

# SUPREME COURT COPY

No. S230051

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

FACEBOOK, INC., et al.,  
*Petitioners,*

v.

SUPERIOR COURT OF THE STATE OF CALIFORNIA,  
SAN FRANCISCO

*Respondent.*

---

DERRICK D. HUNTER and LEE SULLIVAN,

Real Parties in Interest.

---

SUPREME COURT  
FILED

MAY 26 2016

Frank A. McGuire Clerk

---

Deputy

## REAL PARTY'S ANSWER TO GOOGLE'S BRIEF OF AMICUS CURIAE

From the Published Opinion of the Court of Appeal,  
First Appellate District, Division Five, No. A144315

San Francisco San Francisco Superior Court Nos. 13035657,  
13035658.) The Honorable Bruce Chan, Judge, Dept. 22

JANELLE E. CAYWOOD  
(CBN: 189980)  
3223 Webster Street  
San Francisco CA, 94123  
Tel. (415) 370-2673  
Fax. (888) 263-0456  
Email: [janelle@caywoodlaw.com](mailto:janelle@caywoodlaw.com)

Attorney for Real Party  
Lee Sullivan

SUSAN B. KAPLAN  
(CBN: 57445)  
214 Duboce Street  
San Francisco, CA 94103  
Tel. (415) 271-5944  
Fax. (510) 524-1657  
Email: [sbkapl@yahoo.com](mailto:sbkapl@yahoo.com)

Attorney for Real Party  
Lee Sullivan

TABLE OF CONTENTS

	<b>Page(s)</b>
TABLE OF AUTHORITIES .....	iv
ARGUMENT .....	1
<b>I.    INTRODUCTION .....</b>	<b>1</b>
<b>II.    UNDER THE SUPREMACY CLAUSE, A           CRIMINAL DEFENDANT’S FEDERAL CONSTITUTIONAL           RIGHTS, ENFORCEABLE BY CALIFORNIA TRIAL           COURTS, ARE PARAMOUNT TO THE SCA, A FEDERAL           STATUTE .....</b>	<b>5</b>
<b>III.   GOOGLE’S ARGUMENT THAT THIS COURT NEED           NOT DECIDE WHETHER THE SCA MUST YIELD TO           DEFENDANTS’ FEDERAL CONSTITUTIONAL RIGHTS           BECAUSE ELECTRONIC RECORDS MAY BE OBTAINED           FROM THE PROSECUTION IS WITHOUT MERIT.           NEITHER THE FOURTH AMENDMENT, PENAL CODE           SECTION 1524, NOR <i>BRADY V, MARYLAND</i> PERMIT THE           PROSECUTION TO ISSUE SEARCH WARRANTS TO           OBTAIN EXCULPATORY EVIDENCE IN THE POSSESSION           OF THIRD PARTIES .....</b>	<b>7</b>
<b>IV.   GOOGLE’S CONTENTION THAT THE REMEDY IS TO           FORCE THE GOVERNMENT TO DISMISS CRIMINAL           CASES IF THEY DO NOT PROVIDE EXCULPATORY           ELECTRONIC RECORDS TO THE DEFENSE IS WITHOUT           MERIT BECAUSE, UNLIKE CLASSIFIED STATE SECRETS,           ELECTRONIC RECORDS ARE HELD BY THIRD PARTIES.           THE GOVERNMENT CANNOT BE COMPELLED TO PROCURE           RECORDS FOR THE DEFENSE IN THE POSSESSION OF THIRD           PARTIES .....</b>	<b>10</b>

V. **GOOGLE FAILS TO ADDRESS HOW A WITNESS CAN BE COMPELLED TO IDENTIFY HER SOCIAL MEDIA ACCOUNTS AND CONSENT TO THE RELEASE OF HER ELECTRONIC RECORDS WHEN THE WITNESS HAS ASSERTED HER FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION** .....12

