Muransky* v. *Godiva Chocolatier, Inc.*, 905 F.3d 1200, 1209 (11th Cir. 2018).

Those decisions have particular force here. Since at least 1758, see *Duke of Queensberry*, 28 Eng. Rep. at 924, it was recognized that even the recipient of a communication was under an implied obligation to use it only for the "very occasions" for which it was sent—not to profit from further disclosure, *Bartlett*, 2 F. Cas. at 970; see *Morison*, 68 Eng. Rep. at 500-501. Here, the SCA imposes that restriction statutorily, obliging providers of "electronic communications service[s]" to keep the "contents of communications" they receive confidential, and

prohibiting disclosure without consent. 18 U.S.C. §2702(a)-(b).

Here, moreover, there was an *express promise* to keep the communications at issue confidential. The Complaint alleges that Google's disclosure of search terms violated its Terms of Service. Those terms recognized that users "retain ownership of any intellectual property rights [they] hold in" their "content"—a term defined "broadly" to include "written text and search queries used on Google.com." App., *infra*, 15a(¶35); see *Carpenter* v. *United States*, 138 S. Ct. 2206, 2242 (2018) (Thomas, J., dissenting) (citing Google's Terms of Service as an example of a contract that makes data users' "property"). Google's Terms of Service, moreover, "expressly incorporate" additional guarantees. App., *infra*, 53a(¶143). Google's Privacy Policy, for example, promises that Google will share "personal information" only in "limited circumstances": with user's "consent," with affiliated companies or trusted businesses, and as required by law. App., *infra*, 8a-9a(¶25); see App., *infra*, 10a-12a(¶29). A separate policy guarantees Google "will not disclose * * * information" about "the web pages you visit," "your search queries," and "the results you click," "except in the limited circumstances" (described above) that do not encompass Google's indiscriminate disclosure of search terms to website operators. App., *infra*, 14a-15a(¶¶32-34). Courts have long held that disclosures in violation of express undertakings of confidentiality are themselves actionable without more. See pp. 10-11, *supra*; cf. *Bd. of Trade* v. *Christie Grain & Stock Co.*, 198 U.S. 236, 250-251 (1905).

C. The Complaint Alleges the Types of Breaches Courts Have Long Redressed

The Complaint alleges precisely the sorts of breaches—unauthorized disclosure of communications—the law has long made actionable without further allegation of harm.

1. The SCA applies the "high level of protection" the law has always afforded "first class mail" to communications through "telecommunications and computer technolog[ies]." S. Rep. No. 99-541, at 1, 5 (1986). The search terms typed into Google's text box are "communications." App., *infra*, 52a (¶136). They express what the user is looking for—reflecting interests, fears, desires, vanities. (Indeed, as leading privacy experts observe, users "tell the Google search box what they wouldn't tell their own mother, spouse, shrink or priest." App., *infra*, 7a (¶23).)

The Complaint alleges that Google, as recipient of those communications, was not free to disclose them without consent, much less do so for profit. App., *infra*, 8a-16a (¶¶25-37). Yet Google disclosed those communications indiscriminately (to the next website clicked), profiting as a result. App., *infra*, 25a-35a (¶¶56-82). Google thereby invaded the same legal interests—users' "property" in their search terms, App., *infra*, 15a (¶35), and express and implied confidentiality, App., *infra*, 53a-56a (¶¶142-158)—long protected by courts.

The Complaint thus alleges the sort of violation—unauthorized disclosure of communications—that has been actionable for centuries without further harm beyond disclosure itself. Courts would issue injunctions on the "naked" allegation a communication would be disclosed, even if no "mischievous effects" would result. See pp. 6-9, *supra*. Here, the Complaint demanded such injunctive relief to "hold[ ] Google to the terms" of its confidentiality

representations. App., *infra*, 58a (¶170). Courts would award the wrongdoer's profits to prevent unjust enrichment. See p. 9, *supra*. The Complaint seeks "revenues and profits wrongfully obtained" from unauthorized disclosures. App., *infra*, 59a; see App., *infra*, 52a-53a (¶¶138, 141). And courts would award damages, including presumed or nominal damages, for unauthorized disclosures. See p. 10, *supra*. The Complaint seeks that relief too. App., *infra*, 53a (¶141), 59a. The SCA authorizes all that relief—damages, wrongdoers' profits, and injunctions. 18 U.S.C. §2707(a)-(c). And the settlement agreement provided it, including prospective relief mandating changes to Google's representations (to ensure users knowingly agree to its conduct), as well as a monetary payment reflecting profits or damages. See Pet. App. 45-50; Resp. Br. 13-14, 48-49.

It is no answer to suggest that some search terms communicated to Google would not result in embarrassment. But see pp. 18-19, *infra*. The unauthorized interception and disclosure of a letter's contents would still violate the writer's right to control her communications, no matter how pedestrian the content. The law remedies unauthorized disclosures, even by a recipient, whether or not a communication "has any value" or disclosure causes "any injury." *Woolsey*, 11 How. Pr. at 53; see pp. 6-9, *supra*. "[I]nquiries after the health of friends" were still "property" subject to the author's exclusive control. *Pope*, 26 Eng. Rep. at 608. The notion that Article III somehow forecloses actions to redress unauthorized disclosures when the communications consist of search terms defies history.

Legal protection against such invasions into communications, property, and privacy pervades our values. Even an officer's lifting of stereo equipment—to see a serial

number—is sufficient to support the assertion of Fourth Amendment rights. See *Arizona* v. *Hicks*, 480 U.S. 321, 323, 326 (1987). Attaching a tracking device to a car or a listening device to a telephone booth, with no physical, pecuniary, or other harm to the individual, supports the assertion of such rights too. See *United States* v. *Jones*, 565 U.S. 400, 404-405, 410 (2012); *Katz* v. *United States*, 389 U.S. 347, 352 (1967). Similar rules apply to "privacy" interests, derived from traditional protections for letters. See *Harper & Row, Publishers, Inc.* v. *Nation Enters.*, 471 U.S. 539, 554 (1985). "Traditionally, the common law has provided" privacy-tort victims "with a claim for 'general' damages, which for privacy and defamation torts are presumed damages: a monetary award calculated without reference to specific harm." *Doe*, 540 U.S. at 621. Article III does not upend that settled approach by requiring physical, pecuniary, or other harm beyond the invasion itself.

2. This Court thus need not inquire whether Congress has attempted to "'define injuries and articulate chains of causation'" to "'give rise to a case or controversy where none existed before.'" *Spokeo*, 136 S. Ct. at 1549. The historical tradition of providing redress for unauthorized disclosure of communications should be "conclusive." *Vt. Agency*, 529 U.S. at 777. Nonetheless, the SCA's scope—while itself *not* a jurisdictional matter, see *Steel Co.* v. *Citizens for a Better Env't*, 523 U.S. 83, 89 (1998)—reflects the "judgment of Congress" that the unauthorized disclosure of electronic communications itself inflicts actionable harm. *Spokeo*, 136 S. Ct. at 1549.

The SCA prohibits "electronic communication service" providers from "knowingly divulg[ing]" the "contents of a communication" they carry or store, 18 U.S.C. §2702(a), except to "intended recipient[s]" or with "lawful consent,"

§2702(b); see §2702(b)-(c) (other exceptions). The SCA thus does not distinguish by *content*. All content is protected, whether sensitive or banal. Nor does the SCA exempt disclosures if the communication's author is obscured. Congress instead cloaked electronic communications with the legal "sanctity and privacy" enjoyed by letters. 132 Cong. Rec. H4045-H4046 (June 23, 1986).

More telling, §2707 authorizes relief—including monetary recoveries—without "actual damages." That is striking. The Privacy Act, at issue in *Doe*, does the opposite. The Privacy Act imposes liability on the government for "actual damages," and guarantees an award of no "less than the sum of $1,000," but *only* for a "'person entitled to recovery.'" 540 U.S. at 619-620 (quoting 5 U.S.C. §552a(g)(4)(A)). The only substantive recovery authorized, however, was "actual damages." *Ibid.* As a result, *Doe* concluded that Congress had guaranteed the $1,000 minimum "only to plaintiffs who have suffered some actual damages"; only they have the "'entitle[ment] to recovery' necessary to qualify." *Id.* at 627.

In the SCA, Congress again guaranteed a $1,000 minimum for "person[s] entitled to recover," but Congress did *not* limit recovery to "actual damages." 18 U.S.C. §2707(c). The SCA permits a court to "assess as damages * * * *the sum* of the actual damages suffered by the plaintiff *and any profits made by the violator* as a result of the violation." *Ibid.* (emphasis added). Plaintiffs are thus entitled to recover the wrongdoer's profits, which requires "no injury" beyond the violation itself. *Gen. Motors Corp.* v. *Devex Corp.*, 461 U.S. 648, 654 (1983); see p. 9, *supra*.[3] And, as persons "entitled to recover,"

[3] "[P]otential gains"—such as entitlement to recover the wrongdoer's profits, see *Gollust* v. *Mendell*, 501 U.S. 115, 121-122, 125-127

such plaintiffs are guaranteed the statutory $1,000 minimum as well. §2707(c); see *Vista Mktg., LLC* v. *Burkett*, 812 F.3d 954, 971 (11th Cir. 2016) (statutory minimum authorized when "plaintiff shows actual damages or a violator's profits"). Congress also authorized injunctive relief. §2707(b). Those remedies parallel the relief that courts afforded for unauthorized disclosures from before the Framing. And they do not require actual damages.[4]

Congress, moreover, authorized any "subscriber or other person aggrieved by a violation" to sue. §2707(a). That expansive language is a "term of art" that encompasses everyone with standing. *Dir., Office of Workers' Comp. Programs* v. *Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 126-127 (1995). That surely encompasses individuals traditionally entitled to sue when their communications were disclosed. Moreover, as originally enacted, the SCA provided a cause of action to any "subscriber" or "customer aggrieved by any violation." §2707(a) (1994). That focus on "subscribers" and "customers" left no doubt that potential plaintiffs included the

---

(1991)—can confer standing. *Pub. Citizen* v. *U.S. Dep't of Justice*, 491 U.S. 440, 451 (1989).

[4] For those reasons, the cases Google invoked at argument—*Vista*, 812 F.3d 954, and *Van Alstyne* v. *Electronic Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009)—do not help its cause. Oral Arg. Tr. 46. They involved persons who were *not entitled* to recovery of any sort, neither damages nor profits. See *Vista*, 812 F.3d at 961-962; *Van Alstyne*, 560 F.3d at 203. Consequently, the SCA did not afford them the statutory minimum either. See *Vista*, 812 F.3d at 964-965; *Van Alstyne*, 560 F.3d at 208. In any event, whether the SCA affords a plaintiff minimum damages is a merits question—not an Article III limitation. See *Steel Co.*, 523 U.S. at 89. An unlawful disclosure of private information can be "enough to open the courthouse door" even if the statute limits remedies. *Doe*, 540 U.S. at 624-625.

communications' senders—those historically aggrieved by wrongful disclosure.

