

15-1141

No. 15-

Supreme Court, U.S.
FILED

MAR 10 2016

OFFICE OF THE CLERK

IN THE
Supreme Court of the United States

IN RE: GOOGLE INC. COOKIE PLACEMENT
CONSUMER PRIVACY LITIGATION

**On Petition for a Writ of Certiorari
to the United States Court of Appeals
for the Third Circuit**

PETITION FOR A WRIT OF CERTIORARI

EDWARD D. ROBERTSON, JR.
Counsel of Record
BARTIMUS, FRICKLETON AND
ROBERTSON, PC
715 Swifts Highway
Jefferson City, MO 65109
(573) 659-4454
crobertson@bflawfirm.com

March 10, 2016

QUESTIONS PRESENTED

1. Whether third-parties who access Internet cookies without authorization and thereby acquire the content of Internet communications between Internet users and websites are immune from Wiretap Act liability as actual parties to communications between Internet users and those websites.
2. Whether the Stored Communications Act protects data detailing an Internet user's web browsing history stored within a web browser provider's files that are accessible by an Internet user's web-browser provider and contained on the personal computing device of the user.

PARTIES TO THE PROCEEDING BELOW

The parties to the proceeding in the United States Court of Appeals for the Third Circuit were Petitioners / Class Plaintiffs William Gourley, Jose M. Bermudez, Nicholas Todd Heinrich, and Lynne Krause, representing internet users in a consolidated multi-district class action and Defendants Google, Inc., Vibrant Media, Inc., Media Innovation Group, LLC, and WPP PLC.

TABLE OF CONTENTS

QUESTIONS PRESENTED.....	i
PARTIES TO THE PROCEEDING BELOW.....	ii
TABLE OF CONTENTS.....	iii
TABLE OF AUTHORITIES.....	vi
OPINIONS AND ORDERS BELOW.....	1
JURISDICTION.....	1
STATUTORY PROVISIONS INVOLVED.....	2
INTRODUCTION.....	2
STATEMENT OF THE CASE.....	5
The Third Circuit’s Wiretap Opinion.....	6
The Third Circuit’s SCA Opinion.....	6
REASONS THE COURT SHOULD GRANT THIS PETITION FOR WRIT.....	7
1. The Third Circuit’s Opinion Conflicts with other Federal Circuit Courts of Appeal on Whether Third-Party Cookie Companies or Others Deploying Similar Automatic Routing Programs Can Be Liable Under the Wiretap Act.....	7
A. The Third Circuit Has Decided an Important Question of Federal Law That This Court Should Decide with Respect to the Application of the Wiretap Act to Internet Communications.....	11
B. The Third Circuit Upends <i>DoubleClick</i> and Its Progeny.....	12
C. The Third Circuit Opinion Would Lead to Absurd Results.....	15

D. The Third Circuit Opinion Would Justify Sweeping Warrantless Government Surveillance Through Deceit.....	17
2. The Third Circuit Opinion Failed to Determine Whether Web-Browsers are Protected by the SCA, an Important of Question of Law that Affects This Court's Recent Fourth Amendment Jurisprudence	22
A. Case of First Impression for Appellate Courts	22
B. The Third Circuit Opinion Undermines <i>Riley v. California</i>	24
C. This Case Impacts Daily Privacy Rights of Millions of Americans	29
D. For Both the Wiretap Act and SCA, the Third Circuit Opinion Would Significantly Harm the Ability of Tech Companies and Law Enforcement to Deter and Prosecute Computer Hacking.....	31
E. This Case Sits at the Fulcrum of Several Important Issues	34
CONCLUSION.....	35

APPENDIX

- A. November 12, 2015 Opinion of the United States District Court of Appeals for the Third Circuit
.....2a
- B. Court of Appeals' December 11, 2015 denial of petition for rehearing en banc
.....63a
- C. October 9, 2013 Memorandum Opinion of the United States District Court for the District of Delaware
.....65a

TABLE OF AUTHORITIES

Cases

<i>Barnicki v. Vopper</i> , 532 U.S. 514, 526 (2001)	15
<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001).....	4
<i>Garcia v. City of Laredo</i> , 702 F.3d 788, 793 (5th Cir. 2012).....	23
<i>Griffin v. Oceanic Contractor’s Inc.</i> , 458 U.S. 564, 575 (1982)	15
<i>Griswold v. Connecticut</i> , 381 U.S. 479, 486 (1965) ..	30
<i>In re Google Inc. Cookie Placement Consumer Privacy Litigation</i> , 988 F.Supp.2d 434 (D. Del. 2013).....	1
<i>In re: DoubleClick Privacy Litigation</i> , 154 F.Supp.2d 497, 505 (S.D. N.Y. 2001)	12, 13
<i>In re: Google Cookie Placement</i> , 806 F.3d 125, 132 (3rd Cir. 2015).....	passim
<i>In re: iPhone Application Litigation</i> , 844 F.Supp.2d 1040 (N.D. Cal. 2012).....	14
<i>In re: Pharmatrak, Inc.</i> , 329 F.3d 9 (1st Cir. 2003) ..	8, 15
<i>In re: Request for Order Requiring Facebook to Produce Documents and Things</i> , 923 F.Supp.2d 1204 (N.D. Cal. 2012).....	34
<i>Joffe v. Google</i> , 746 F.3d 920, 931 (9th Cir. 2013) ..	15, 17
<i>Kewanee Oil v. Bicron</i> , 416 U.S. 470, 478 (1973).....	30
<i>Microsoft v. Does 1-18</i> , 13-cv-139 (E.D. Va. 2013) ...	23
<i>Microsoft v. Does 1-27</i> , 10-cv-00156 (E.D. Va. 2010)23	
<i>Microsoft v. Does 1-39</i> , 12-cv-1335 (E.D. N.Y. 2012)23	
<i>Microsoft v. Does 1-8</i> , 14-cv-00811-LO-IDD, Dkt. #57, July 20, 2015	23
<i>Microsoft v. Does 1-82</i> , 13-cv-00319 (W.D. N.C. 2013)	23
<i>Olmstead v. U.S.</i> , 277 U.S. 438, 478 (1928).....	30