VI. **SINCE GOOGLE, FACEBOOK, INSTAGRAM, AND TWITTER PROVIDE THEIR USERS’ ELECTRONIC RECORDS TO LAW ENFORCEMENT AND TO THIRD PARTIES FOR THE PURPOSES OF TARGETING ADVERTISEMENTS FOR FINANCIAL GAIN, THEY MUST ALSO PROVIDE CRIMINAL DEFENDANTS WITH ELECTRONIC RECORDS WHEN A SUPERIOR COURT ORDERS THEM TO DO SO FOLLOWING AN *IN CAMERA* HEARING, GIVEN THE IMPORTANT FEDERAL CONSTITUTIONAL RIGHTS AT STAKE**.....13

CONCLUSION.....19

**TABLE OF AUTHORITIES**

<b>Cases</b>	<b>Page(s)</b>
<i>Brady v. Maryland</i> 373 U.S. 83 (1963) .....	7-9
<i>Davis v. Alaska</i> (1974) 415 U.S. 308 .....	2-3
<i>Delaney v. Superior Court</i> (1990) 50 Cal 3d. 785.....	6
<i>General Dynamics Corp v. United States</i> (2011) 563 U.S. 478 .....	10
<i>In re Garcia</i> (2014) 58 Cal.4th 440 .....	6
<i>In re Littlefield</i> 5 Cal.4th 122 (1993) .....	9
<i>Jacob B. v. Superior Court</i> (2007) 40 Cal.4th 968 .....	5
<i>Jencks v. United States</i> (1957) 353 U.S. 657 .....	10
<i>Miller v. Superior Court</i> (1999) 21 Cal.4th 883 .....	11-12
<i>Pennsylvania v. Ritchie,</i> 480 U.S. 39 (1987).....	1,2,3
<i>People v. Hammon</i> 15 Cal.4th 117 (1997) .....	4
<i>Swidler &amp; Berlin v. United States</i> (1998) 524 U.S. 399 .....	3

*United States v. Chronic*  
(1984) 466 U.S. 648 .....8

*United States v. Hanna*  
(6<sup>th</sup> Cir. 2001) 66 F.3d 271 .....8

*United States v. Warshak*  
631 F.3d 266 (2011) .....7, 8

**Federal Statutes**

18 U.S.C. § 2703.....passim

**California Statutes**

Penal Code §§ 1326-1327 .....passim

Penal Code § 1524 .....7,8, 11

## ARGUMENT

### I. INTRODUCTION

Google's *amicus curiae* brief merely repeats Facebook's flawed arguments which reveal a profound misunderstanding of constitutional law in criminal cases. To start, under the Supremacy Clause, a criminal defendant's federal constitutional rights are paramount to the SCA, a federal statute. California courts are not only authorized, but required, to enforce a criminal defendant's federal constitutional rights. If California courts do not have the authority to enforce a criminal defendant's federal constitutional rights, then California courts should not be conducting jury trials in criminal cases.

Like Facebook, Google cites a litany of inapt civil cases in which the litigants do not have the same federal constitutional rights as do criminal defendants. Thus, these civil cases are inapposite and shed no light on how superior court judges in criminal cases are to reconcile a criminal defendant's federal constitutional rights when in conflict with the Stored Communications Act ("SCA".)

Tellingly, in arguing that the SCA prohibits judges from reviewing electronic records *in camera* for evidence a criminal defendant needs to defend a case, Google fails to address the fact that in *Pennsylvania v.*

*Ritchie*, 480 U.S. 39, the United States Supreme Court held that when a statute declares records to be confidential, but that statute is not an absolute bar to the use of records at trial because it contains exceptions to the general rule of confidentiality, the federal Due Process Clause requires superior courts to conduct an *in camera* review of the confidential records and produce exculpatory records to the defense. Under *Ritchie*, superior court judges should have the authority to conduct this *in camera* review at a meaningful time, which in this case is prior to trial given the voluminous nature of social media records, so that defendants can mount an intelligent defense armed with the materials necessary to effectively cross-examine adverse witnesses.