3. Finally, the Complaint alleges that the named plaintiffs' searches created sufficient "risk of real harm." *Spokeo*, 136 S. Ct. at 1549. For example, named plaintiff Anthony Italiano searched for his name, his "soon-to-be ex-wife['s]" name, and "forensic accounting" in a single search, revealing worries and perhaps legal vulnerabilities related to his impending divorce. App., *infra*, 45a (¶¶ 107-108). He "did not want" those "sensitive" searches "disclosed to third parties." App., *infra*, 45a-46a (¶¶ 108, 111). Yet those were disclosed to the next website clicked. App., *infra*, 45a (¶¶ 109-110). Gabriel Privyev searched for "sensitive" information about his "health." App., *infra*, 46a-47a (¶¶ 115, 118).

The Complaint makes clear that disclosed searches now can be routinely reidentified with users. See App., *infra*, 35a-43a (¶¶ 83-98). For example, when AOL released supposedly anonymized search terms, "New York Times journalists were able to reidentify individual 'anonymized' AOL search users" by cross-referencing searches. App., *infra*, 21a (¶ 47). Moreover, "[f]or the vast majority of Google users, the user's IP address is concurrently transmitted along with the search query." App., *infra*, 41a (¶ 95). An IP address, like a "phone number," allows a website operator to "identif[y] the exact computer being used." *Ibid.* As Google observed, "[o]ther parties can often link IP addresses to [users'] identit[ies]," App., *infra*, 41a-42a (¶ 96)—a process enhanced by cookies and other ubiquitous tools for tracking internet users, App., *infra*, 42a-43a (¶¶ 97-98). Google has cited those very privacy risks in refusing to turn over even anonymized search terms to the government. App., *infra*, 17a-20a (¶¶ 41-44).

Those risks are magnified by the increasing ubiquity of data brokers that aggregate enormous quantities of data from myriad websites. App., *infra*, 38a-39a (¶89). The resulting data libraries are so massive as to permit the identification of users by cross-referencing searches and other data, and even the development of data fingerprints. App., *infra* 37a-40a (¶¶86, 88-91). That exposes users to the "Imminent Threat of Concrete and Particularized Privacy Harm." App., *infra*, 2a (¶4), 40a. At the pleading stage, "all reasonable inferences" must be "drawn in favor of the pleader." 5B C. Wright & A. Miller, *Federal Practice and Procedure* §1357 (3d ed.). The Complaint includes sufficient allegations of threatened harm to support Article III jurisdiction.

II. The Four Other Claims Independently Support Jurisdiction

The named plaintiffs also have standing to assert breach-of-contract and quasi-contract causes of action. See *Spokeo*, 136 S. Ct. at 1551 (Thomas, J., concurring). Those claims—for breach of contract (Count II), breach of covenant of good faith and fair dealing (Count III), breach of implied-in-law contract (Count IV), and unjust enrichment (Count V), see App., *infra*, 53a-56a—are claims "'traditionally amenable to, and resolved by, the judicial process,'" *Vt. Agency*, 529 U.S. at 774, even when a breach results in no loss, *Wilcox*, 29 U.S. (4 Pet.) at 181-182. The notion that Article III excludes the traditional grist of judicial resolution defies credulity.

A. Breach of Contract Is Actionable Here

The Complaint asserts a traditional breach-of-contract claim. It alleges that Google's transmittal of referrer headers violated its Terms of Service (either directly or under California's implied covenant of good faith and fair dealing). App., *infra*, 4a (¶11), 53a-55a (¶¶142-152). Goo-

gle's Privacy Policy promises that Google will share "personal information" only in "limited circumstances" not applicable here: with users' "consent," with affiliated companies or trusted businesses, and as required by law. App., *infra*, 8a-9a (¶25); see App., *infra*, 10a-12a (¶29). Google promises it "will not disclose" information about "the web pages you visit," "your search queries," and "the results you click on"—"except in the limited circumstances described in our main Google Privacy Policy, or with your consent." App., *infra*, 14a-15a (¶¶32-34). The Complaint alleges that Google breached those representations by providing "individual search queries * * * and results containing personal information" "to third-parties and advertisers." App., *infra*, 15a-16a (¶36); see App., *infra*, 25a-35a (¶¶56-82).

The traditional rule for breach-of-contract actions was that the breach was a sufficient basis for suit—a rule applied with rigor for express or implied confidences. See pp. 10-11, *supra*. "[T]here having been a breach of * * * contract, the plaintiff is entitled to recover nominal damages." *Marzetti* v. *Williams* (1830) 109 Eng. Rep. 842, 845 (KB). "[A]ny breach is sufficient to entitle the Plaintiff to nominal damages." *Godefroy* v. *Jay* (1831) 131 Eng. Rep. 159, 162 (CP).

Nearly 190 years ago, this Court recognized that contract breaches were actionable, for nominal damages, absent harm beyond the breach itself. *Wilcox*, 29 U.S. (4 Pet.) at 181-182. Early state courts agreed. See, *e.g.*, *Clinton* v. *Mercer*, 7 N.C. 119, 120 (1819); *Jenkins* v. *Hopkins*, 26 Mass. 543, 555 (1830); *Seat* v. *Moreland*, 26 Tenn. 575, 576 (1847). Under "established practice," if a defendant "broke[] his contract" but "no actual injury" was sustained, nominal damages were awarded. 2 T. Parsons, *The Law of Contracts* 493 (1855).

Thus, a "breach of contract always creates a right of action." *Restatement (First) of Contracts* §328 & cmt. a (1932). "If the breach caused no loss * * * , a small sum * * * will be awarded as nominal damages." *Restatement (Second) of Contracts* §346(2) (1981). California so provides by statute. See Cal. Civ. Code §3360. In appropriate cases, disgorgement remedies are available as well. See *Restatement (Third) of Restitution and Unjust Enrichment* §39 (2011); *Snepp* v. *United States*, 444 U.S. 507, 515-516 (1980) (per curiam) (disgorgement remedy for breach placing "sensitive information at risk"). The breach-of-contract allegations alone support standing.

B. Quasi-Contract Claims Likewise Support Jurisdiction

The named plaintiffs likewise have standing to pursue claims for breach of implied contract and unjust enrichment. App., *infra*, 55a-56a(¶¶153-163). Those counts allege a contract implied at law, App., *infra*, 56a(¶157), and seek the "revenues and profits" Google made from "peddling" users' "search terms or results," App., *infra*, 55a-56a(¶¶156, 163). Quasi-contract claims for profits arising from the unauthorized disclosure of communications have ancient roots. See p. 9, *supra*. Such claims for "unjust enrichment" were "not contingent on a plaintiff's allegation of damages beyond the violation of his private legal right." *Spokeo*, 136 S. Ct. at 1551 (Thomas, J., concurring).

The cases are legion. See, *e.g.*, *Gollust* v. *Mendell*, 501 U.S. 115, 121-122, 125-127 (1991); *Mosser* v. *Darrow*, 341 U.S. 267, 272-274 (1951); *Gen. Motors*, 461 U.S. at 654; *Jackson* v. *Smith*, 254 U.S. 586, 588-589 (1921). Where the plaintiff's rights are violated, unjust enrichment entitles him to sue to recover the wrongdoer's gains. He may do so even if he "has not suffered a corresponding

loss"—or indeed "any loss" at all. *Restatement (First) of Restitution* § 1 cmt. e (1937); see 1 G. Palmer, *The Law of Restitution* § 2.10, at 133 (1978). Even nominal damages can be awarded. See Cal. Civ. Code § 3360. For those actions, too, plaintiffs have standing.

III. The Complaint Establishes Jurisdiction Over The Settlement

The allegations of the Complaint thus establish historically recognized and constitutionally sufficient injuries-in-fact from the unauthorized disclosures for each of the named plaintiffs.[5] Causation-in-fact is not disputed. See *Lujan*, 504 U.S. at 560. And the Complaint leaves no doubt the injuries would "be redressed by the requested relief." *Allen* v. *Wright*, 468 U.S. 737, 751 (1984). The Complaint prays for precisely the remedies—injunctive relief, an award of the wrongdoer's profits, and damages (as well as statutory sums)—courts have awarded for the wrongful disclosure of communications for centuries. See pp. 6-11, *supra*.

That is "enough to open the courthouse door." *Doe*, 540 U.S. at 625. With power to hear at least one claim for one named representative under Article III, the district court had jurisdiction to review and approve the parties' settlement—the terms of their contractual compromise—as well. See *Rufo* v. *Inmates of Suffolk Cty. Jail*, 502 U.S. 367, 389 (1992); *Local No. 93, Int'l Ass'n of Firefighters* v. *City of Cleveland*, 478 U.S. 501, 525 (1986).

---

[5] Jurisdiction exists so long as at least one class representative has standing. See Fed. R. Civ. P. 23(a) ("[o]ne or more members of a class may sue or be sued as representative parties"); see also *Horne* v. *Flores*, 557 U.S. 433, 446 (2009); *Sosna* v. *Iowa*, 419 U.S. 393, 400-403 (1975).

CONCLUSION

To the extent the Court addresses standing, rather than remanding or dismissing, the Court should find standing sufficiently alleged.

Respectfully submitted.

KASSRA P. NASSIRI
Counsel of Record
NASSIRI & JUNG LLP
47 Kearny St.
Suite 700
San Francisco, CA 94108
(415) 762-3100
kass@njfirm.com

MICHAEL ASCHENBRENER
KAMBERLAW, LLC
201 Milwaukee St.
Suite 200
Denver, CO 80206
(303) 222-0281
masch@kamberlaw.com

JEFFREY A. LAMKEN
MICHAEL G. PATTILLO, JR.
JAMES A. BARTA
WILLIAM J. COOPER
MOLOLAMKEN LLP
The Watergate, Suite 660
600 New Hampshire Ave., N.W.
Washington, D.C. 20037
(202) 556-2000
jlamken@mololamken.com

JORDAN A. RICE
MOLOLAMKEN LLP
300 N. LaSalle St.
Chicago, IL 60654
(312) 450-6700

Counsel for Class Respondents

NOVEMBER 2018

APPENDIX

APPENDIX A
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

Case No. 5:10-cv-04809-EJD

In re GOOGLE REFERRER
HEADER PRIVACY LITIGATION

This Document Relates To: All Actions

April 26, 2013

CONSOLIDATED COMPLAINT
CLASS ACTION
JURY TRIAL DEMANDED

Plaintiffs Paloma Gaos, Anthony Italiano, and Gabriel Priyev (collectively "Plaintiffs") bring this suit on behalf of themselves and all others similarly situated, and make the following allegations on information and belief, except as to allegations pertaining to Plaintiffs, which are based on their personal knowledge:

INTRODUCTION

1. Plaintiffs bring this class action complaint against Google Inc. ("Google") for storing and intentionally, systematically and repeatedly divulging its users' search queries and histories to third parties via "Referrer

Headers." This practice adversely impacts billions of searches conducted by millions of consumers.

2. Google, the largest search engine in the United States, has repeatedly touted the numerous ways in which it protects user privacy, particularly with regard to the terms that consumers search for using the company's search engine. Over protests from privacy advocates, however, Google has consistently and intentionally designed its services to ensure that user search queries, which often contain highly-sensitive and personally-identifiable information ("PII"), are routinely transferred to marketers, data brokers, and sold and resold to countless other third parties.

3. The user search queries disclosed to third parties contain, without limitation, users' real names, street addresses, phone numbers, credit card numbers, social security numbers, financial account numbers and more, all of which increases the risk of identity theft. User search queries also contain highly-personal and sensitive issues, such as confidential medical information, racial or ethnic origins, political or religious beliefs or sexuality, which are often tied to the user's personal information.

