UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

FACEBOOK, INC.,

Defendant.
_____/

CASE NO.: 19-cv-2184 (TJK)

BRIEF OF THE CENTER FOR THE LEGALIZATION OF PRIVACY AS *AMICUS CURIAE* IN OPPOSITION TO CONSENT MOTION

Amy Lynn Peikoff (*Pro hac vice*)
THE CENTER FOR LEGALIZATION OF PRIVACY
3024 E. Chapman Ave. #129
Orange, CA 92869
Telephone: (714) 409-8275
legalizeprivacy@icloud.com

Stephen R. Klein (Bar No. 177056)
STATECRAFT PLLC
1629 K Street NW, Suite 300
Washington, DC 20006
Telephone: (202) 804-6676
steve@statecraftlaw.com
Local counsel to amicus curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Local Civil Rule 7(o)(5) and Federal Rules of Appellate Procedure 29(a)(4), 32 and 26.1, to enable this Court to evaluate possible disqualification or recusal the undersigned counsel for the Center for the Legalization of Privacy certifies that it has no parent corporation and no publicly held corporation owns any stock in it.

/s/ Amy Peikoff
Amy Lynn Peikoff

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Treatises

STATEMENT OF INTEREST OF *AMICUS CURIAE*

The Center for the Legalization of Privacy ("CLP") is a public interest legal organization dedicated to education about and promotion of the proper legal protection for privacy, based on common-law rights to property and contract. A primary focus of CLP is the problem of the "third-party doctrine," which is implicated by the proposed settlement in a manner that threatens the privacy of Facebook users vis-à-vis the government.

No party's counsel authored this brief in whole or in part, no party or party's counsel contributed money intended to fund the preparation of this brief, and no person other than the Center for the Legalization of Privacy, its members or counsel contributed money intended to fund the preparation of this brief.

ARGUMENT

Should an individual lose the protection of our Fourth Amendment's warrant requirement simply because he or she shares information, for a limited purpose, on Facebook? CLP believes this issue is raised by the Stipulated Order currently before this Court. Dkt. 2-1. Given the procedural posture of this case, in which "Defendant and Plaintiff waive all rights to appeal or otherwise challenge or contest the validity of this Stipulated Order", *id.* at 2, CLP believes it is important that this issue be addressed before the order is made final. In particular, CLP believes that the order, as written, could be reasonably interpreted to grant both the Federal Trade Commission and the Department of Justice, the latter of which has the "same rights as the Commission" to request a wide range of documents from Facebook, warrantless access to Facebook user data. *Id.* at 4. Regardless of any other issues that may exist with the Stipulated Order—issues beyond the scope of CLP's mission of improving legal protection for privacy—CLP believes it is both unreasonable and unjust to create such a risk to Facebook user privacy under the guise of protecting it. Moreover, as will be explained in this brief, doing so is legally

invalid, particularly after the Supreme Court's decision last year in *Carpenter v. United States*. 138 S.Ct. 2206 (2018). Accordingly, this Court should not approve the Stipulated Order until these issues are clarified. If CLP's interpretation of the provisions of the Stipulated Order is correct, the Court should deny the Order.

I. The Stipulated Order, as Written, Can be Reasonably Interpreted to Grant the Federal Trade Commission and the Department of Justice Warrantless Access to Facebook User Data

The Stipulated Order gives the Department of Justice "the same rights" as the Federal Trade Commission to request a wide range of documents, as provided for under other Parts of the Order. Dkt. 2-1 at 4. Accordingly, wherever the Order can be reasonably interpreted to grant the Commission warrantless access to Facebook user data, the Department of Justice may also be granted such access.

First, CLP notes that the Stipulated Order appears to give Facebook permission to retain metadata associated with data that a User deletes:

> If a User deletes an individual piece of Covered Information but does not delete his or her account, nothing in this paragraph shall be construed to require deletion or de-identification of metadata (*e.g.*, logs of User activity) that may remain associated with the User's account after the User has deleted such information.