<i>Quon v. Arch Wireless</i> , 529 F.3d at 900	27
<i>Riley v. California</i> , 134 S.Ct. 2473 (2014)	passim
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	25
<i>Steve Jackson Games v. U.S.</i> , 36 F.3d 457, 462 (5th Cir. 1994)	3
<i>U.S. v. Anderson</i> , 2007 WL 1121319 at 6 (N.D. Ind. Apr. 16, 2007)	28
<i>U.S. v. Beckett</i> , 544 F.Supp.2d 1346, 1350 (S.D. Fla. 2008)	28
<i>U.S. v. Councilman</i> , 373 F.3d 197, 211 (1st Cir. 2004)	2
<i>U.S. v. Councilman</i> , 418 F.3d 67, 81 (1st Cir. 2005) ..	3
<i>U.S. v. Jones</i> , 132 S.Ct. 945, 957 (2012)	25, 29, 34
<i>U.S. v. Szymuszkiewicz</i> , 622 F.3d 701 (7th Cir. 2010)	10, 32
<i>U.S. v. Young</i> , 350 F.3d 1302, 1308-09 (11 th Cir. 2003)	28
<i>United States v. Matlock</i> , 415 U.S. 164 (1974)	25

Statutes

18 U.S.C. § 2510	2
18 U.S.C. § 2701	2
28 U.S.C. § 1254	1

Other Authorities

A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208 (2004)	3, 24
S. Rep. No. 99-541	2, 26, 32
The Lesson of Google's Safari Hack," Wall Street Journal, July 2012	33

Regulations

26 C.F.R. 1.501(c)(4)-1(a)(2)(i)	20
--	----

PETITION FOR WRIT OF CERTIORARI

Petitioners Class Plaintiffs respectfully petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the Third Circuit in this case.

OPINIONS AND ORDERS BELOW

In re Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015) (Opinion of the United States Court of Appeals, Third Circuit).

In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434 (D. Del. 2013) (Decision of the United States District Court for the District of Delaware).

JURISDICTION

This Court has jurisdiction pursuant to 28 U.S.C. § 1254 in that:

- A three-judge panel of the United States Court of Appeals, Third Circuit issued its opinion on November 10, 2015;
- Petitioners timely filed a petition for en banc rehearing, which the Third Circuit denied on December 11, 2015; and,
- The Third Circuit issued its mandate in this case on December 21, 2015.

STATUTORY PROVISIONS INVOLVED

1. Title I to the Electronic Communications Privacy Act;
18 U.S.C. § 2510, et. seq. (Wiretap Act)
2. Title II to the Electronic Communications Privacy Act
18 U.S.C. § 2701, et. seq. (Stored Communications Act)

INTRODUCTION

Congress passed the Electronic Communications Privacy Act in 1986 “to provide greater protections to electronic communications[.]” *U.S. v. Councilman*, 373 F.3d 197, 211 (1st Cir. 2004). In particular, Congress noted a purpose to ensure the continued relevance of the Fourth Amendment:

[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

S. Rep. No. 99-541 at 5 (1986).

Since passage of the ECPA, the Internet has become a dominant medium of communication in American life. According to Pew, 87 percent of Americans use the Internet to send and receive

electronic communications.¹ The average American spends 60 hours a month on the Internet via a smart-phone or desktop computer.²

This case involves two provisions of the ECPA: (1) the amended Wiretap Act, and (2) the Stored Communications Act. Despite the efforts of Congress to ensure that federal law would “advance with the technology to ensure the continued vitality of the fourth amendment,” federal courts have struggled with these provisions of ECPA. *See, e.g., Steve Jackson Games v. U.S.*, 36 F.3d 457, 462 (5th Cir. 1994) (describing Wiretap portion of ECPA as “complex” and “famous (if not infamous) for its lack of clarity.”); *U.S. v. Councilman*, 418 F.3d 67, 81 (1st Cir. 2005) (describing intersection of Wiretap and SCA as “complex” and “often convoluted.”); and Kerr, Orin S., A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It, 72 GEO. WASH. L. REV. 1208 (2004) (“Despite its obvious importance, the [SCA] remains poorly understood. ... The statute is dense and confusing, and few cases exist explaining how the statute works.”)

On the Wiretap issue, this case provides the Court with a vehicle to resolve a circuit conflict on

¹ <http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/>
<http://www.pewinternet.org/data-trend/internet-use/internet-use-over-time/>

² The Digital Consumer Report Nielson, Feb. 2014, available at: <http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2014%20Reports/the-digital-consumer-report-feb-2014.pdf>

whether the Wiretap Act applies to companies that place or access what the Defendants describe as and are commonly known as “third-party” cookies without authorization from the Internet users and the websites with which they are communicating.

On the SCA issue, this case provides the Court a vehicle to ensure that it meant what it said in its recent unanimous opinion in *Riley v. California*. If left to stand, the Third Circuit decision would render *Riley* meaningless in the real world. See *Riley v. California*, 134 S.Ct. 2473 (2014).

Though this Court has decided several cases applying the Fourth Amendment to modern technologies, it has yet to determine the extent of protections that electronic, and, in particular, Internet communications are afforded under the ECPA.³ This case is a vehicle for the Court to clarify the extent to which the ECPA protects Internet communications.⁴

³ *Bartnicki v. Vopper*, 532 U.S. 514 (2001), involved the ECPA. However, it is best characterized as a First Amendment case.