4. In many instances, the information contained in disclosed search queries does not directly identify the Google user. Through the reidentification (explained below) or deanonymizing of data, however, the information contained in search queries can and, on information and belief, are associated with the actual names of Google users. Computer science academics and privacy experts are calling for the reexamination of privacy concerns in light of the growing practice and power of reidentification.

5. Google has acknowledged that search query information alone may reveal sensitive PII. And Google

has demonstrated that it could easily stop disclosing search query information to third parties, without disrupting the effectiveness of its service to its users, if it wished to do so. But because the real-time transmission of user search queries increases Google's profitability, it chooses not to utilize the demonstrated technology that would prevent the disclosure of its users' PII.

6. Moreover, in October 2011, Google confirmed that it is, in effect, selling individual user search queries to advertisers. In October 2011, Google started proactively scrubbing user search queries from the information it passes on to third parties when some users click on regular, organic search results, but would continue sending search queries to third parties when all users click on paid listings. While this is, in a way, a small win for privacy advocates, it also demonstrates just how valuable the search queries are to Google and others: Google no longer gives away this precious data for free, but will do so when it gets paid for it.

PARTIES

7. Plaintiff Paloma Gaos is a resident of San Francisco County, California. Plaintiff has at all material times been a user of Google's search engine services.

8. Plaintiff Anthony Italiano is a resident of Pasco County, Florida. Plaintiff has at all material times been a registered Google Accounts user and a user of Google's search engine services.

9. Plaintiff Gabriel Priyev is an individual and a citizen of the State of Illinois. Plaintiff has at all material times been a registered Google Accounts user and a user of Google's search engine services, at different times in California and Illinois.

10. Defendant Google Inc. ("Google") is a Delaware corporation that maintains its headquarters in Mountain View, Santa Clara County, California. Google conducts business throughout California and the nation from California. Google makes and implements all relevant decisions, including those at issue in this case, in California. Its Terms of Service and Privacy Policy were decided on and implemented in California.

JURISDICTION AND VENUE

11. This Court has personal jurisdiction over Google because (a) a substantial portion of the wrongdoing alleged in this complaint took place in this state, (b) Google is authorized to do business here, has sufficient minimum contacts with this state, and/or otherwise intentionally avails itself of the markets in this state through the promotion, marketing and sale of products and services in this state, and (c) in its Terms of Service, to which all Google Account holders who use Google Search, including Plaintiffs, must purportedly assent, Google consents to the personal jurisdiction of this Court:

> The laws of California, U.S.A., excluding California's conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services. All claims arising out of or relating to these terms or the Services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1331, 18 U.S.C. §2702 and 18 U.S.C. §2707. This Court has supplemental jurisdiction over the California state law claims pursuant to 28 U.S.C. §1367.

13. Venue is proper in this District under 28 U.S.C. § 1391(b) and (c). A substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred in this District.

INTRADISTRICT ASSIGNMENT

14. Pursuant to Civil Local Rule 3-2(e), this case shall be assigned to the San Jose Division.

STATEMENT OF FACTS

A. Google's Dominance in Search

15. "Searching" is one of the most basic activities performed in the Internet. Most everyone with access to the Internet uses search engines to find information on the Internet. When using a search engine, users formulate a search query using keywords and phrases reflecting the information sought by the user. The search engine then matches the search query with websites matching the query and provides a list of those matching websites to the user. The user clicks on the link in the resulting list and is redirected to the website containing the sought-after information.

16. Google's core service centers on its proprietary search engine. Google runs millions of servers in data centers around the world and processes over one billions user-generated search requests every day. On information and belief, Google is the most-used search engine in the world and enjoys a market share of over 50% in the United States.

17. Google generates substantial profits from selling advertising. The revenue it generates is derived from offering search technology and from the related sale of advertising displayed on its site and on other sites across the web. On information and belief, nearly 95% of Google's revenue is derived from its advertising pro-

grams, with total advertising revenues estimated at $28 billion in 2010, $36.5 billion in 2011, and $43.7 billion in 2012. Google has implemented various innovations in the online advertising market that helped make it one of the biggest advertising platforms in the world.

18. Google AdWords is Google's main advertising product and source of advertising revenue. The AdWords program allows advertisers to select a list of words that, when entered by users in a search query, trigger their targeted ads. When a user includes words that match an advertiser's selections within a search query, paid advertisements are shown as "sponsored links" on the right side of the search results screen. Accordingly, much of Google's advertising revenue depends directly on the search queries that its users run on Google search.

19. Using technology from its wholly-owned subsidiary DoubleClick, Google can also determine user interests and target advertisements so they are relevant to their context and the user that is viewing them. Google's Analytics product allows website owners to track where and how people use their website, allowing in-depth research to get users to go where you want them to go.

20. Third-party search engine optimization ("SEO") companies help businesses design their websites so that users conducting internet search using search engines like Google get search results containing their business at or near the top of the search results page. SEOs accomplish this task by ensuring that a business's relevant pages are designed to work with Google's search algorithms. Google has a symbiotic relationship with SEOs. Google wants relevant results at the top of their search results page, and SEOs want their customers' relevant webpages to appear at the top of Google's search results. To the extent that SEOs are successful in getting their

clients' relevant pages to appear at or near the top of Google's search results page, users are more likely to return to Google next time they want to search for information on the internet. And the more people use Google for search, the more revenue Google derives from its advertising business.

21. Google Web History is a free service Google provides to users of Google Search. A user's search queries, search results and/or Referrer Headers form a substantial part of what Google's Terms of Service identify or define as the user's "Web History," which Google stores for users by default.

22. Google Analytics is a free service Google provides to those who manage websites. Analytics allows website managers to see detailed search query and search results reports including user Web History information or search terms. Such information provides valuable business intelligence to third-party website owners, particularly those who buy advertising on Google.com or with Google Adwords.

B. Google's Privacy Promises

23. Leading thinkers in the privacy community have long argued that consumers "treat the search [engine] box like their most trusted advisors. They tell the Google search box what they wouldn't tell their own mother, spouse, shrink or priest."[1] Peer reviewed academic studies confirm this fact, particularly regarding the use of search engines to look up sensitive health information.[2]

---

[1] Christopher Ketchum & Travis Kelly, The Cloud Panopticon (April 9, 2010), http://www.theinvestigativefund.org/investigations/rights liberties/1274/the_cloud_panopticon (last visited October 24, 2010).

[2] Gunther Eysenbach and Christian Köhler, How do consumers search for and appraise health information on the world wide web?

24. Google has always recognized that user trust is paramount to its search business success. To that end, Google adopted "Don't be evil" as its motto, and Google states that its Code of Conduct is one of the ways it puts that motto into practice.[3] Google's Code of Conduct recognizes that it is "asking users to trust [it] with their personal information. Preserving that trust requires that each of us respect and protect the privacy of that information. Our security procedures strictly limit access to and use of users' personal information."[4]

25. Because Google's success depends on gaining the trust of its users, Google's Privacy Policy sets forth representations intended to foster the safety and privacy protection offered by Google's search services. As of October 14, 2005, Google's Privacy Policy[5] stated as follows:

> Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:
>
> - We have your consent. We require opt-in consent for the sharing of any sensitive personal information.
> - We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require

---

Qualitative study using focus groups, usability tests, and in-depth interviews, BMJ 2002; 324:573, available at http://www.bmj.com/cgi/content/full/324/7337/573.

[3] Google's Code of Conduct, http://investor.google.com/corporate/code-of-conduct.html (last visited April 26, 2012).

[4] *Id.*

[5] Google's October 14, 2005 Privacy Policy, http://www.google.com/intl/en/privacy_archive_2005.html (last visited April 26, 2012).

that these parties agree to process such information based on our instructions and in compliance with this Policy and any other appropriate confidentiality and security measures.

- We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law.

26. In October 2010, Google defined in its Privacy Center FAQ "Personal information" as "information that [the user] provide[s] to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google" and "Sensitive Information" as "information we know to be related to confidential medical information, racial or ethnic origins, political or religious beliefs or sexuality and tied to personal information. As of April 2012, Google no longer defines "Personal Information" at all in its Privacy Center FAQ.

27. Google also stated in its October 14, 2005 Privacy Policy that "We may share with third parties certain pieces of *aggregated, non-personal information*, such as the number of users who searched for a particular term, for example, or how many users clicked on a particular advertisement. Such information does not identify you

individually."[6] Google defined "aggregated, non-personal information" as "information that is recorded about users and *collected into groups* so that it no longer reflects or references an individually identifiable user."[7]

28. Google's privacy policy was unchanged until October 3, 2010, when it was revised to exclude any statement about how Google shares search queries with third parties. The representations that Google shares information only in "limited circumstances" remained unchanged.

29. On March 1, 2012, Google implemented a new, singular privacy policy for all Google products.[8] While the new policy has broad implications for how Google shares user data internally, Google makes the following representations regarding how it shares data with third parties:[9]

> **Information we share**
>
> We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances apply:
>
> - **With your consent**
>
> We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We

---

[6] Google's October 14, 2005 Privacy Policy, *supra*, n.5 (emphasis supplied).

[7] Google's October 14, 2005 Privacy FAQs, http://web.archive.org/web/20070113102317/www.google.com/intl/en/privacy_faq.html (last visited October 24, 2010) (emphasis supplied).

[8] http://www.google.com/intl/en/policies/privacy/ (last visited April 26, 2012).

[9] *Id.*

require opt-in consent for the sharing of any sensitive personal information.

- **With domain administrators**

  If your Google Account is managed for you by a domain administrator (for example, for Google Apps users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

  - view statistics regarding your account, like statistics regarding applications you install.
  - change your account password.
  - suspend or terminate your account access.
  - access or retain information stored as part of your account.
  - receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
  - restrict your ability to delete or edit information or privacy settings.

  Please refer to your domain administrator's privacy policy for more information.

- **For external processing**

  We provide personal information to our affiliates or 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 legal reasons**

  We will share personal information with companies, organizations or individuals 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.
  - 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 aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

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

30. Google makes similar representations about the privacy of its users' search queries on its video "Privacy Channel" on YouTube. In October 2010, Google showcased a video on its Privacy Channel that starts with the statement "at Google, we make privacy a priority in eve-

rything we do."[10] Google also stated in another privacy video from 2010 that "We don't sell user information to other companies."[11] In a 2011 video on its Privacy Channel called "What is a search log?," Google explains that it keeps logs of user search queries for a short period of time, but does not disclose that it shares those search logs with any third parties.[12]

31. In 2010, Google reiterated its commitment to user privacy to the Federal Trade Commission. In a letter to the FTC, Google wrote that it "supports the passage of a comprehensive federal privacy law that . . . build[s] consumer trust . . . enact[s] penalties to deter bad behavior . . . include[s] uniform data safeguarding standards, data breach notification procedures, and stronger procedural protections relating to third party access to individuals' information."[13] Google also wrote that it "acts every day to promote and expand free expression online and increase global access to information. As new technology empowers individuals with more robust free expression tools and greater access to information, we believe that governments, companies, and individuals must work together to protect the right to online free expression.

---

[10] Google's Privacy Principles, http://www.youtube.com/watch?v=5fvL3mNt1g (January 26, 2010) (last visited October 25, 2010) (not available as of April 26, 2012).