Whether records are in the physical possession of electronic record providers or the government is a distinction without meaning under *Pennsylvania v. Ritchie*. The records are being withheld from the defense by the federal government by an act of Congress under the SCA. It matters not whether the records are held by third party bailees or the government for purposes of evaluating whether a defendant is constitutionally entitled to pretrial access to exculpatory evidence in order to prepare for trial. Due process and the right to defend a case requires that exculpatory electronic records be produced to a defendant at a meaningful time following an *in*

camera review, subject to protective orders protecting the privacy rights of witnesses.<sup>1</sup>

Google also fails to mention the seminal case of *Davis v. Alaska* (1974) 415 U.S. 308, at any point in its brief. In *Davis*, the United States Supreme Court held that a defendant's federal constitutional right to cross-examine witnesses trumps a statute declaring juvenile records to be confidential and not to be disclosed to the public. In *Davis*, the Sixth Amendment confrontation right arose at the time of trial. Here, the assertion of the right arises in the context of pretrial discovery one day prior to trial. Real parties believe this distinction is one without a difference given that in this case, the defendants cannot effectively cross-examine witnesses unless armed with the necessary records to impeach Reneesha Lee as well as the prosecution's gang expert prior to trial. Given the voluminous nature of social media records, it is clear that these defendants cannot receive a fair

---

1

A criminal defendant's constitutional right to due process is so sacrosanct, the United States Supreme Court has left open the question of whether the attorney-client privilege, an absolute privilege, can be pierced if necessary to secure a criminal defendant's right to a fair trial under the Due Process Clause. (*Swidler & Berlin v. United States* (1998) 524 U.S. 399, 415, fn 3.) Here, the SCA, is not an absolute bar to disclosure because the statute contains exceptions which permit law enforcement and other government officials, to obtain content-based electronic records. (18 U.S.C. § 2703.) Because there are exceptions to the general rule of confidentiality, the SCA must yield to the a defendant's constitutional rights under *Pennsylvania v. Ritchie*, *supra*, 480 at p. 58.)



trial unless these records are reviewed prior to trial so defense counsel can be effective in voir dire, opening statements, and in questioning witnesses. Insofar as *Hammon v Superior Court* (1997) 15 Cal.4th 117 holds otherwise, real parties ask that it be overruled or limited to psychiatric records. Delaying access to social media records until mid-trial would run afoul of defendants' fair trial rights because the records would not be received in time to mount an intelligent defense, and would lead to statewide chaos because trials would be stopped midway to review records, to investigate information contained in the records, and to engage in protracted litigation with the holders of electronic records while juries stand idly by awaiting the conclusion of the litigation. Mistrials would be the norm due to jury attrition and new evidence uncovered during trial. Moreover, Google fails to address how criminal defendants are to mount a defense in a criminal case without the ability to subpoena relevant electronic records before trial.

It is this Court's solemn duty to protect the rights of indigent criminal defendants from misguided acts of Congress as well as from powerful electronic records holders such as Google and Facebook who believe that they should be permitted to reap billions of dollars from storing electronic records and disseminating their customers' electronic data to

third parties obtain advertising dollars, but not be forced to respond to indigent criminal defendants' subpoenas despite that every other holder of confidential records in this State must comply with the procedures set forth in Penal Code section 1326.

Google's arguments fail as discussed below.

**II. UNDER THE SUPREMACY CLAUSE, A CRIMINAL DEFENDANT'S FEDERAL CONSTITUTIONAL RIGHTS, ENFORCEABLE BY CALIFORNIA TRIAL COURTS, ARE PARAMOUNT TO THE SCA, A FEDERAL STATUTE**

Google, like Facebook, misunderstands the Supremacy Clause and the well-established hierarchy of rights. Specifically, Google incorrectly states that a criminal defendant cannot obtain privileged records at trial notwithstanding his or her panoply of federal constitutional rights. (Google Br. at p. 7.) Google also states "that there is no source of law that could outweigh the express prohibitions of the SCA." (Google Br. at p. 2.) Not so. The United States Constitution can and does trump conflicting provisions of the SCA. A review of the hierarchy of rights is in order.