Id. at 14. Per this language, unless a Facebook user decides to delete his or her entire Facebook account, and forgo the benefits of having such an account, such metadata, much of which could be personal in nature, is potentially subject to a request from the Commission or the Department of Justice, as provided in the Order's subsequent provisions.

In addition, although the Stipulated Order specifies that Facebook shall not share with a "Covered Third Party . . . any telephone number that Respondent has identified through its source tagging system as being obtained from a User . . . for the specific purpose of enabling an account security feature designed to protect against unauthorized account access", government

agencies are not encompassed by the Order's definition of "Covered Third Parties". *Id.* at 11, 15. Accordingly, Facebook users' phone numbers are also potentially subject to request from both the Commission and the Department of Justice.

CLP also notes that, while the Stipulated Order contains robust safeguards for the retention, use and sharing of "Covered Information"—in particular, facial recognition data—none of these robust safeguards apply, per the terms of the Order, to the sharing of such Information or data with government agencies. Such agencies are neither "Covered Third Parties" nor "Facebook-owned affiliates". *Id.* at 19.

Per the terms of the Stipulated Order, it is not clear that the required "Quarterly Privacy Review Report" would or should contain any identifiable Facebook User data, as the report is to be prepared by Facebook's Designated Compliance Officer(s). *Id.* at 18–19. The "Independent Privacy Program Assessment" required by Part III of the Order, however, could possibly contain such identifiable data and, moreover, the Order requires that "all documents *relevant* to each Assessment" be retained for five (5) years and be furnished to the Commission (also, presumably the Department of Justice) "within ten (10) days of receipt of a written request." *Id.* at 20 (emphasis added). Note that the selection and appointment of the "Assessor" is, per the Stipulated Order, subject to the approval of both the Associate Director for Enforcement for the Bureau of Consumer Protection of the Federal Trade Commission and the Department of Justice. *Id.* at 4, 20–21. Moreover, "[e]ach Assessment must . . . identify specific evidence (including, but not limited to, documents reviewed, *sampling and testing performed*, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings." *Id.* at 21 (emphasis added). A reasonable interpretation of this language encompasses specific,

identifiable Facebook user data—if not in the Assessment itself, at least in the "documents relevant to each Assessment" that are also required to be turned over to the Commission (or to the Department of Justice) upon written request. That this Assessment is to be performed by someone appointed at the pleasure of the same two government agencies that are entitled to request that data is another reason for concern.

The most concerning provisions of the order are contained in its last two substantive parts, "Recordkeeping" and "Compliance Monitoring". *Id.* at 19–20. The former requires that Facebook "create and retain" a record of "documents and information sufficient to show *each User's consent*" to any "Changes To Sharing of Covered Information." *Id.* at 27 (emphasis added). How else might Facebook demonstrate compliance with this provision except to submit, upon request, to either the Commission or the Department of Justice, specifically identifiable Facebook user data? Also note that recordkeeping, like the privacy assessment provision, requires that Facebook retain "[a]ll records necessary to demonstrate full compliance with each Part of this Order, including all submissions to the Commission." *Id.* at 28.

Finally, in the compliance monitoring section, we see what might reasonably be deemed necessary to "demonstrate full compliance" with the order. *Id.* at 28. Per its terms, Facebook is required to: "Within fourteen (14) days of receipt of a written request from a representative of the Commission . . . submit additional compliance reports *or other requested information*. . . ." *Id.* (emphasis added). In addition, that subpart provides that "[t]he Commission is also authorized to obtain discovery, *without further leave of court*, using [among other methods] telephonic depositions. . . ." *Id.* (emphasis added). Subpart B of this section makes it clear that "the Commission [and so also the Department of Justice] is authorized to communicate directly with [Facebook]." *Id.* It does not take much creativity to imagine someone from the Commission (or

the Department of Justice) calling Facebook to obtain "other requested information" per the terms of the Stipulated Order, and for that information to contain specifically identifiable Facebook user data. And per the terms of the Order, this arrangement is contemplated to persist for at least 20 years. *Id.*

II. The Stipulated Order, Insofar as it Permits Warrantless Access to Facebook User Data, Rests on an Unjustified Assumption about the Validity and Scope of the "Third-Party Doctrine."