[11] Google's Privacy Principles, http://googleblog.blogspot.com/2010/01/googlesprivacyprinciples.html at 1:44 (January 27, 2010, 7:00 p.m.) (last visited October 23, 2010) (not available as of April 26, 2012).

[12] http://www.youtube.com/watch?v=PIdfBUm0CPo&list=UUsB_OLJA28Nc-47BihG2_Ww&index=6&feature=plcp (October 18, 2011) (last visited April 26, 2012).

[13] Google's April 14, 2010 letter to Donald S. Clark, http://www.scribd.com/doc/30196432/FTCRoundtable-Comments-Final (last visited October 24, 2010).

Strong privacy protections must be crafted with attention to the critical role privacy plays in free expression. The ability to access information anonymously or pseudonymously online has enabled people around the world to view and create controversial content without fear of censorship or retribution by repressive regimes or disapproving neighbors . . . If all online behavior were traced to an authenticated identity, the free expression afforded by anonymous web surfing would be jeopardized."[14]

32. At all relevant times, Google has maintained a separate privacy policy for Web History (the "Web History Privacy Policy").

33. Google defines "Web History" and "Personal Information" as follows:

> WEB HISTORY
>
> Personal Information
>
> Web History records information about the web pages you visit and your activity on Google, including your search queries, the results you click on, and the date and time of your searches in order to improve your search experience and display your web activity. Over time, the service may also use additional information about your activity on Google or other information you provide us in order to deliver a more personalized experience.

34. Google has promised that it will use Web History solely for the benefit of the user or with the user's consent. Google promised to Plaintiffs and the Class at relevant times:

> Web History uses the information from your web history or other information you provide us to im-

---

[14] *Id.*

> prove your Google search experience, such as improving the quality of your search results and providing recommendations. In addition to enabling the Web History functionality, the information we collect when you use Web History may be shared among all of our services in order to provide you with a seamless experience and to improve the quality of our services. We will not disclose this information to other companies or individuals, except in the limited circumstances described in our main Google Privacy Policy, or with your consent.

35. At relevant times Google's Terms of Service expressly provided that information entered by a user on Google.com, including Plaintiffs' and other Class members' search terms, remain the property of the user: "Google acknowledges and agrees that it obtains no right, title or interest from you (or your licensors) under these Terms in or to any Content that you submit, post, transmit or display on, or through, the Services"[15] Currently, Google's Terms of Service expressly state: "Some of our Services allow you to submit content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours."[16] "Content" is broadly defined and includes and is clearly meant to include written text and search queries used on Google.com.

36. Google's conduct has breached the above-described privacy promises. Contrary to these terms, Google has provided individual search queries, non-aggregated search queries, search queries and results

---

[15] http://www.google.com/accounts/TOS (as of November 19, 2010).

[16] http://www.google.com/accounts/TOS (last viewed on March 29, 2013).

containing personal information, Web History including "search queries" or search terms and "results," and Referrer Headers, to third-parties and advertisers, including via Google Analytics, and not for the benefit of the user experience (*i.e.*, not "to provide you with a seamless experience and to improve the quality of our services" as Google's terms have promised). Rather, Google's conduct was designed to enhance Google's profit and position by peddling user Web History and search queries to third-party website owners via Google Analytics reports, in order to market and expand its Google AdWords advertising services for Google's financial gain.

37. In addition, because Web History and search queries or results constitute and/or contain "personal information," Google's provision of such information through Google Analytics breaches its Privacy Policy. Google agreed to share personal information only in the following limited circumstances, none of which applies here: (1) with user consent – opt-in consent is required; (2) to Google "subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on [Google's] behalf"; and (3) as reasonably necessary to follow applicable law and the like.

38. Additionally, though Google compiles Web History by default, Google has represented that users can "choose to stop storing [their] web activity in Web History either temporarily or permanently" and delete or turn off their Web History:

> [D]eleting web history from your Google Account will erase all items from your web history and stop your web history from being recorded in the future.

> You can also remove individual items without deleting all of your web history.[17]

39. Such terms convey that when Web History is deleted, Google no longer holds onto it or uses it, but rather, "erases," "deletes" and "removes" it from its records.

40. Upon information and belief, in violation of these promises, Google continues to store in its files, and transmit to third-parties via Referrer Headers or Google Analytics, Web Histories even after a user has deleted or turned it off.

C. Google Admits Search Queries Contain Sensitive, Personal Data

41. In 2006, the Department of Justice sought to compel Google to produce thousands of users' individual search queries.[18] As set forth in the Government's subpoena, it sought only "anonymized" data, namely, the text of the search string entered by Google users, and not "any additional information that may be associated with such a text string that would identify the person who entered the text string into the search engine, or the computer from which the text string was entered."[19]

42. To its credit, Google fought the government's request. In a declaration submitted to the court describing the kind of personal information that can end up in the

---

[17] *E.g.*, http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=54067. See also http://www.google.com/intl/en/privacypolicy.html; http://www.google.com/history/privacyfaq.html?hl=en ("[i]f you remove items [from your Web History], they will be removed from the service . . . .").

[18] *Gonzales* v. *Google*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW).

[19] *Id.* at 682.

company's search query logs, Matt Cutts, a Senior Staff Engineer who specializes in search optimization issues at Google, stated as follows:[20]

- Google does not publicly disclose the searches [sic] queries entered into its search engine. If users believe that the text of their search queries could become public knowledge, they may be less likely to use the search engine for fear of disclosure of their sensitive or private searches for information or websites.
- There are ways in which a search query alone may reveal personally identifying information. For example, many internet users have experienced the mistake of trying to copy-and-paste text into the search query box, only to find that they have pasted something that they did not intended. Because Google allows very long queries, it is possible that a user may paste a fragment of an email or a document that would tie the query to a specific person. Users could also enter information such as a credit card, a social security number, an unlisted phone number or some other information that can only be tied to one person. Some people search for their credit card or social security number deliberately in order to check for identity theft or to see if any of their personal information is findable on the Web.

43. Similarly, in its Opposition to the Government's Motion to Compel the disclosure of Google users' search queries, the company argued that:

---

[20] Declaration of Matt Cutts at 9, *Gonzales* v. *Google*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW).

- Google users trust that when they enter a search query into a Google search box, not only will they receive back the most relevant results, but that Google will keep private whatever information users communicate absent a compelling reason.[21]
- The privacy and anonymity of the service are major factors in the attraction of users – that is, users trust Google to do right by their personal information and to provide them with the best search results. If users believe that the text of their search queries into Google's search engine may become public knowledge, it only logically follows that they will be less likely to use the service.[22]
- This is no minor fear because search query content can disclose identities and personally identifiable information such as user-initiated searches for their own social security or credit card numbers, or their mistakenly pasted but revealing text."[23]

44. In its order[24] denying the Government's request to discover Google users' search queries, the Court shared Google's concern that disclosing search queries would raise serious privacy issues:

> The Government contends that there are no privacy issues raised by its request for the text of search queries because the mere text of the queries would

---

[21] Google's Opposition to the Government's Motion to Compel at 1, *supra*, n.12.

[22] *Id.* at 18.

[23] *Id.*

[24] *Gonzales*, 234 F.R.D. at 687.

> not yield identifiable information. Although the Government has only requested the text strings entered . . . basic identifiable information may be found in the text strings when users search for personal information such as their social security numbers or credit card numbers through Google in order to determine whether such information is available on the Internet. The Court is also aware of so-called 'vanity searches,' where a user queries his or her own name perhaps with other information. Google's capacity to handle long complex search strings may prompt users to engage in such searches on Google. Thus, while a user's search query reading '[username] stanford glee club' may not raise serious privacy concerns, a user's search for '[user name] third trimester abortion san jose,' may raise certain privacy issues as of yet unaddressed by the parties' papers. This concern, combined with the prevalence of Internet searches for sexually explicit material—generally not information that anyone wishes to reveal publicly—gives this Court pause as to whether the search queries themselves may constitute potentially sensitive information.

45. Google's awareness of the privacy concerns surrounding search queries was also demonstrated in response to a massive disclosure of user search queries by AOL. In August 2006, AOL released an "anonymized" dataset of 20 million search queries conducted by 658,000 AOL users over a three-month period.[25] That data included search queries revealing names, addresses, local

---

[25] Complaint at ¶ 16, *Doe 1* v. *AOL LLC*, 2010 WL 2524494 (N.D. Cal. June 23, 2010) (No. C-06-5866-SBA).

landmarks, medical ailments, credit card numbers and social security numbers.[26]

46. In an article about the incident, the New York Times wrote that the AOL dataset "underscored how much people unintentionally reveal about themselves when they use search engines," and referred to search queries about "depression and medical leave," "fear that spouse contemplates cheating," "child porno," and "how to kill oneself by natural gas."[27]

47. Even more surprising, however, was that the New York Times journalists were able to reidentify individual "anonymized" AOL search users due to the vanity searches they had conducted, and then link other, non-vanity search queries in the dataset to those individuals through the crosssession identifiers (cookies) included in the dataset.[28] One AOL user who was reidentified said she was shocked to learn that AOL had published her search queries: "My goodness, it's my whole personal life. I had no idea somebody was looking over my shoulder."[29]

48. An AOL spokesman, Andrew Weinstein, apologized on behalf of AOL and said he wasn't surprised that the New York Times was able to connect the dots and reidentify "anonymous" users in the dataset: "We acknowledged that there was information that could potentially lead to people being identified . . . "[30]

---

[26] *Id.* at ¶ 18.

[27] Michael Barbaro and Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times, August 9, 2006, available at http://www.nytimes.com/2006/08/09/technology/09aol.html.

[28] *Id.*

[29] *Id.*

[30] *Id.*

49. Soon after the release of the search query data by AOL, Google CEO Eric Schmidt spoke about the AOL privacy breach. He called AOL's release of user search data "a terrible thing" and reassured Google users that their search queries were safe and private:

> Well, [this sort of privacy breach is] obviously a terrible thing. And the data as released was obviously not anonymized enough, and maybe it wasn't such a good idea to release it in the first place. Speaking for Google, we exist by virtue of the trust of our end users. So if we were to make a mistake to release private information that could be used against somebody, especially if it could be used against them in a way that could really hurt them in a physical way or something like that, it would be a terrible thing. We have lots and lots of systems in the company to prevent that.
>
> It's funny that we talk about the company being more transparent. But there are many things inside our company that are important that we don't share with everyone, starting with everyone's queries and all the information that that implies. I've always worried that the query stream was a fertile ground for governments to randomly snoop on people [for example]. We had a case where we were only a secondary party, where the government gave us a subpoena, which was in our view, over-broad. And this over-broad subpoena we fought in federal court – one of the great things about the American system is that you can actually have a judge make an impartial decision. And the judge ruled largely

in our favor. So that's an example of how strongly we take this point.[31]

D. A Brief Primer on "Referrer Headers"

50. Software engineers are generally familiar with the risk of Referrer Header "leakage" of information companies intended to keep confidential and/or are obliged to keep confidential.

51. The HTTP Referrer function is a standard web browser function, provided by standard web browsers since the HTTP 1.0 specification in May 1996.[32] When an internet user visits a web page using their computer or mobile device, every major web browser (*e.g.*, Internet Explorer, Firefox, Chrome, Safari) by default reports the last page that the user viewed before clicking on a link and visiting the current page — that is, the page that "referred" them to the current page. This information is transmitted in the HTTP Referrer Header.