The Supremacy Clause simply means that rights based on federal law prevail over rights based on state law. (U.S. Const., Art. VI, Section 2.) California statutes must yield to California Constitutional rights. (*Jacob B. v. Superior Court* (2007) 40 Cal.4th 968.) Both California statutes and the California constitution must yield to a federal statute. (*In re Garcia* (2014)

58 Cal.4th 440, 452.) Everything is trumped by, and must yield to, the United States Constitution as it is the highest law of the land. (See e.g. *Delaney v. Superior Court* (1990) 50 Cal 3d. 785, 805-806.) Thus, a criminal defendants' federal constitutional rights to a fair trial, to present a complete defense, and to confront witnesses trump the privacy protections under the SCA, a federal statute. As briefed extensively by real parties and by California Attorneys for Criminal Justice ("CACJ") and National Association of Criminal Defense Lawyers ("National Association of Criminal Defense Lawyers"), California courts are vested with the authority to enforce a criminal defendant's federal constitutional rights in a criminal case. (Reply Br. pp. 6-8; CACJ/NACDL Br. pp. 6-11.) ) Conflicting statutes must yield. Neither Google nor Facebook cite a single case which holds that federal privacy statutes are paramount to a criminal defendant's federal constitutional rights. Not one.

Moreover, as discussed below, Google's suggestion that the SCA need not yield to a criminal defendant's federal constitutional rights because the records can be obtained by the prosecution is without merit. (Google Br. pp. 2, 14, 15.)

**III. GOOGLE’S ARGUMENT THAT THIS COURT NEED NOT DECIDE WHETHER THE SCA MUST YIELD TO DEFENDANTS’ FEDERAL CONSTITUTIONAL RIGHTS BECAUSE ELECTRONIC RECORDS MAY BE OBTAINED FROM THE PROSECUTION, IS WITHOUT MERIT. NEITHER THE FOURTH AMENDMENT, PENAL CODE SECTION 1524, NOR *BRADY V, MARYLAND* PERMIT THE PROSECUTION TO ISSUE SEARCH WARRANTS TO OBTAIN EXCULPATORY EVIDENCE IN THE POSSESSION OF THIRD PARTIES**

Real parties assert that the SCA cannot be interpreted in a manner that precludes a superior court judge from reviewing social media records *in camera* prior to trial if necessary to obtain records from third parties a defendant needs to defend a case or cross-examine witnesses. Google contends that holders of electronic records should be exempt from responding to criminal defendants’ subpoenas. Instead, Google argues, the prosecution should procure the records from the providers and disclose exculpatory records it obtains pursuant to *Brady v. Maryland* (1963) 373 U.S. 83. If the prosecution fails to do so, the case should be dismissed the case or the testimony excluded. (Google Br. pp. 2, 14, 15.)

This argument reveals a fundamental lack of understanding of criminal and constitutional law. Google contends that the prosecution can issue subpoenas or search warrants to third party electronic record holders to obtain defense evidence pursuant to 18 U.S.C 2703. (Google Br. p. 14.) Petitioners contend that under *United States v Warshak* (6<sup>th</sup> Cir. 2010) 631

F.3d 266, 288 and *United States v. Hanna* (6<sup>th</sup> Cir. 2001) 66 F.3d 271, 288 fn 4, the SCA is unconstitutional insofar as it permits the government to procure a electronic records by subpoena and that a search warrant in compliance with the Fourth Amendment is required. (Answer Br. p. 8.) Google side steps the fact that the prosecution cannot be compelled to procure records for the defense under the Stored Communications Act (“SCA”) because the Fourth Amendment and Penal Code sections 1523, 1524 establish that the government can *only* get search warrants to obtain contraband or evidence that a felony has been committed, not to obtain exculpatory evidence or evidence that raises an affirmative defense for defendants. (Opening Br., p. 26.) Indeed, neither Google nor Facebook cite authority for their argument that the Fourth Amendment permits the government to issue search warrants on behalf of criminal defendants for exculpatory records.