⁴ Because the ECPA applies both to private and governmental actors, the decision in this case will also directly impact important questions of governmental tracking by the National Security Agency which would otherwise be unlikely to come before this Court because of the statutory structure of the Foreign Intelligence Surveillance Court, established by Congress in 1978 to oversee national security applications to surveil domestic and foreign targets.

STATEMENT OF THE CASE

This case arises from the Defendants' successful computer hack around the privacy settings of Apple Safari and Microsoft Internet Explorer, two of the most popular web-browsing services that Americans use to send and receive communications on the Internet. The Defendants accomplished this hack through the use of a computer technology that the Defendants themselves describe as "third-party" cookies that were placed or accessed on the Plaintiffs' web-browsers through surreptitious computer code. In particular, "Google and the other defendants ... discovered, and were surreptitiously exploiting loopholes in both the Safari cookie blocker and the Internet Explorer cookie blocker." *In re: Google Cookie Placement*, 806 F.3d 125, 132 (3rd Cir. 2015). (App. 7a).

After hacking their way around privacy settings, the Defendants secretly acquired, tracked, and recorded the private electronic communications of Internet users while those communications were *in transit* between and the users and websites and *in storage* within web-browser files. As explained by the Third Circuit, Google's third-party acquisitions were "characterized by deceit and disregard," and were carried out without the knowledge or consent of Apple, Microsoft, the Internet users being tracked, or the websites with which those users were communicating. *In re: Google Cookie*, 806 F.3d at 150. (App. 55a).

The Plaintiffs filed suit to vindicate statutory and common law rights to privacy. The Third Circuit

remanded the case back to the District Court on December 21, 2015 for further proceedings on the Plaintiffs' common law claims for invasion of privacy and intrusion upon seclusion. In this Petition for Writ of Certiorari, Petitioners/Plaintiffs seek review of their claims under the ECPA, in particular the Wiretap and Stored Communications Acts.⁵

The Third Circuit's Wiretap Opinion

This Petition for Writ seeks review of the Third Circuit's ruling that a defendant utilizing third-party cookies is immune from suit under the Wiretap Act as an actual "party" to the communication between Internet users and the websites with which they are communicating. The Third Circuit opinion creates a circuit conflict and, if allowed to stand, would eviscerate Wiretap protections for Internet communications.

The Third Circuit's SCA Opinion

This Petition also seeks review of the Third Circuit's ruling that a web-browser and its constituent files are not protected by the SCA. In this case, the Third Circuit explained its decision that a person's personal computing device is not protected by the SCA. However, it failed to address whether web-browsers and the files contained within them are protected. The Third Circuit's opinion on this matter

⁵ Though based on the same operative set of facts, these federal statutory claims have different elements than the common law claims. Just as important and as explained below, the ultimate resolution of these federal statutory claims will have tremendous impact on the privacy rights of all Americans.

substantially undermines this Court's unanimous opinion in *Riley v. California*, leaves the stored electronic communications of millions of Americans unprotected from warrantless disclosure to the government or access by governmental actors through deceit, and, though there is no other circuit opinion on the issue, conflicts with every district court to have considered the issue.

REASONS THE COURT SHOULD GRANT THIS PETITION FOR WRIT

1. The Third Circuit's Opinion Conflicts with other Federal Circuit Courts of Appeal on Whether Third-Party Cookie Companies or Others Deploying Similar Automatic Routing Programs Can Be Liable Under the Wiretap Act

Question Presented:

Whether third-parties who access Internet cookies without authorization and thereby acquire the content of Internet communications between Internet users and websites are immune from Wiretap Act liability as actual parties to communications between Internet users and those websites.

The Third Circuit opinion creates a split of authority on whether the Wiretap Act applies to surreptitious computer-code-based acquisitions of content by third-party cookie companies without the

knowledge or consent of the actual parties to the communication. The Third Circuit held that the third-party cookie company Defendants were parties to the communications because “the defendants were the intended recipients of the transmissions at issue – i.e. GET requests that the plaintiffs’ browsers sent directly to the defendants’ servers[.]” *In re: Google Inc. Cookie Placement*, 806 F.3d 125, 143 (3rd Cir. 2015). (App. 34a). This holding conflicts with *In re: Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003).

In *Pharmatrak*, the defendant was also a third-party cookie company that had placed computer code on websites. The cookies in *Pharmatrak* were functionally identical to the cookies in this case. The First Circuit explained that they “cause[d] the user’s computer to communicate directly with Pharmatrak’s web server.” *Pharmatrak* at 14.⁶

In ruling that third-party cookie companies can be liable under the Wiretap Act, the First Circuit explained that third-party cookies involve separate channels of information. *Id.* at 22. Pharmatrak’s coding “was effectively an automatic routing program. It was code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third-party.” *Id.*

⁶ In footnote 64, the Third Circuit attempts to factually distinguish the *Pharmatrak* cookies, citing that the *Pharmatrak* code “automatically duplicated part the communication between a user and a [website] and sent this information to a third party.” The *Pharmatrak* description of third-party cookies applies equally to the cookies in this case – and every other third-party cookie.

at 22. By finding that *Pharmatrak* intercepted a communication with these cookie technologies, the First Circuit also necessarily determined that a third-party cookie company is not a “party to the communication” between Internet users and websites.