52. The current version of the publicly-available HTTP specification, RFC 2616,[33] provides for HTTP Referrer Headers in its provision 14.36.[34] It is well known that if a site places confidential information, such as a username, in a URL, then the site risks releasing this information whenever a user clicks a link to leave the site. Indeed, the HTTP specification specifically flags this risk; in section 15.1.3, the HTTP specification advises developers of substantially the same problem: "Authors of services which use the HTTP protocol SHOULD NOT

---

[31] Conversation with Eric Schmidt hosted by Danny Sullivan, http://www.google.com/press/podium/ses2006.html (last visited April 26, 2012).

[32] http://www.w3.org/Protocols/rfc1945/rfc1945

[33] http://www.w3.org/Protocols/rfc2616/rfc2616.html

[34] http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.36

use GET based forms for the submission of sensitive data, because this will cause this data to be encoded in the REQUESTURI."[35]

53. While the HTTP Referrer function is a standard web browser function, Google ultimately determines whether to send referrer header information to third parties and exercises control over the content of the URL that is referred by this function to the owner of the destination web page.

54. Google's use and provision of Referrer Headers for third-party advertising (and without filtering or deleting user information) appears to go well beyond the intended use of this function pursuant to the internet community Hypertext Transfer Protocol. See internet community Hypertext Transfer Protocol—HTTP /1.1, http://tools.ietf.org/html/rfc2616.

55. The Protocol indicates that Referrer information is for the server's benefit to provide service: in the words of the Hypertext Transfer Protocol for internet functions, "The Referrer request-header allows a server to generate lists of back-links to resources for interest, logging, optimized caching, etc. It also allows obsolete or mistyped links to be traced for maintenance." *Id.* at 14.36. Referrer headers have also been used to provide browsing security. According to the industry Protocol, contrary to Google's practice, "Because the source of a link might be private information or might reveal an otherwise private information source, it is strongly recommended that the user be able to select whether or not the Referrer field is sent." *Id.* at 15.1.3.

---

[35] http://www.w3.org/Protocols/rfc2616/rfc2616-sec15.html#sec15.1.3

E. Google Transmits Individual User Search Queries to Third Parties

56. Since the service's launch, and continuing to this day, Google's search engine has included its users' search terms in the URL of the search results page. Thus, for example, a search for "abortion clinics in Indianapolis" would return a page with a URL similar to http://www.google.com/search?q=abortion+clinics+in+Indianapolis.

57. Because the search terms are included in the search results URL, when a Google user clicks on a link from Google's search results page, the owner of the website that the user clicks on will receive from Google the user's search terms in the Referrer Header.

58. Several web analytics services, including SEOs, include and use functionality to automatically parse the search query information from web server logs, or to otherwise collect the search query from the referrer header transmitted by each visitor's web browser. Google's own analytics products provide webmasters with this information at an aggregate level (*e.g.*, revealing how many visitors were drawn by particular search terms).

59. By transmitting user search queries to third parties, Google is also violating its Web History-specific privacy promises as described above.

F. Google's Transmission of User Search Queries is Intentional

60. Because Google's financial success depends on, among other things, the symbiotic relationship it shares with SEOs and the ability for third parties to engage in web analytics, Google has placed a high priority on revealing individual user search queries to third parties. Notwithstanding its repeated representations to the con-

trary in its Privacy Policy and to privacy regulators, Google continues to this day to transmit user search queries.

61. Neither Google's search technology nor the nature of the Internet compels Google to divulge user search queries. Google could easily cease transmission of user search queries to third parties, but chooses not to.

62. On September 6, 2010, a former FTC employee, Christopher Soghoian, filed a complaint with the FTC accusing Google of not adequately protecting the privacy of consumers' search queries. Much of the following information comes from Mr. Soghoian's complaint.[36]

63. Starting approximately in November 2008, Google began to test a new method of delivering search results that uses advanced AJAX (Asynchronous JavaScript and XML) technologies.[37] AJAX is one of the key pillars of the Web 2.0 experience.[38] This pilot was initially deployed in the Netherlands,[39] but in subsequent months, was observed by users in other countries.

---

[36] *In the Matter of Google, Inc.*, FTC Complaint, available at http://online.wsj.com/public/resources/documents/FTCcomplaint100710.pdf.

[37] Jesse James Garrett, *Ajax: A New Approach to Web Applications* (February 18, 2005), http://www.adaptivepath.com/ideas/essays/archives/000385.php ("Ajax isn't a technology. It's really several technologies, each flourishing in its own right, coming together in powerful new ways").

[38] Tim O'Reilly, *What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software* (September 30, 2005), http://oreilly.com/web2/archive/what-is-web-20.html ("AJAX is also a key component of Web 2.0 applications such as Flickr, now part of Yahoo!, 37signals' applications basecamp and backpack, as well as other Google applications such as Gmail and Orkut.")

[39] Ulco, "Google Search in AJAX?!" (November 19, 2008), http://www.ulco.nl/gibberish/googlesearch-in-ajax.

64. One of the side effects of the AJAX search page is that the URL of the search results page includes the search query terms after a # symbol in the URL. Thus, on an AJAX enabled search page, the URL listed at the top of the page will be similar to: http://www.google.com/#hl=en&source=hp&q=drug+addiction

65. The addition of the # symbol had a significantly positive, albeit unintentional impact upon Google user privacy. This is because web browsers do not pass on any information after the # symbol in the referrer header. Thus, using the previous example of a search for the query "drug addiction," if a user clicked on the first result, the owner of that web site would only receive "http://www.google.com/" in the referrer header, rather than the search terms that follow the # symbol.

66. This change was immediately noticed by the webmaster and SEO community, who complained to Google:

- "I'm seeing hundreds of these empty google referrers today and wondered what was going on."[40]
- "This means organic searches from Google will now show up as just http://www.google.com/, with no search parameters. In other words, no analytics app can track these searches anymore. I started noticing lots of hits from just 'http://www.google.
  com/' recently in our own search logs. I thought maybe it was just a bug with Clicky. But then one of our users contacted me about this article,

[40] Posting of sorabji.com to Clicky.blog, http://getclicky.com/blog/150/googles-new-ajaxpoweredsearch-results-breaks-search-keyword-tracking-for-everyone (February 03 2009, 1:05 p.m.).

and my jaw about broke from hitting the floor so hard."[41]

- "What actually breaks if Google makes this switchover, and is in fact broken during any testing they are doing, is much more widespread. Every single analytics package that currently exists, at least as far as being able to track what keywords were searched on to find your site in Google, would no longer function correctly."[42]

67. Responding to complaints from the webmaster community, Google quickly issued a public statement:

> Currently AJAX results are just a test on Google. At this time only a small percentage of users will see this experiment. It is not our intention to disrupt referrer tracking, and we are continuing to iterate on this project and are actively working towards a solution. As we continue experiments, we hope that this test may ultimately provide an easier solution for our customers and a faster experience for our users.[43]

---

[41] Clicky.blog, http://getclicky.com/blog/150/googles-new-ajax-poweredsearch-resultsbreakssearch-keyword-tracking-for-everyone (February 03, 2009, 9:50 a.m.).

[42] Posting of Michael VanDeMar to Smackdown!, What Will *Really* Break If Google Switches To AJAX . . . ?, http://smackdown.blogs blogsblogs.com/2009/02/02/what-will-reallybreak-if-googleswitches-to-ajax/ (February 2, 2009, 11:26 a.m.).

[43] Posting of Matt McGee to Search Engine Land, Google AJAX Search Results = Death To Search Term Tracking?, http://searchengineland.com/google-ajax-search-results-death-to-search-termtracking-16431 (February 3, 2009, 5:41 p.m.) (emphasis supplied).

68. Google soon ended the test of the AJAX search results page, a fact confirmed by Google Senior Engineer Matt Cutts, who specializes in search optimization issues at Google:

> [T]he team didn't think about the referrer aspect. So they stopped [the test]. They've paused it until they can find out how to keep the referrers.[44]

69. In March 2009, Google again began to test technology that unintentionally caused the users' search terms to be stripped from the referrer header transmitted to web sites. The following is an example of the format of the new URL that was being tested in March 2009:

> http://www.google.com/url?q=http://www.webmd.com&ei=in66ScnjBtKgtwfn0LTiDw&sa=X&oi=smap&resnum=1&ct=result&cd=1&usg=AFQjCNF9RdVC6vXBFOYvdia1s_ZE_BMu8g

70. Michael VanDeMar, a prominent member of the SEO community noticed that he was again seeing AJAX based search results in addition to redirected URLs for every link in the search results page:

> Occasionally you will see these Google redirects in the normal [search engine results pages] as well, although usually not. The thing is, I was seeing them on every search I performed. It struck me as odd, until I suddenly realized that every search was being done via AJAX.[45]

---

[44] Posting of Lisa Barone to Outspoken Media, Keynote Address – Matt Cutts, Google, http://outspokenmedia.com/internet-marketing-conferences/pubcon-keynote-matt-cutts/ (March 12, 2009).

[45] Posting of Michael VanDeMar to Smackdown!, Google Re-initiates Testing of AJAX SERP's With Faulty Proposed Fix, http://smack

71. Google's Matt Cutts soon responded to VanDeMar by leaving a comment on his blog:

> Hi Michael, I checked with some folks at Google about this. The redirection through a url redirector was separate from any AJAX-enhanced search results; we do that url redirection for some experiments, but it's not related to the JavaScript-enhanced [AJAX] search results.
>
> **The solution to the referrer problem will be coming online in the future. It uses a JavaScript-driven redirect that enables us to pass the redirect URL as the referrer. This URL will contain a 'q' param that matches the user's query.**[46]

72. On April 14, 2009, Google announced that it would be deploying the URL redirection tool for all links in the search results. The company described the details in a blog post to the webmaster community:

> Starting this week, you may start seeing a new referring URL format for visitors coming from Google search result pages. Up to now, the usual referrer for clicks on search results for the term "flowers", for example, would be something like this:
>
> http://www.google.com/search?hl=en&q=flowers&btnG=Google+Search
>
> Now you will start seeing some referrer strings that look like this:

---

down.blogsblogsblogs.com/2009/03/13/google-re-initiates-testing-of-ajax-serps-with-faulty-proposed-fix/ (March 13, 2009, 11:14 a.m.).

[46] Posting of Matt Cutts to Smackdown!, *supra*, n.39, http://smackdown.blogsblogsblogs.com/2009/03/13/google-re-initiates-testing-of-ajax-serps-withfaulty-proposed-fix/ (March 17, 2009, 10:10 a.m.) (emphasis added).

> http://www.google.com/url?sa=t&source=web&ct=res&cd=7&url=http%3A%2F%2F**www.example.com**%2Fmypage.htm&ei=OSjdSa-1N508M_qW8dQN&rct=j&q=**flowers**&usg=AFQjCNHJXSUh7Vw7oubPA03tZOzz-F-u_w&sig2=X8uCFh6IoPtnwmvGMULQfw
>
> . . . .
>
> The new referrer URLs will initially only occur in a small percentage of searches. You should expect to see old and new forms of the URLs as this change gradually rolls out.[47]

73. The redirection tool that Michael VanDeMar described in March 2009 did not include the search terms in its URL (and thus, these terms were not subsequently transmitted to webmasters via the browser's referrer header). However, one month later when Google announced that it would be using the redirection tool for all links, the redirection script was changed to include the search terms in the redirection URL (via a new "q" parameter), thus guaranteeing that webmasters would not lose access to user search query data.