Defendants, with the assistance of the superior court through the procedures set forth in Penal Code section 1326, are solely responsible for obtaining the evidence from third parties necessary to cross-examine witnesses or to prepare for trial. Moreover, it is well-settled that our system of justice is an adversarial one and defendant should not be compelled to disclose confidential work product or privileged

communications to the prosecutor, or to provide the information necessary to prepare a statement probable cause for obtaining the warrant, or to justify the issuance of a subpoena, because such a procedure would run afoul of his or her right to effective assistance of counsel. If a criminal case “loses its character as a confrontation between adversaries, the constitutional guarantee [to effective assistance of counsel] is violated.” (*United States v. Chronic* (1984) 466 U.S. 648, 656.)

Because we have an adversarial system of justice, defendants’ Sixth Amendment right to effective assistance of counsel precludes defense counsel from providing defense work product or other privileged material to the prosecution in order to explain the relevance of the social media records sought in order to convince the prosecutor to issue a warrant or subpoena.

Moreover, as briefed in full by real parties, *Brady v Maryland*, *supra*, cannot be used to compel the prosecution to procure electronic records from third parties, such as holders of electronic records, because Facebook, Instagram, Twitter, and Google, are not members of the prosecution team and are not agents of the government. (Opening Br. pp. 24-26; see *In re Littlefield* (1993) 5 Cal.4th 122 [The prosecution has no general duty to seek out information from third parties that might be

beneficial to the defense.] )

Thus, Google's proposed remedy to avoid the constitutional issues fails because there is zero authority for the proposition that the prosecution can be forced to procure from third parties exculpatory evidence that defendants need to prepare for trial.

**IV. GOOGLE'S CONTENTION THAT THE REMEDY IS TO FORCE THE GOVERNMENT TO DISMISS CRIMINAL CASES IF THEY DO NOT PROVIDE EXCULPATORY ELECTRONIC RECORDS TO THE DEFENSE IS WITHOUT MERIT BECAUSE, UNLIKE CLASSIFIED STATE SECRETS, ELECTRONIC RECORDS ARE HELD BY THIRD PARTIES. THE GOVERNMENT CANNOT BE COMPELLED TO PROCURE RECORDS FOR THE DEFENSE IN THE POSSESSION OF THIRD PARTIES**

Google contends that rather than force providers to comply with a subpoena or litigate whether the SCA should yield to a defendant's federal constitutional rights, the prosecution should be forced to dismiss a case, or suffer an adverse evidentiary ruling, if they do not procure electronic records from a third party provider that a criminal defendant needs for trial. (Google Br.pp. 14-15.) Again, Google misses the mark. Unlike the classified information at issue in *Jencks v. United States* (1957) 353 U.S. 657, and *General Dynamics Corp v. United States* (2011) 563 U.S. 478, the confidential records at issue here are in the hands of third parties, not the government. Therefore, California courts cannot penalize the prosecution for failure to procure defense evidence from third parties, it has no authority

to obtain in the first place.

As discussed in Section III, the government has no authority whatsoever issue a search warrant to compel a third party to produce exculpatory evidence to the defense. Under Fourth Amendment jurisprudence codified in Penal Code sections 1523 and 1524, search warrants can *only* be issued to obtain contraband or evidence that a felony has been committed. Warrants cannot be issued to procure exculpatory evidence for the defense. Moreover, the prosecution cannot be forced to procure records possessed by third parties under *Brady*. There is simply no authority whatsoever to support Google's position.