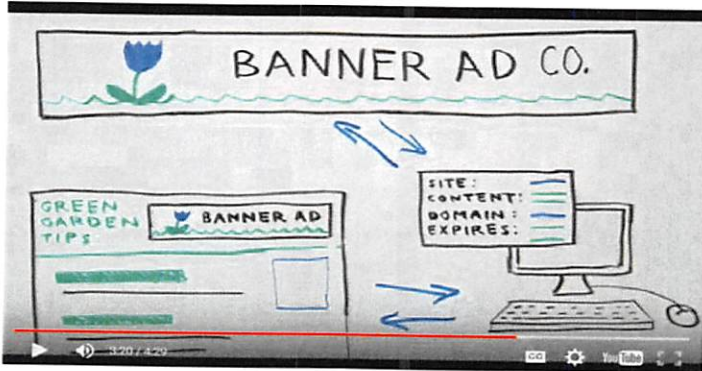
Google itself has explained why a third-party cookie company is not a party to the communication between Internet users and websites:

Unlike first-party cookies, that travel back-and-forth between your browser and the website you’re visiting, third-party cookies typically travel between your browser and the website of a company that’s displaying an ad on the website you’re visiting. That’s why they’re called third-party cookies. Because the website sending cookies to your browser, usually an ad-serving company, is actually a different site from the one you’re visiting.⁷

The Third Circuit’s holding fails to distinguish between the intended, actual communications between Internet users and the websites with which they communicate versus the unintended and separate GET request between the user’s web-browser and the Defendants’ ad server. These communications are not the same, and Google is clearly not a party to

⁷See video at <https://www.google.com/intl/en/policies/technologies/cookies/>. Explanation starting 2:53.

the communications between the user and the website. Google itself has illustrated the distinction:⁸



The Third Circuit’s opinion also conflicts with the result in *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). In *Szymuszkiewicz*, the Seventh Circuit found against a defendant who used computer code that instructed the victim’s email service to automatically re-direct all emails received by the victim to the defendant. In other words, just as in this case and *Pharmatrak*, the defendant in *Szymuszkiewicz* surreptitiously directed an electronic communication service employed by the victim to automatically send the content of her communications directly to the defendant. *Id.* at 703. It was another “automatic routing program.” The defendant did not directly argue that he was a party to the communication. Instead, he argued no “interception” occurred because he only acquired the communications after they had arrived in the victim’s

⁸ This diagram is captured from a screenshot on Google’s website at <https://www.google.com/intl/en/policies/technologies/cookies/>, wherein at the 3:20 mark of the video, Google’s explains, “That’s why they’re called third-party cookies. Because the website sending the cookies to your browser, usually an ad serving company, is actually a different site from the one you’re visiting.”

email in-box, and they were thus sent directly from the victim to him. *Id.* at 703. The Seventh Circuit rejected the argument. However, under the First Circuit's logic in this case – that a defendant can be deemed a party simply because a communication was sent from the plaintiffs' ECS "directly to the defendants' server" – the result would have been different.

A. The Third Circuit Has Decided an Important Question of Federal Law That This Court Should Decide with Respect to the Application of the Wiretap Act to Internet Communications

The Third Circuit's interpretation of the Wiretap Act is manifestly important to the future of Internet privacy in the United States. As explained by Professor Orin Kerr regarding this case:

The Third Circuit has handed down a very important opinion on Internet surveillance law. ... The decision is the first case to grapple in detail with how the Wiretap Act applies to the Internet. *If you're interested in surveillance law, you need to give this opinion a close and careful read. It's a big deal.*⁹

⁹ See Kerr, Orin, *Websurfing and the Wiretap Act, part 2: The Third Circuit's Ruling*, WashingtonPost.com, Nov. 19, 2015. Available at <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/19/websurfing-and-the-wiretap-act-part-2-the-third-circuits-ruling/>.

Indeed, the ultimate resolution of this case will have a profound impact on the everyday privacy of hundreds of millions of Americans. If left to stand, the Third Circuit opinion would (A) upend the legal regime governing third-party cookies on the Internet; (B) effectively transform the Internet to a place where the Wiretap Act rarely, if ever applies; (C) justify sweeping government surveillance, without a warrant, through surreptitious and deceitful government tracking; and (D) significantly hamper the ability of Internet technology companies and law enforcement to deter and prosecute Internet crimes. The frequency with which similar questions have faced the District Courts supports resolution by this Court.

B. The Third Circuit Upends *DoubleClick* and Its Progeny

Since *In re: DoubleClick Privacy Litigation*, 154 F.Supp.2d 497, 505 (S.D. N.Y. 2001), the legality of persistent third-party tracking cookies has rested on the implied consent of Internet users and the entities with which they are communicating. In *DoubleClick*, the Court explained that persistent third-party tracking cookies were legal because DoubleClick “would not collect information from any user who [took] simple steps to prevent DoubleClick’s tracking ... [including] configuring their browsers to block any cookies from being deposited” which, the Court noted, could be done “easily” and “at no cost.” *Id.*

This case also involves DoubleClick cookies.¹⁰ Except, in this case, Google and the other Defendants accomplished their acquisitions after users had taken the very “simple” steps that the *DoubleClick* Court said would “prevent DoubleClick’s tracking.” In other words, the Plaintiffs did exactly as the *DoubleClick* Court advised to protect the privacy of the electronic communications – and the Third Circuit ruled it did not matter.

The Third Circuit opinion is an outlier. To Petitioners’ knowledge, it is the only federal court to have found that a third-party cookie company is immune as a “party to the communications” between Internet users and websites. Under the Third Circuit’s logic, a hacker who exceeds authorizations and thereby surreptitiously acquires the content of communications automatically becomes an exempt party to the communication under the Wiretap Act – regardless of whether the Internet users or websites had knowledge of or consented to the extent of the third-party’s acquisition.

The Third Circuit’s opinion recognizes its own circular logic:

Tautologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient. As the intended recipient of a communication is

¹⁰ Google acquired DoubleClick in 2007.

necessarily one of its parties, and the defendants were the intended recipients of the GET requests acquired here, the defendants were parties to the transmissions at issue in this case. *Emphasis added.*

In re: Google Cookie Placement at 143. (App. 35a).