74. The new redirection tool also leaks data to web site administrators that had never before been available to anyone but Google: The item number of the search result that was clicked non (*e.g.*, the 3rd link or 5th link from the search results page).[48] The leakage of this addi-

---

[47] Posting of Brett Crosby to Google Analytics Blog, An upcoming change to Google.com search referrals; Google Analytics unaffected, http://analytics.blogspot.com/2009/04/upcoming-change-togooglecom-search.html (April 14, 2009, 2:50 p.m.).

[48] Posting of Patrick Altoft to Blogstorm, Google Ads Ranking Data to Referrer String, http://www.blogstorm.co.uk/google-adds-ranking-data-to-referrer-string/ (April 15, 2009).

tional information was confirmed by Matt Cutts, which he described as a benefit to web site administrators:

> I think if you do experiments, you'll be able to confirm your speculation . . . **I think this is awesome for webmasters—even more information than you could glean from the previous referrer string.**[49]

75. A May 2009 video featuring Matt Cutts, posted to the official GoogleWebmasterHelp YouTube channel, describes the change in the search query information leaked via the referrer header:

> [T]here is a change on the horizon and it's only a very small percentage of users right now, but I think that it probably will grow and it will grow over time where Google's referrer, that is whenever you do a Google search and you click on a result, you go to another website and your browser passes along a value called a referrer. That referrer string will change a little bit.
>
> It used to be google.com/search, for example.
>
> Now, it will be google.com/url.
>
> **And for a short time we didn't have what the query was which got a lot of people frustrated**, but the google.com/search, **the new Google referrer string will have the query embedded in it.**
>
> And there's a really interesting tidbit that not everybody knows, which is--it also has embedded in

[49] Posting of Matt Cutts to Blogstorm, Google Ads Ranking Data to Referrer String, http://www.blogstorm.co.uk/google-adds-ranking-data-to-referrerstring/#IDComment77457344 (April 15, 2009, 7:28 p.m.) (emphasis added).

> that referrer string a pretty good idea of where on the page the click happened.
>
> So, for example, if you were result number one, there's a parameter in there that indicates the click came from result number one. If you were number four, it will indicate the click came from, result number four. So, now, you don't necessarily need to go scraping Google to find out what your rankings were for these queries. You can find out, "Oh, yeah. I was number one for this query whenever someone clicked on it and came to my website."
>
> So that can save you a ton of work, you don't need to worry nearly as much, you don't have to scrape Google, you don't have to think about ranking reports. Now, we don't promise that these will, you know, be a feature that we guarantee that we'll always have on Google forever but definitely take advantage of it for now.
>
> . . . .
>
> [F]or the most part, this gives you a very accurate idea of where on the page you were, so you get all kinds of extra information that you can use in your analytics and to compute your ROIs without having to do a lot of extra work. So, if you can, it's a good idea to look at that referrer string and start to take advantage of that information."[50]

76. In or around July 2010, Google again began stripping the search terms from the Referrer Headers transmitted by a small percentage of browsers. On July 13, 2010, individuals in the SEO community noticed the

---

[50] Matt Cutts, Can you talk about the change in Google's referrer string?, GoogleWebMasterHelp Channel (May 6, 2009), http://www.youtube.com/watch?v=4XoD4XyahVw (last viewed October 24, 2010).

change made by Google. One commentator in a web forum wrote that:

> More and more visits from Google in my server log files are without exact referrer information, and have only 'http://www.google.com', 'http://www.google.com.au', etc. which doesn't allow to find out keyword and SERP [search engine results] page from which this visit was made.[51]

77. On July 13 2010, Matt Cutts posted a message to the same SEO forum:

> Hey everybody, I asked folks who would know about this. It turns out there was an issue a couple weeks ago where some code got refactored, and the refactoring affected referrers for links opened in a new tab or window. Right now the team is **expecting to have a fix out in the next week** or so. Hope that helps.[52]

78. On or about May 21, 2010, Google introduced an encrypted search service at https://www.google.com.[53] By using the encrypted search service, Google would no longer pass along search queries via Referrer Headers to unencrypted search links. On or about June 25, 2010, Google moved the encrypted search service to https://encrypted.google.com.

79. Later, on or about October 18, 2011, Google announced a change in policy for how it handled search

---

[51] Posting of at2000 to Webmaster World, More and more referrals from Google are without exact referrer string, http://www.webmasterworld.com/google/4168949.htm (July 13, 2010, 4:01 a.m.).

[52] Posting of Matt Cutts to Webmaster World, *supra*, n.45 (July 13, 2010, 9:46 p.m.) (emphasis added).

[53] http://googleblog.blogspot.com/2010/05/search-more-securely-with-encrypted.html (last visited April 26, 2012).

queries embedded in Referrer Headers.[54] According to its new policy, Google would proactively scrub out any and all search queries from all searches performed by users who were logged in to any Google service, such as Google Docs, before sending the Referrer Headers to the sites in the results on which users would click. Thus, when logged-in users would click on a search result link (whether the results link is encrypted or unencrypted), Google would no longer pass on the search queries used to find those results.

80. For users not logged in, Google would still transmit search queries via Referrer Headers to the results sites on which users would click, unless those users entered the search at https://encrypted.google.com.

81. Moreover, the new policy only applies to organic sites. For clicks on paid links or advertisements, Google would still pass on the search queries.

82. If nothing else, Google's new policy regarding search queries demonstrates two things: 1) Google is fully capable of determining independently whether to transmit search queries to third parties—transmitting search queries embedded within Referrer Headers is not just how the Internet works; and, 2) Google is now effectively selling search queries to paying advertisers. Stated differently, part of what paying advertisers pay for when they buy AdWords are the search queries users enter.

G. The Science of Reidentification

83. "Reidentification" is a relatively new area of study in the computer science field. Paul Ohm, a professor of law and telecommunications at the University of Colora-

---

[54] http://googleblog.blogspot.com/2011/10/making-search-more-secure.html (last visited April 26, 2012).

do Law School, is a leading scholar on how reidentification impacts internet privacy. Much of the following information comes from Professor Ohm's article entitled "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymizaton" published in the UCLA Law Review in August of 2010.[55]

84. In a nutshell, reidentification creates and amplifies privacy harms by connecting the dots of "anonymous" data and tracing it back to a specific individual. Professor Ohm describes it as follows:

> The reverse of anonymization is reidentification or deanonymization. A person, known in the scientific literature as an adversary, reidentifies anonymous data by linking anonymized records to outside information, hoping to discover the true identity of the data subjects.
>
> . . .
>
> Reidentification combines datasets that were meant to be kept apart, and in doing so, gains power through accretion. Every successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification. Accretive reidentification makes all of our secrets fundamentally easier to discover and reveal.[56]

85. Reidentification techniques, like those used in the AOL debacle, can be used as links in chains of inference connecting individuals to harmful facts. Reidentification works by discovery pockets of surprising uniqueness in aggregated data sets. Just as human fingerprints can uniquely identify a single person and link that person

---

[55] 57 UCLA L. Rev. 1701 (2010).

[56] *Id.* at *7-8.

with "anonymous" information—a print left at a crime scene—so too do data subjects generate "data fingerprints"—combinations of values of data shared by nobody else. What has surprised researchers is that data fingerprints can be found in pools of non-PII data, such as the uniqueness of a person's search queries in the AOL debacle.[57]

86. Once a person finds a unique data fingerprint, he can link that data to outside information, sometimes called auxiliary information. "Anonymous" search query information would protect privacy, if only the adversary knew nothing else about people in the world. In reality, however, the world is awash in data about people, with new databases created, bought and sold every day. "Adversaries" (as defined above) combine anonymized data with outside information to pry out obscured identities.[58]

87. And the amount of information contained in new databases has grown exponentially. What's more, the type of available data is increasingly personal and specific. Take, for example, the phenomenon of Facebook's growth. The data created by Facebook users is highly personal, and includes actual names, religious, sexual and political preferences, identification of friends, pictures, messages intended to be shared with friends, and more. With the exploding popularity of social network sites like Facebook, and personal blogs, the information available to adversaries is not only highly-specific to individuals, it is often user-created, increasing accuracy and veracity of available data. Never before in human history has it been so easy to peer into the private diaries of so many

---

[57] *Id.* at *17.

[58] *Id.*

people. Some researchers call this the "age of self-revelation."[59]

88. Reidentification is characterized by accretion, or the growing together of separate parts into a single whole. As Professor Ohm explains:

> The accretion problem is this: once an adversary has linked two anonymized databases together, he can add the newly linked data to his collection of outside information and use it to help unlock other anonymized databases. Success breeds further success . . . ***once any piece of data has been linked to a person's real identity, any association between this data and a virtual identify breaks the anonymity of the latter. This is why we should worry even about reidentification events that seem to expose only non-sensitive information, because they increase the linkability of data, and thereby expose people to potential future harm.***[60]

89. The accretive reidentification problem is exacerbated by the growing prevalence of internet "data brokers." The buying and selling of consumer data is a multibillion-dollar, unregulated business that's growing larger by the day.[61] Data is increasingly bought, sold and resold by data brokers, which amplifies the accretion problem. Advancements in computer science, data storage and processing power, and data accretion by data brokers make it much more likely that an adversary

---

[59] *Id.* at *17-18.

[60] *Id.* at *29 (emphasis added).

[61] Rick Whiting, *Data Brokers Draw Increased Scrutiny* (July 10, 2006), http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=190301136.

could link at least one fact to any individual and blackmail, discriminate against, harass, or steal the identity of that person.

90. On October 25, 2010, the Wall Street Journal reported that a highly-sophisticated data broker, RapLeaf Inc. is accomplishing accretive reidentification of "anonymous" data with astonishing success.[62] According to the report, RapLeaf has been gathering data, including user names and email addresses, from numerous sources across the internet. Using accretive reidentification techniques, RapLeaf is able to cross-index "anonymous" data with email addresses and thereby associate real names with Web-browsing habits and highly-personal information scraped from social network sites such as Facebook. By 2009, RapLeaf had indexed more than 600 million unique email addresses, and was adding more at a rate of 35 million per month.

91. Data gathered and sold by data brokers like RapLeaf can be very specific. RapLeaf deanonymizes and connects to real names a wide variety of data types, including data regarding demographics, interests, politics, lifestyle, finances, donations, social networks, site memberships, purchases, and shopping habits. RapLeaf's segments recently included a person's household income range, age range, political leaning, and gender and age of children in the household, as well as interests in topics including religion, the Bible, gambling, tobacco, adult entertainment and "get rich quick" offers. In all, RapLeaf segmented people into more than 400 categories. This aggregated and deeply personal information is

---

[62] Emily Steele, *A Web Pioneer Profiles Users by Name* (October 25, 2010), available at http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

then sold to or used by tracking companies or advertisers to rack users across the Internet.