Furthermore, Google reliance on *Miller v. Superior Court* (1999) 21 Cal.4th 883, 901, is misplaced. (Google Br. pp. 3, 7.) In *Miller*, this Court held that the Newspersons' shield law, which immunizes newspersons from contempt sanctions for refusing to disclose a confidential source or unpublished material, must give way to a conflicting federal constitutional right of a criminal defendant. (*Id.* at 891.) The prosecution's due process right under Article 1 section 29, of the California Constitution did not conflict with the Newspersons' shield law, which is also grounded in the California Constitution. Because the prosecutor's due process right was not grounded in the federal constitution, it could not compel information



protected by the Newspersons' shield law. (*Id.* at 883-900.) Because real parties' fair trial rights are grounded in the federal constitution, *Miller* supports defendants' position, not Google's.

**V. GOOGLE FAILS TO ADDRESS HOW A WITNESS CAN BE COMPELLED TO IDENTIFY HER SOCIAL MEDIA ACCOUNTS AND TO CONSENT TO THE RELEASE OF HER ELECTRONIC RECORDS WHEN THE WITNESS HAS ASSERTED HER FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION**

Google contends that the SCA need not yield to criminal defendants' federal constitutional rights because account holders can simply be ordered to consent to the release of their records. (Google Br. p. 12.) Google cites numerous civil cases which are inapt because those cases do not involve litigants who are protected by a panoply of federal constitutional rights as are criminal defendants. Moreover, these cases do not address how deceased account holders or witnesses who assert their Fifth Amendment privilege can be forced to consent. As the respondent court correctly noted in the instant case, Reneesha Lee, could not be compelled to identify her social media accounts nor consent to the release of her electronic records because of her Fifth Amendment privilege against self-incrimination. (Petitioners' Appendix to Exhibits, Supplemental Exhibit V, pp. 286, 287.) Moreover, forcing witnesses to consent is not good policy in criminal cases given the important constitutional rights at stake in conjunction with the

reality that witnesses can and will simply refuse to cooperate even if held in contempt of court.

Similarly, even if decedent in a criminal case was prescient enough to appoint someone as their online representative upon their death - likely a tiny percentage - these estate holders also cannot be compelled to consent to the release of a decedent's electronic records. They can and will simply refuse to cooperate. Because of the important constitutional rights at stake, criminal defendants must have the ability to compel disclosure when account holders or their representatives refuse to cooperate like witness Reneesha Lee did in the trial of the juvenile codefendant. (AE pp. 196-197.)

**VI. SINCE GOOGLE, FACEBOOK, INSTAGRAM, AND TWITTER PROVIDE THEIR USERS' ELECTRONIC RECORDS TO LAW ENFORCEMENT AND TO THIRD PARTIES FOR THE PURPOSES OF TARGETING ADVERTISEMENTS FOR FINANCIAL GAIN, THEY MUST ALSO PROVIDE CRIMINAL DEFENDANTS WITH ELECTRONIC RECORDS WHEN A SUPERIOR COURT ORDERS THEM TO DO SO FOLLOWING AN *IN CAMERA* HEARING, GIVEN THE IMPORTANT FEDERAL CONSTITUTIONAL RIGHTS AT STAKE**

Real parties appreciate that Facebook and Google have changed the way society communicates with their technology. But these technological advances do not erode a criminal defendant's federal constitutional rights because these rights are enshrined in the Constitution as the bedrock of our

criminal justice system. Google and petitioners are in the business of collecting and storing electronic information and must respond to defense subpoenas the same as other holders of confidential records do pursuant to the procedures set forth in Penal Code section 1326. There is no innovation exception to the statute nor to the federal constitution which establishes that confidential records must be disclosed to the defense, following a superior court's *in camera* review, if such disclosure is necessary to a fair trial.

Google's Privacy Policy makes it clear that they disclose electronic information about their users activity on their site, and on the internet, to third parties for the purpose of targeting advertisements.<sup>2</sup> Similarly,

---

<sup>2</sup> Google's Privacy Policy states as follows in pertinent part:

Cookies and similar technologies

We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites.

In addition to collecting their customers' browsing history, Google

Facebook's Data Use Policy reveals that it also shares users' electronic data with third parties to target advertisements.<sup>3</sup> Instagram makes it crystal

---

reads user emails and shares that information with Google's advertising partners, to target users' advertisements:

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.