In this case, however, the Defendants were not the intended recipients of, nor a party to, the Internet user's communication with the subject website. Nor were Defendants a party to the website's return communication to the user. In fact, the GET requests acquired by the Defendants did not necessarily contain information about the substance, purport, or meaning of the separate but simultaneous communications between the users and the websites. That information – the “content” acquired – was contained within a “referrer” header acquired by the Defendants. Moreover, the Defendants' placement of a tracking cookie, accomplished in contravention of the Internet user's web browser privacy settings, further allowed the Defendants to attach meaning to the communications they were obtaining (i.e. the identity of the user making the communication).

In addition to “cookie” cases, the Third Circuit's opinion conflicts with *In re: iPhone Application Litigation*, 844 F.Supp.2d 1040 (N.D. Cal. 2012). In that case, the plaintiffs alleged Apple violated the Wiretap Act by acquiring their geo-location information without their consent. Apple argued it

was immune under the same “party to the communication” exception at issue in this case. Apple claimed it was “an intended recipient” of the plaintiffs’ location data because it had “designed iOS 4 to access and transmit location data from the mobile device to Apple’s servers.” *iPhone App* at 1062. Judge Lucy Koh rejected the argument, explaining, “Apple cannot manufacture a statutory exemption through its own accused conduct.” *Id.*

C. The Third Circuit Opinion Would Lead to Absurd Results

“Interpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available.” *Griffin v. Oceanic Contractor’s Inc.*, 458 U.S. 564, 575 (1982). In this case, the paramount legislative purpose of the Wiretap Act is widely recognized – it is to “protect effectively the privacy of communications.” *Pharmatrak*, 329 F.3d 9, 18 (1st Cir. 2003), see also *Barnicki v. Vopper*, 532 U.S. 514, 526 (2001). Though not intended by the Third Circuit, the practical effect of its opinion is that the Internet would become a zone where the Wiretap Act rarely applies. This is absurd and contrary to the intent of the ECPA.

In *Joffe v. Google*, 746 F.3d 920, 931 (9th Cir. 2013), Google presented a similar argument with regard to the definition of “radio communication” under the ECPA. In that case, Google had collected Wi-Fi communications sent over unencrypted

networks. *Id.* at 923. Google argued it was immune because, even though the plaintiffs had made the subject communications from the privacy of their homes and businesses, since the communications were sent over Wi-Fi, they were “readily accessible to the general public.” *Joffe*, at 924.

The *Joffe* Court explained that Google’s proposed definition of “radio communication” was “in tension with how Congress – and virtually everyone else – uses the phrase.” *Id.* at 928. “In common parlance,” the Court continued, “watching a television show does not entail ‘radio communication.’ Nor does sending an email or viewing a bank statement while connected to a Wi-Fi network. There is no indication that the Wiretap Act carries a buried implication that the phrase ought to be given a broader definition than the one that is commonly understood.” *Id.*

Further, the Court stated that Google’s “expansive definition” would mean that Wiretap Act protection turned on whether recipients to communications had decided to secure their wireless networks – even though “the sender ... is in no position to ensure that the recipient ... has taken care to encrypt [their] Wi-Fi network.” *Id.* at 931. The *Joffe* Court rejected Google’s argument because of these absurd results.

Respectfully, this Court should grant certiorari to reject Google’s similarly expansive argument in this case. In common parlance, third-party cookie companies are not actual parties to communications

between Internet users and web-sites. By their very name, they are third-parties.

Moreover, similar to *Joffe*, because Google only accomplished this feat by hacking its way around the Plaintiffs' privacy setting, the Third Circuit opinion would make Wiretap protection for ordinary consumers contingent on whether the web-browsers they utilize and the web-sites with which they communicate adequately secured their services and websites against third-party hackers.

If accepted outside the Internet context, the Third Circuit's logic would undermine the Wiretap Act even in more traditional scenarios. Consider the classic wiretap case where a person places a mechanical device directly into the victim's telephone that directs the phone to send the substance of every call to a third person or location unknown to the caller. By placing the device on the telephone, the interceptor creates a direct path between the user and the recipient. Tautologically, the interceptor receives the communication just as the intended recipient of the communication does. Yet under the logic of the Third Circuit, because the communication was sent directly from the victim's telephone to the defendant's receiving device, the defendant is an exempt party. Such is the absurd result of the Third Circuit's ruling.

D. The Third Circuit Opinion Would Justify Sweeping Warrantless Government Surveillance Through Deceit

The ECPA protects privacy by limiting both private and government surveillance of Americans. The “content” of electronic communications is “protected by a super-warrant” under the Wiretap Act against government surveillance. *In re: Google Cookie* at 136, n. 32. (App. 18a, note 32). Federal courts consider hundreds, if not thousands, of cases every year dealing with the different parts of the ECPA (Wiretap Act, SCA, and Pen Register Act). The Third Circuit opinion, however, would provide government entities with a way to hack around the super-warrant requirement to obtain the “content” of communications.

Consider the following example. According to an online tax preparation company, more than 90 percent of Americans filed their taxes online in 2015.¹¹ Suppose the IRS, for “security purposes,” places cookies on the computing devices of every American who files their taxes online. The IRS informs tax-filers of the cookies, but promises not to access them except when the tax-filer is actually attempting to file their taxes.

Further, suppose the IRS requires tax preparation firms to place a specific computer code in the header or footer of each web-page that places an IRS-approved logo on the page in order to permit the tax preparation firms’ clients to file their taxes online. The IRS tells the tax preparation firms that the computer code is necessary for security purposes so

¹¹ <http://www.efile.com/efile-tax-return-direct-deposit-statistics/>

the IRS can verify that the website is an approved vendor. As with other code placed on web-pages, the IRS informs the web-page that it will get certain information about each web-page, including the detailed URL, via a referer header, but promises that it will not track individual tax-filers through these cookies.