H. Google's Systematic Disclosure of Billions of User Search Queries Each Day Presents an Imminent Threat of Concrete and Particularized Privacy Harm

92. One type of anonymization practice is called "release-and-forget," in which the data administrator will release records, and then forgets, meaning she makes no attempt to track what happens to the records after release.[63] To protect the privacy of the users in the released data, prior to releasing the data, the administrator will single out identifying information and either strip that information from the database, or modify it to make it more general and less specific to any individual.[64] Many of the recent advances in the science of reidentification target release-and-forget anonymization in particular.[65]

93. Google's transmission of search queries is a type of piecemeal "release-and-forget" anonymization.[66] Google transmits a single user search query each time a Google user clicks on a link in Google's search results page. Over the course of just one day, on information and belief, Google transmits millions of search queries to third parties. Google will likely argue that search query information alone contains no personally-identifiable information. Such an argument is practically equivalent to the data administrator who "anonymizes" data before releasing it to the outside world. But, as repeatedly

---

[63] Ohm, *supra*, n.47 at *9-10.

[64] *Id.* at *11-12.

[65] *Id.* at *10.

[66] *Id.* at *9.

demonstrated, easy reidentification of "anonymous" highlights the flaws in this thinking.

94. Google itself has taken the position that even seemingly benign, "anonymous" information presents serious privacy concerns. For example, in *Gonzales* v. *Google*, *supra*, n.12, even though the Government was requesting search queries stripped of any "identifying information" (such as the user's IP address), Google argued that releasing such data would nonetheless risk disclosure of user identities.

95. In fact, when a Google user clicks on a link in Google's search results page, the user's search query is not the only information revealed. For the vast majority of Google users, the user's IP address is concurrently transmitted along with the search query. An IP address is similar to a phone number in that it identifies the exact computer being used by the user to search and navigate the internet.

96. In response to an inquiry from Congressman Joe Barton about privacy issues surrounding Google's acquisition of DoubleClick, Google admitted that "information that can be combined with readily available information to identify a specific individual is also generally considered personal information."[67] But Google has repeatedly downplayed the existence of "readily available information" helpful for tying IP addresses to places and individuals. Professor Ohm highlights Google's untenable position as follows:

---

[67] Letter from Alan Davidson, Google's Senior Policy Counsel and Head of U.S. Public Policy, to Congressman Joe Barton at 12-13 (December 21, 2007), available at http://searchengineland.com/pdfs/071222-barton.pdf.

> For example, websites like Google never store IP addresses devoid of context; instead, they store them connected to identity or behavior. Google probably knows from its log files, for example, that an IP address was used to access a particular email or calendar account, edit a particular word processing document, or send particular search queries to its search engine. By analyzing the connections woven throughout this mass of information, Google can draw some very accurate conclusions about the person linked to any particular IP address.
>
> Other parties can often link IP addresses to identity as well. Cable and telephone companies maintain databases that associate IP addresses directly to names, addresses, and credit card numbers. That Google does not store these data associations on its own servers is hardly the point. Otherwise, national ID numbers in the hands of private parties would not be "personal data" because only the government can authoritatively map these numbers to identities.[68]

97. Similarly, an independent European advisory body on data protection and privacy found that "The correlation of customer behaviour across different personalised services of a search engine provider . . . can also be accomplished by other means, based on cookies or other distinguishing characteristics, such as individual IP addresses."[69]

---

[68] Ohm, *supra*, n.47 at *41.

[69] Article 29 Data Protection Working Party at 21 (January 2008), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

98. Congressman Barton's inquiry in connection with the DoubleClick acquisition also focused on cookies and privacy. Cookies are small data files that store user preferences and other information, and allow websites to recognize the user or computer visiting their site. In its response to Congressman Barton, Google wrote that "online ad-serving technology can be used by advertisers to serve and manage ads across the web . . . the ad server sets a cookie on the user's computer browser when the user views an ad served through the ad server. That cookie may be read in the future when the ad server serves other ads to the same browser."[70] An ad serving company with any substantial market share would thus be able to readily link the search queries that Google provides to the IP addresses or cookies of internet users visiting the websites they serve.

I. Google Accounts

99. In addition to search, Google operates many services that require users to register for Google Accounts. Google Accounts grant access to services such as Gmail, Google Docs, and Google+, among others.

FACTS RELATING TO PLAINTIFFS

A. Paloma Gaos

100. Plaintiff Paloma Gaos has a Google Account and has at all material times been a user of Google's search engine services, including the period prior to November 2008 when Google first began to test advanced AJAX technologies that temporarily eliminated user search queries from referrer headers coming from Google search results pages, and for all periods thereafter when Google was disseminating search queries to third party websites.

---

[70] Letter from Davidson to Barton, *supra*, n.58 at 15.

101. During all time periods in which Google was transmitting user search queries to third parties, Plaintiff Gaos conducted numerous searches, including "vanity searches" for her actual name and the names of her family members, and clicked on links on her Google search results pages.

102. As a result, Google transmitted Plaintiff Gaos's full search queries to third parties by sending the URLs containing her search queries to third party websites that appeared in Plaintiff Gaos's Google search results page and which Plaintiff Gaos clicked on a link.

103. In other words, when Plaintiff Gaos clicked on each link on her Google search results pages, the owner of the destination website that Plaintiff clicked on received from Google Plaintiff Gaos's search terms through the Referral Header function.

104. As a result, Plaintiff Gaos has suffered actual harm in the form of Google's unauthorized and unlawful dissemination of Plaintiff Gaos's search queries, which sometimes contained sensitive personal information, to third parties.

B. Anthony Italiano

105. Plaintiff Anthony Italiano has at all material times been a user of Google's search engine services, including the period prior to November 2008 when Google first began to test advanced AJAX technologies that temporarily eliminated user search queries from referrer headers coming from Google search results pages, and for all periods thereafter when Google was disseminating search queries to third party websites.

106. Plaintiff Italiano has also had a Google Account since at least January 2008.

107. During all time periods in which Google was transmitting user search queries to third parties, including the time period from July 2010 to August 2011, Plaintiff Italiano conducted numerous searches on Google's unencrypted search service, including:

a. His name + his home address;
b. His name + bankruptcy;
c. His name + foreclosure proceedings;
d. His name + short sale proceedings;
e. His name + Facebook; and,
f. His name + the name of his then soon-to-be ex-wife + forensic accounting.

108. These searches and the timeframe during which he conducted them are particularly memorable to Plaintiff Italiano because it was during this time that he was going through formal divorce proceedings. Moreover, many of his searches related directly or indirectly to his divorce proceedings—exactly the sort of personal, confidential searches that he did not want disclosed to third parties without his knowledge or consent, and exactly the sort of personal, confidential searches Google described to the federal government in the *Gonzales* matter.

109. As a result, Google transmitted Plaintiff Italiano's full search queries to third parties by sending the URLs containing his search queries to third party websites that appeared in Plaintiff Italiano's Google search results page and which Plaintiff Italiano clicked on a link.

110. In other words, when Plaintiff Italiano clicked on each link on his Google search results pages, the owner of the destination website that Plaintiff clicked on received from Google Plaintiff Italiano's search terms through the Referral Header function.

111. As a result, Plaintiff Italiano has suffered actual harm in the form of Google's unauthorized and unlawful

dissemination of Plaintiff Italiano's search queries, which sometimes contained sensitive personal information, to third parties.

C. Gabriel Priyev

112. Plaintiff Gabriel Priyev has at all material times been a user of Google's search engine services, including the period prior to November 2008 when Google first began to test advanced AJAX technologies that temporarily eliminated user search queries from referrer headers coming from Google search results pages, and for all periods thereafter when Google was disseminating search queries to third party websites.

113. Plaintiff Priyev began using Google search in the fall of 2005, while living in California. Plaintiff Priyev's Web History, kept by Google, reinforces this fact, stretching all the way back to September 2006. Plaintiff Priyev has continued to search using Google in both California, from the Fall of 2005 through the Spring of 2008, and then in Illinois from the Spring of 2008 until the present.

114. Priyev has also had a Google Account at all relevant times.

115. During all time periods in which Google was transmitting user search queries to third parties, Plaintiff Priyev conducted numerous searches, including searches for financial and health information, and clicked on links on his Google search results pages.

116. As a result, Google transmitted Plaintiff Priyev's full search queries to third parties by sending the URLs containing his search queries to third party websites that appeared in Plaintiff Priyev's Google search results page and which Plaintiff Priyev clicked on a link.

117. In other words, when Plaintiff Priyev clicked on each link on his Google search results pages, the owner of the destination website that Plaintiff clicked on received from Google Plaintiff Priyev's search terms through the Referral Header function.

118. As a result, Plaintiff Priyev has suffered actual harm in the form of Google's unauthorized and unlawful dissemination of Plaintiff Priyev's search queries, which sometimes contained sensitive personal information, to third parties.

CLASS ALLEGATIONS

119. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring these claims on behalf of themselves as individuals and all other similarly situated persons in the following class:

> *All persons in the United States who submitted a search query to Google at any time between October 25, 2006 and the date of notice to the class of certification* (the "Class"). Excluded from the Class are Google, its officers and directors, legal representatives, successors or assigns, any entity in which Google has or had a controlling interest, any judge before whom this case is assigned and the judge's immediate family.

120. The Class is composed of numerous people, whose joinder in this action would be impracticable. The disposition of their claims through this class action will benefit Class members, the parties and the courts. Upon information and belief, Google's search engine has been used by hundreds of millions of users during the relevant time period.

121. There is a well-defined community of interest in questions of law and fact affecting the Class. These ques-

tions of law and fact predominate over individual questions affecting individual Class members, including, but not limited to, the following:

a. whether and to what extent Google has disclosed its users' search queries to third parties, and whether the disclosure is ongoing;
b. whether Google continues to use or store information that is part of Web History after users choose to delete, remove or to no longer store with Google such information;
c. whether Google's conduct described herein violates Google's Terms of Service, Privacy Policy, Web History policy and representations to Plaintiffs and the Class;
d. whether Google's conduct described herein violates the Electronic Communications Privacy Act, 18 U.S.C. § 2702 *et seq.*;
e. whether Google's conduct described herein constitutes a breach of contract or implied contract;
f. whether Google's conduct breached its duty of good faith and fair dealing;
g. whether Google is unjustly enriched as a result of its conduct described herein; and
h. whether Plaintiffs and members of the Class are entitled to injunctive and other equitable relief.

122. Google has engaged, and continues to engage, in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs and the Class. Similar or identical statutory and common law violations, business practices and injuries are involved. Individual questions, if any, pale by comparison to the numerous common questions that dominate.

123. The injuries, actual and imminent, sustained by Plaintiffs and the Class flow, in each instance, from a common nucleus of operative facts. In each case, Google caused or permitted unauthorized communications of private and personally-identifying information to be delivered to third parties without adequate or any notice, consent or opportunity to opt out.

124. Given the similar nature of the Class members' claims and the absence of material differences in the statutes and common laws upon which the Class members' claims are based, a nationwide class action will be easily managed by the Court and the parties.

125. Because of the relatively small size of the individual Class members' claims, no Class user could afford to seek legal redress on an individual basis.

126. Plaintiffs' claims are typical of those of the Class as all members of the Class are similarly affected by Google's uniform and actionable conduct as alleged herein.

127. Google has acted and failed to act on grounds generally applicable to Plaintiffs and members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class.

128. Plaintiffs will fairly and adequately protect the interests of the Class, and have retained counsel competent and experienced in class action litigation. Plaintiffs have no interests antagonistic to, or in conflict with, the Class that Plaintiffs seek to represent.