(Google's Privacy Policy: Reviewed by author on May 26, 2016:  
<https://www.google.com/policies/privacy/>)

<sup>3</sup> Facebook's Data Use Policy provides the following in pertinent part:

Sharing With Third-Party Partners and Customers

We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world.

Here are the types of third parties we can share information with about you:

Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only). We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their

clear that their users essentially have no rights to the electronic data they post. In fact, in Instagram’s Terms of Use states that by using their site, users “hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to use the Content that you post on or through the Service, subject to the Service’s Privacy Policy.” (Instagram Privacy Policy. Reviewed by author on May 26, 2016: <https://help.instagram.com/478745558852511>.) Instagram also discloses users’ electronic information to the third-parties to target advertisements.<sup>4</sup> Twitter also provides users’ electronic data to target ads

---

ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to these partners to help them understand their audience or customers, but only after the advertiser has agreed to abide by our advertiser guidelines.

Vendors, service providers and other partners. We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them. (Facebook’s Data Use Policy; Reviewed by author May 26, 2016: [https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy).)

<sup>4</sup> Item No. 3 of Instagram’s Privacy Policy States as follows:

Parties with whom we may share your information:

based upon browsing history.<sup>5</sup>

---

We may share User Content and your information (including but not limited to, information from cookies, log files, device identifiers, location data, and usage data) with businesses that are legally part of the same group of companies that Instagram is part of, or that become part of that group ("Affiliates"). Affiliates may use this information to help provide, understand, and improve the Service (including by providing analytics) and Affiliates' own services (including by providing you with better and more relevant experiences). But these Affiliates will honor the choices you make about who can see your photos.

We also may share your information as well as information from tools like cookies, log files, and device identifiers and location data, with third-party organizations that help us provide the Service to you ("Service Providers"). Our Service Providers will be given access to your information as is reasonably necessary to provide the Service under reasonable confidentiality terms.

We may also share certain information such as cookie data with third-party advertising partners. This information would allow third-party ad networks to, among other things, deliver targeted advertisements that they believe will be of most interest to you. (Facebook's Privacy Policy, Reviewed by author on May 26, 2016; <http://instagram.com/legal/privacy/> )

<sup>5</sup> Twitter's Privacy Policy states as following in pertinent part:

Third-Parties and Affiliates:

Twitter uses a variety of third-party services to help provide our Services, such as hosting our various blogs and wikis, and to help us understand and improve the use of our Services, such as Google Analytics. These third-party service providers may collect information sent by your device as part of a web page request, such as cookies or your IP address. Third-party ad partners may share information with us, like a browser cookie ID, website URL visited, mobile device ID, or cryptographic hash of a common account identifier (such as an email address), to help us measure and tailor ads.

If Google and petitioners make billions of dollars storing communications, and provider their users information to advertisers, then they must respond to subpoenas in criminal cases the same as every other holder of confidential records, such as hospitals, telephone companies, banks, and private employers. Any burden placed on Google and Facebook because they have to respond to subpoenas pales in comparison to the billions they earn collecting electronic data, as well as the importance of affording criminal defendants the right to a fair trial.

Real parties do not seek encrypted records. If Google and providers are handing over electronic records to law enforcement, and providing their customers' electronic records to third parties to target advertisements, it is absurd to suggest the criminal defendants who face life and death sentences,

---

For example, this allows us to display ads about things you may have already shown interest in off of our Services. If you prefer, you can turn off tailored ads in your privacy settings so that your account will not be matched to information shared by ad partners for tailoring ads. Learn more about your privacy options for tailored ads here and about how ads work on our Services here. We may also receive information about you from our corporate affiliates in order to help provide, understand, and improve our Services and our affiliates' services, including the delivery of ads.

(Twitter Privacy Policy as of May 26, 2016:  
<https://twitter.com/privacy?lang=en>)

....