In response, tax preparation firms place IRS computer code on every web-page on their sites, including pages like: <http://www.efile.com/what-are-the-penalties-for-not-filing-a-tax-return-or-not-to-pay-taxes-IRS-penalty-list/>. As in this case, however, unbeknownst to the tax-filers and the tax preparation firms, the IRS computer code is not limited to passively collecting referer headers and ensuring security. Instead, the IRS code secretly collects the full-string referer headers attached to cookies which individually identify each particular tax-filer. Thus, the IRS obtains the contents of communication that tax-filer John Doe makes with his tax preparation firm through his web-browser. The IRS then uses this information to determine which tax-filers to audit.

Is the IRS a party to the communication between the tax-filer and their chosen tax preparation firm? Under the Third Circuit's logic, it is.

Next assume the IRS tells groups applying for or that have received 501(c)(4) non-profit status that it may install computer code on each webpage of their website that makes it easier for the IRS to determine whether they qualify and are indeed "operated

primarily for the purpose of bringing about civic betterments and social improvements” as required by 26 C.F.R. 1.501(c)(4)-1(a)(2)(i). As before, the IRS tells applicants that the code is only for the purpose of determining eligibility and that it will not access cookies associated with tax-filer accounts through this code.

As with the tax-preparation firm example and this case, however, the IRS code secretly collects full-string referer headers attached to the tax-filer cookies. Through this code, the IRS acquires the content of communications sent by millions of Americans to non-profit websites. As with the instant case, neither the non-profit nor the tax-filer knows the IRS has secretly hacked its way in to acquire this complete information.

Is the IRS a party to these communications? Under the Third Circuit’s logic, it is.

Or consider the NSA, FBI, DEA, ATF, DHS, FDA, EPA, FCC, NLRB, or HHS. Would they be parties to communications if they attempted a similar scenario? At the state level, could a state health agency track communications of medical providers through similar hacking schemes? If a government agency tricks or coerces a regulated entity into placing computer code from the government agency on their website, and then the government agency surreptitiously uses that code to track individual Americans, is the agency a party to the communications of the unknowing Americans they are tracking? Under the Third

Circuit's logic, they are. That is a dangerous result that Petitioners respectfully request this Court to address by granting their Petition for Writ of Certiorari.

2. The Third Circuit Opinion Failed to Determine Whether Web-Browsers are Protected by the SCA, an Important Question of Law that Affects This Court's Recent Fourth Amendment Jurisprudence

Question Presented:

Whether the Stored Communications Act protects data detailing an Internet user's web browsing history stored within a web browser provider's files that are accessible by an Internet user's web-browser provider and contained on the personal computing device of the user.

A. Case of First Impression for Appellate Courts

The Third Circuit held that Plaintiffs had not adequately alleged unauthorized access to a "*facility* through which an electronic communication service is provided" under the SCA. In making its ruling, the Third Circuit ruled that "an individual's personal computing device is not a facility" but failed to address a key allegation of the Plaintiffs' Complaint – that Plaintiffs' web-browsers and the constituent files contained within them are "facilities" protected by the SCA.

To date, no federal appellate court has considered whether web-browsers are protected by the SCA. However, there are several district court cases on

point. In fact, Microsoft has quietly, consistently, and successfully used the SCA as a sword to prosecute computer hackers who gain unauthorized access to Internet Explorer and its constituent files located on the operating systems of Internet Explorer users' personal computing devices.

For example, in *Microsoft v. Does 1-8*, 14-cv-00811-LO-IDD, Dkt. #57, July 20, 2015, the Eastern District of Virginia found that Microsoft IE and the files contained within it are protected by the SCA. In that case, much like this one, the defendants hacked their way around the web-browser's privacy settings to take information from the browsers and computers of IE users. The district court found that the plaintiffs, which included Microsoft and a consortium of banks and other financial service industry businesses, had "alleged sufficient facts substantiating their [SCA] claim[s]," and, in unequivocal terms, found that "Microsoft's Windows operating system and Internet Explorer software are facilities through which electronic communications services are provided." *Id.* at 15. See also, *Microsoft v. Does 1-27*, 10-cv-00156 (E.D. Va. 2010)(Brinkema, J.); *Microsoft v. Piatti*, 11-cv-01017 (E.D. Va. 2011)(Cacheris, J.); *Microsoft v. Does 1-39*, 12-cv-1335 (E.D. N.Y. 2012)(Johnson, J.); *Microsoft v. Does 1-18*, 13-cv-139 (E.D. Va. 2013)(Brinkema, J.); *Microsoft v. Does 1-82*, 13-cv-00319 (W.D. N.C. 2013).

The Third Circuit's opinion in this case relied on the logic of *Garcia v. City of Laredo*, 702 F.3d 788, 793 (5th Cir. 2012), which held that "a home computer of an end user is not protected by the [SCA]." *In re:*

Google Cookie at 146, (App. 43a) Critically, *Garcia* was not a case about web-browsers, and the court failed to take into account that Internet users do not own their web-browsers, but only use them subject to a license that allows web-browsing companies to maintain the right to access them.¹² Thus, when the Third Circuit opinion explained that the SCA “envisions a provider ... and a user ..., with the user’s communication in the possession of the provider,” it described the precise relationship that exists between web-browsing companies, such as Apple and Microsoft, and their users, such as the Plaintiffs. *In re: Google Cookie* at 147, (App. 46a), citing Kerr, *A User’s Guide to the Stored Communications Act*, 72 GEO. WASH. L. REV. at 1215. Indeed, the communications contained within web browser-operated files are accessible to and in possession of both the web-browser company and the user.