129. Plaintiffs reserve the right to revise the above class definition as appropriate or based on facts learned in discovery.

COUNT I

Violation of the SCA, 18 U.S.C. § 2702
(on behalf of all Plaintiffs individually and the Class)

130. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

131. The Electronic Communications Privacy Act (the "ECPA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . " 18 U.S.C. § 2510(12).

132. The ECPA also broadly defines the contents of a communication. Pursuant to the ECPA, "contents" of a communication, when used with respect to any wire, oral, or electronic communications, include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). "Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication. The definition thus includes all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. The privacy of the communication to be protected is intended to be comprehensive.

133. Pursuant to the ECPA, "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A).

134. Pursuant to the ECPA, Google operates an "electronic communications service" as defined in 18 U.S.C. §2510(15). Pursuant to the Stored Communications Act of 1986 (the "SCA"), Google also provides a "remote computing service" to the public. 18 U.S.C. §2711(2).

135. In relevant part, 18 U.S.C. §2702(a) of the ECPA provides as follows:

> (a) **Prohibitions**.— Except as provided in subsection (b) or (c)—
>
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

> (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

136. As alleged herein, by disclosing the private search queries and Web History information of Plaintiffs and members of the Class without authorization, Google has knowingly divulged the contents of communications of Plaintiffs and members of the Class while those communications were in electronic storage on its service, in violation of 18 U.S.C. § 2702(a)(1).

137. As alleged herein, by disclosing the private search queries and Web History information of Plaintiffs and members of the Class without authorization, Google has knowingly divulged the contents of communications of Plaintiffs and members of the Class carried or maintained on its systems, in violation of 18 U.S.C. § 2702(a)(2).

138. Google intentionally disclosed its users' communications to third parties to enhance its profitability and revenue. The disclosures were not necessary for the operation of Google's systems or to protect Google's rights or property.

139. As a result of Google's unauthorized and unlawful disclosure of Plaintiffs' and the Class members' private search queries and Web History information, Plaintiffs and members of the Class have suffered damages from Google's violations of 18 U.S.C. § 2702 in an amount to be determined at trial.

140. Plaintiffs and Class members are "person[s] aggrieved by [a] violation of [the SCA] in which the conduct constituting the violation is engaged in with a knowing or intentional state or mind . . . " within the meaning of 18 U.S.C. §2707(a).

141. Plaintiff and members of the Class therefore seek remedy as provided for by 18 U.S.C. §2707(b) and (c), including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and attorneys' fees and other litigation costs reasonably incurred.

COUNT II

Breach of Contract

(on behalf of all Plaintiffs individually and the Class)

142. Plaintiffs incorporate by reference the foregoing allegations.

143. The provisions of Google's Terms of Service, which expressly incorporate its Privacy Policy, and Web History Privacy Policy constitute a valid and enforceable contract between Plaintiffs and the Class on the one hand, and Google on the other.

144. Under the Terms of Service, Web History Privacy Policy and Privacy Policy, Plaintiffs and the Class agreed to use Defendant's services and transmit sensitive personally-identifiable information to Google in exchange for Google's promise that it would not share that personal information with third parties without users' authorization.

145. Google materially breached the terms of its Terms of Service, Web History Privacy Policy and Privacy Policy through its unlawful conduct alleged herein, including the disclosure of Plaintiffs and the Class's private

search queries and Web History information to third parties, as more fully set forth above.

146. Google's conduct also violates principles of equity and justice, which prohibit Google from retaining the above-described benefits.

147. As a result of Google's misconduct and breaches of Google's Terms of Service, Web History Privacy Policy and Privacy Policy described herein, Plaintiffs and the Class suffered injury. Plaintiffs, on behalf of themselves and the Class, seek damages and/or restitution from Google in an amount to be determined at trial.

COUNT III

Breach of Covenant of Good Faith and Fair Dealing (on behalf of all Plaintiffs individually and the Class)

148. Plaintiffs incorporate by reference the foregoing allegations.

149. At all times, Google owed Plaintiffs and the Class a duty of good faith and fair dealing.

150. Google delivered search services, and maintained Web History, pursuant to contract, whereby Plaintiffs and other Class members' Web History, Personal Information, search queries, and Referrer Headers were to be stored and used only according to Google's published terms, which promise that their information is private, and is their property, as set forth more fully above.

151. Google abused its discretion as described above for its own benefit, and to the detriment of the property rights and expectations of Plaintiffs and the Class. Google's conduct breached its duty of good faith and fair dealing to Plaintiffs and the Class and damaged Plaintiffs and the Class.

152. Google was unjustly enriched by its aforementioned conduct and Plaintiffs and the Class are entitled to restitution. Google should account for revenues and profits it improperly collected from its transmission of Referrer Headers and Web History information, including from increased Google AdWords business, and should have a constructive trust imposed with respect to such monies until further order of the Court.

COUNT IV

Breach of Contract Implied in Law
(on behalf of all Plaintiffs individually and the Class)

153. Plaintiffs incorporate by reference the foregoing allegations.

154. Google has knowingly, voluntarily and willfully received and retained benefits by sharing Plaintiffs' and other Class members' Web History, Personal Information and search queries or results via Referrer Headers and/or Google Analytics, as set forth above, under circumstances that would render it unjust to allow Google to retain such benefits.

155. The benefits received by Google from sharing Plaintiffs and other Class members' Web History, Personal Information and search queries via Referrer Headers and/or Google Analytics were related to the obligation and duty of Google to use such information only as outlined in the Google's Web History Privacy Policy which does not include dissemination to third parties and in Google's other above-described terms of use, and/or as prescribed by applicable law.

156. Google has increased its revenues and profits by peddling Plaintiffs' and the Class members' Personal Information, Web History, Referral Headers, or search terms or results without notice or their consent.

157. Google's above-described conduct violates principles of equity and justice, which prohibits Google from retaining these above-described benefits and constitutes a breach of contract implied in law.

158. As a result, Plaintiffs and other Class members are entitled to disgorgement and restitution of Google's revenues, profits and/or monies received by Google due to Google's use of Plaintiffs' and other Class members' property *i.e.*, their search terms and results.

COUNT V

Unjust Enrichment (In the Alternative)
(on behalf of all Plaintiffs individually and the Class)

159. Plaintiffs incorporate by reference the foregoing allegations.

160. Plaintiffs and members of the Class have conferred a benefit upon Google. Google has received and retained valuable information belonging to Plaintiffs and members of the Class, and as a result of sharing its users' search queries with third parties without their consent, Google has improved the quality of its search engine and enjoyed increased revenues from advertisers.

161. Google appreciates or has knowledge of said benefit.

162. Under principles of equity and good conscience, Google should not be permitted to retain the benefits that it unjustly received as a result of its actions.

163. Plaintiffs, on their own behalf and on behalf of the Class, seek the imposition of a constructive trust on and restitution of the proceeds of Google received as a result of its conduct described herein, as well as attorney's fees and costs pursuant to Cal. Civ. Proc. Code § 1021.5.

COUNT VI

Declaratory Judgment and Corresponding Injunctive Relief

28 U.S.C. §§ 2201, 2202

(on behalf of all Plaintiffs individually and the Class)

164. Plaintiffs incorporate by reference the foregoing allegations.

165. Google has violated applicable law as more fully set forth above.

166. Plaintiffs and the Class are entitled to a declaration of their rights in connection with what Google can and cannot do with their Web History and search queries.

167. Plaintiffs and the Class and Google have adverse legal interests, and there is a substantial controversy between Plaintiffs and the Class, and Google, to warrant the issuance of a declaratory judgment as to whether Google violated applicable law by its above-described practice of sharing Plaintiffs' and other Class members' Referrer Headers, and whether Google is entitled to share the Web Histories of Plaintiffs and the Class with third-parties for its commercial gain, in violation of its preexisting contract and terms of use.

168. Absent injunctive relief, Google is likely to continue its above-described practices, as Google is endowed with all of the discretion to do as it wishes with Plaintiffs' and the Class members' information.

169. As a result of Google's above-described conduct in violation of applicable law, Plaintiffs and the Class are entitled to corresponding injunctive relief, and an order establishing a constructive trust, for the benefit of Plaintiffs and the Class, consisting of monies received by Google from its unlawful sharing of Plaintiffs' and the

Class's search queries with third-party persons and entities.

170. Google's new Terms of Use do not directly address preexisting Web History, changes to Web History, or the issues described above leaving Plaintiffs and the Class without any indication of what Google intends to do with the Web Histories belonging to Plaintiffs and the Class creating a need for injunctive relief holding Google to the terms of previous contract with and terms of use for Plaintiffs and the Class described in detail above.

171. As a result of Google's above-described conduct in violation of applicable law, Plaintiffs and the Class are also entitled to an order requiring Google not to use or store preexisting Web History for purposes of profiting by transmitting their information to third-parties.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, pray that the Court provide the following relief:

A. Certify this case as a class action on behalf of the Class, as defined above, appoint Plaintiffs Gaos, Italiano, and Priyev as representatives of the Class, and appoint their counsel as counsel for the Class, pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Declare that Google's actions, as described herein, violate the Stored Communications Act (18 U.S.C. § 2702 *et seq.*), constitute Breach of Express and Implied Contracts, and unjust enrichment;

C. Award injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including, *inter alia*, an order declaring the rights of the parties as stated above and prohibiting Google

from engaging in the wrongful and unlawful acts described herein;

D. Award damages, including statutory damages where applicable, to Plaintiffs and the Class, in an amount to be determined at trial;

E. Award all economic, monetary, actual, consequential, and compensatory damages caused by Google's conduct, and if its conduct is proved willful, awarding Plaintiffs and the Class exemplary damages;

F. Award restitution against Google for all money to which Plaintiffs and the Class are entitled in equity;

G. Establish a constructive trust, until further order of the Court, consisting of monies Google improperly collected or received from its above-described illicit conduct;

H. Order Google to disgorge revenues and profits wrongfully obtained;

I. Award Plaintiffs and the Class their reasonable expenses and attorneys' fees;

J. Award Plaintiffs and the Class interest, to the extent allowable; and,

K. Award such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Dated: April 26, 2013 Respectfully submitted,

/s/ Kassra P. Nassiri

KASSRA P. NASSIRI (215405)
knassiri@nassiri-jung.com
NASSIRI & JUNG LLP
47 Kearny St, Suite 700
San Francisco, California 94108
Telephone: (415) 762-3100
Facsimile: (415) 534-3200

MICHAEL J. ASCHENBRENER (277114)
mja@aschenbrenerlaw.com
ASCHENBRENER LAW, P.C.
795 Folsom Street, First Floor
San Francisco, California 94107
Telephone: (415) 813-6245
Facsimile: (415) 813-6246

ILAN CHOROWSKY
ilan@progressivelaw.com
ALEX STEPICK
alex@progressivelaw.com
1 N LaSalle Blvd, Suite 2255
Chicago, IL 60602
Telephone: (312) 787-2717
Facsimile: (888) 574-9038

Attorneys for Plaintiffs and the Putative Class

APPENDIX B
RELEVANT STATUTORY PROVISIONS

1. 18 U.S.C. § 2702(a)-(c) provides:

§ 2702. Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processsing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such

service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108–21, title V, §508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

2. 18 U.S.C. § 2707(a)-(c) provides:

§ 2707. Civil action

(a) CAUSE OF ACTION.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.