B. The Third Circuit Opinion Undermines *Riley v. California*

In *Riley v. California*, 134 S.Ct. 2473 (2014), this Court unanimously held that digital information on a cell phone is protected by the Fourth Amendment. The

¹² For examples, see Google Chrome, Apple Safari, and Microsoft Internet Explorer’s licensing agreements at:
https://www.google.com/intl/en_us/chrome/browser/privacy/eula_text.html
<https://www.apple.com/legal/sla/docs/SafariWindows.pdf>
<http://windows.microsoft.com/en-US/internet-explorer/ie10-win8-privacy-statement>

Court took particular note of the expectation of privacy that a person has in communications made through their web-browser, reasoning that “[a]n Internet search and browsing history ... could reveal an individual’s private interests or concerns – perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.” *Id.* at 2490. *Riley* protects this data from a direct search by the government.

However, under the third-party doctrine, data that is either voluntarily provided to or under the common authority of a third-party is not fully protected by the Fourth Amendment. See *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Matlock*, 415 U.S. 164 (1974). In this case, because a third-party (the web-browsing service provider) has joint access to data contained in the files contained within a user’s web-browser on their computing device, the same data protected by *Riley* is left without Fourth Amendment protection under the third-party doctrine. Instead of seeking the data through the front door, an officer needs only to serve a subpoena to the web-browsing company with access to the very same information.

As Justice Sotomayor has pointed out, in the digital age, the third-party doctrine punches an enormous hole in the constitutional protection of communications and data. See *U.S. v. Jones*, 132 S.Ct. 945, 957 (2012) (Sotomayor concurrence). (“[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”). This is because the third-party doctrine is “ill-suited

to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.” As Justice Sotomayor pointed out, “People disclose ... the URLs that they visit” and that, while some people “may find the tradeoff of privacy for convenience worthwhile,” Justice Sotomayor “doubt[s] that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.” *Id.*

This case shows why Justice Sotomayor’s doubt is well-founded. If the Third Circuit decision is left to stand, web-browsing companies may be required to make warrantless disclosure to the government of every web communication their users made in the last week, month, or year. Similarly, if the Third Circuit decision is left to stand, web-browsing companies may also be permitted to voluntarily consent to a government search of the files to which it has joint access.

As detailed above, Congress understood the relationship between the ECPA and the Fourth Amendment. It enacted the ECPA precisely so that the law would “advance with technology to ensure the continued vitality of the fourth amendment.” In creating the SCA, Congress explicitly expressed concern that the Fourth Amendment might not protect against searches and seizures (or voluntary disclosure by an ECS provider) of copies of an electronic communication “subject to control by a third-party computer operator[.]” See S. Rep. No. 99-541 (1986) at 3. See also *Quon v. Arch Wireless*, 529

F3d at 900 (“The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.”). As described by Defendant Vibrant Media in its brief before the Third Circuit, “[t]he SCA fills that constitutional gap by proscribing unauthorized access to electronic communications in third-party hands” or, to use the precise language from the legislative history, “subject to control by a third-party computer operator.”

Though home computers and mobile devices are protected by the Fourth Amendment when the government attempts to access them directly through an Internet user, because the same data is “subject to control by a third-party computer operator,” it is subject to the third-party doctrine and thus not fully protected by the Fourth Amendment.

It may seem odd at first glance that a person’s Internet communications contained within the files of their web-browser are “subject to control” by the web-browsing company that they use. However, to Petitioners’ knowledge, every major web-browser, including the two at issue in this case (Apple Safari and Microsoft Internet Explorer) requires users to agree to a licensing agreement that gives the web-browsing company the right to access a user’s computing device, and to allow authorized third-parties to do the same.¹³

¹³ The Department of Justice explains, “for Fourth Amendment purposes, commercial service providers typically have terms of service that confirm their authority to access information stored

If the Third Circuit opinion is left to stand, this Court's unanimous opinion in *Riley v. California* effectively means nothing in the real world. Rather than gaining access to a citizens' information through a warrantless search or seizure of their computer or smart phone, government officials could instead subpoena a citizens' web-browsing company or, in the case of Microsoft, the provider of their computer operating system. Because these electronic communications services have access to the same information, the data subject to their control falls under the third-party doctrine and outside the protection of the Fourth Amendment.

Instead of requiring a warrant, the same data this Court unanimously held was protected by the Fourth Amendment in *Riley* would be subject to disclosure by their web-browsing service provider via (1) private search, (2) third-party consent to a search of web-browser files; (3) the direct disclosure of the data by

on their systems, and such terms of service may establish a service provider's common authority over their users' accounts." See "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" at 25, published by the Office of Legal Education for the Executive Office for United States Attorneys and available at <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>. Internally citing *U.S. v. Young*, 350 F.3d 1302, 1308-09 (11th Cir. 2003) and *U.S. v. Beckett*, 544 F.Supp.2d 1346, 1350 (S.D. Fla. 2008). At least one other court has held that a computer repair technician could consent to a search of a computer brought in for repair because they had authority to access the computer. *U.S. v. Anderson*, 2007 WL 1121319 at 6 (N.D. Ind. Apr. 16, 2007).

the web-browser company to government officials; or (4) administrative subpoena.

The SCA, however, was designed precisely to give statutory protection to this information. Respectfully, Petitioners request that the Court grant the writ of certiorari to uphold the plain language and intent of the SCA – and, in the process, ensure *Riley's* rule remains as the Court issued it.

C. This Case Impacts Daily Privacy Rights of Millions of Americans

I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they visited in the last week, or month, or year.

United States v. Jones, 132 S.Ct. 945, 957 (Sotomayor concurrence).

In *U.S. v. Jones* and *Riley v. California*, in the context of applying the Fourth Amendment to modern technology, members of this Court noted the particular importance of Internet privacy. In *Jones*, Justice Sotomayor used web-browsing histories to question the continuing validity of the third-party doctrine in Fourth Amendment cases. In *Riley*, a unanimous Court explained that Internet “search and browsing history” is “qualitatively different” than physical records because it “could reveal an individual’s private interests or concerns – perhaps a

search for certain symptoms of disease, coupled with frequent visits to WebMD.” *Riley v. California*, 134 S.Ct 2473, 2490 (2014).

In constitutional and other cases, this Court has described the right to privacy as “the most comprehensive of rights,” “the right most valued by civilized men,” a right “older than the Bill of Rights – older than our political parties, older than our school system,” and “a most fundamental human right ... that is threatened when industrial espionage is condoned or is made profitable[.]” *See, Olmstead v. U.S.*, 277 U.S. 438, 478 (1928); *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965); *Kewanee Oil v. Bicron*, 416 U.S. 470, 478 (1973).

In addition to constitutional protections, Americans enjoy statutory protection of their rights to privacy. The ECPA is the primary federal law protecting the privacy of electronic communications, and since its passage in 1986, the Internet has become a dominant medium of communication in American life. According to Pew, 87 percent, or more than 271 million Americans, use the Internet to send and receive electronic communications.¹⁴ Three out of four

¹⁴ <http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/>
<http://www.pewinternet.org/data-trend/internet-use/internet-use-over-time/>

Americans communicate on the Internet every day – and one in five go online “almost constantly.”¹⁵

Of those Americans, the vast majority use web-browser type applications to send these communications. As explained by Google, the web-browser is where we “search, chat, email, ... collaborate, ... shop, bank, read news, and keep in touch with friends.”¹⁶ The Internet – and, in particular, the web-browser – has become the dominant mode of communication for commercial and personal purposes. There are literally trillions of private Internet communications that are sent and received by Americans on web-browsers every year. By granting certiorari in this case, the Court will determine whether these communications are protected against non-consensual tracking and acquisition by third-parties.

D. For Both the Wiretap Act and SCA, the Third Circuit Opinion Would Significantly Harm the Ability of Tech Companies and Law Enforcement to Deter and Prosecute Computer Hacking

As Congress explained when passing the ECPA in 1986, uncertainty over the privacy of electronic communications “unnecessarily discourage[s]

¹⁵ <http://www.pewresearch.org/fact-tank/2015/12/08/one-fifth-of-americans-report-going-online-almost-constantly/>

¹⁶ <https://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html>

potential customers from using innovative communications systems.” S. Rep. at 5. “It probably encourages unauthorized users to obtain access to communications to which they are not a party.” *Id.* And, “[i]t may discourage American businesses from developing new innovative forms of telecommunications and computer technology.” *Id.*

Indeed, the ECPA is used by innovative technology businesses as both a sword and a shield. Tech companies and law enforcement use the ECPA offensively to prosecute computer hackers who steal communications or communications of consumers. In turn, tech businesses also use it as a shield against government requests for data.

1. The Wiretap Act

The Wiretap Act portion of the ECPA carries significant criminal penalties, and, as shown by the *Szymuskiwicz* and *Councilman* cases, is used by law enforcement to prosecute computer hackers. Michael Chertoff, a former judge on the Third Circuit and former Secretary of the U.S. Department of Homeland Security, viewed this case as about far more than consumer privacy. Chertoff wrote:

[I]f Google can spoof Safari to allow tracking cookies without seeming to, then so can anyone else. Imagine how this vulnerability might affect a government employee who used Safari

on a government-issued computer as part of his official duties and whose browser usage would now be open to surreptitious inspection. ...

If an analyst at the Food and Drug Administration starts Web-based research for data on a new drug compound, a secret intruder might infer that the compound was next in line for evaluation. A Web search by an FBI agent may identify a person of interest in the early stages of a criminal or terrorist investigation.

Michael Chertoff, "The Lesson of Google's Safari Hack," Wall Street Journal, July 2012, available at: <http://www.chertoffgroup.com/article-the-lesson-of-googles-safari-attack.php>.

The Third Circuit opinion takes a key tool away from prosecutors and tech companies to deter and punish the types of hacks outlined by Mr. Chertoff and countless others.

2. The Stored Communications Act

Technology companies also use the SCA as a sword. *See, e.g.*, the Microsoft cases cited above. And they use it as a shield to defend against demands for their consumers' data. *See, e.g., In re: Request for Order Requiring Facebook to Produce Documents and*

Things, 923 F.Supp.2d 1204 (N.D. Cal. 2012). Under the Third Circuit’s opinion, the SCA will no longer be available to web-browsing companies to use as a sword to stop hackers. Nor will the SCA be available to web-browsing companies to use as a shield to protect their customers’ data from government inspection.

E. This Case Sits at the Fulcrum of Several Important Issues

The right to privacy finds protection in the First, Second, Third, Fourth, and Fifth Amendments. What the government can surveil affects not only a person’s effects, but also their thoughts and expressions. *See, U.S. v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor concurrence) (“Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.”)

This Court has long held that the right to privacy is a fundamental human right. What happens to the fundamental human right to privacy when every electronic communication made by an American citizen is subject to unauthorized, warrantless tracking by private or governmental actors? What happens to freedom of thought and expression when every thought and word is subject to private or government surveillance?

Petitioners respectfully suggest that this case provides the Court with an opportunity to resolve this most important privacy issue.

CONCLUSION

For this and the other reasons stated above, Petitioners respectfully request the Court grant certiorari.

Respectfully Submitted,

Edward D. Robertson, Jr.
Counsel of Record
BARTIMUS, FRICKLETON AND
ROBERTSON, PC
715 Swifts Highway
Jefferson City, MO 65109
573-659-4454
crobertson@bflawfirm.com