As shown in the previous section, the Stipulated Order would in all likelihood provide the Commission and the Department of Justice warrantless access to Facebook User data. Any legal justification for permitting this must rest on the so-called "third-party doctrine," the validity and scope of which has been called into question in the last several years, most notably by the Supreme Court in *Carpenter v. United States*. 138 S.Ct. 2206 (2018). CLP welcomes this development because, as will be argued in this section, the doctrine, insofar as it permits justifiable government action, is superfluous.

The third-party doctrine (in its undiluted form) says that, once we share information with a third party, the Fourth Amendment warrant requirement no longer applies. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *U.S. v. Miller*, 425 U.S. 435, 443 (1976). In other words, the government may obtain whatever information we share with third parties, without presenting a warrant based on probable cause and particularized suspicion. All data that you share with anyone, in essence, can be turned over to the U.S. government—unless there's a statute protecting it. The danger of this could be no more apparent than in the proposed settlement here, potentially turning Facebook into an open information pipeline to the Commission and the Department of Justice.

Even when a statute or other law does protect data from government's prying eyes, it typically requires the government to establish something less than probable cause and

particularized suspicion.[1] Moreover, once the government has obtained assorted pieces of information about a citizen, all it takes these days is a president's "pen and phone" to combine databases across alphabet-agency lines. With settlements as broad as the Stipulated Order, all of the data about one's daily activities may soon be collected in one place, accessible to any politician, bureaucrat—or hacker.

The ominous implications of this doctrine were not always apparent. In fact, it made a lot of sense when it was first formulated in the so-called "secret agent cases." *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH L. REV. 561, 567–68 (2009). Think of Tony Soprano divulging information about the operation of his illegal businesses to a government informant, and the informant later turning that information over to a prosecutor, who uses it to indict and prosecute Soprano. The fact that the Fourth Amendment does not protect the Tony Sopranos of the world in situations like this probably does not bother most people. But then, in the 1970s, the doctrine was, with almost no justification, deemed to apply not only to mafia dons, but also to any citizen who shares information with third parties in the ordinary course of doing business or living life.

Alarm bells did not go off immediately after the Court extended the doctrine into a non-criminal context. Back in the 1970s, citizens did not share nearly as much data with third parties and, moreover, the government seemed to be accessing only the tiniest bit of the most innocuous metadata in order to catch and prosecute criminals. But gradually that changed. Many Americans learned just how much it changed during the so-called "Snowden revelations" in 2013. Edward

---

[1] The standard used in the Stored Communications Act, as amended in 1994, for example, is that the Government must offer "specific and articulable facts showing that there is reasonable grounds to believe" that the information sought is "relevant and material to an ongoing criminal investigation." 18 U. S. C. § 2703(d).

Snowden revealed, for example, that the National Security Agency had been continuously collecting phone record metadata of all Verizon customers for several years, and that the NSA was accessing e-mail and other forms of Internet communication—including Skype voice and video communications—via a secret program called Prism. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 6, 2013, *available at* https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN, June 6, 2013, *available at* http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

Following Snowden's revelations there have been attempts to chisel away at the third-party doctrine, or to limit some of what most people consider to be the most egregious invasions it permits. The most significant thus far, in terms of litigation, was *Carpenter v. United States*, decided by the Supreme Court last year. 138 S.Ct. 2206. The case concerned the application of the third-party doctrine to Cell Site Location Information (CSLI) collected by service providers. *Id.* at 2211–13. Petitioner Carpenter argued that, unlike other data shared with a third party, longer-term cell phone location data (in his case collected for 127 days) is something in which one has a "reasonable expectation of privacy." *See Katz v. U.S.*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). A majority of the Court, in an opinion written by Justice Roberts, agreed with Carpenter: "[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search." *Carpenter*, 138 S.Ct. at 2217.

As we'll see more fully in the next section, the holding in *Carpenter* raises an important issue: how can one draw even a semi-bright line, much less one for which there is a principled rationale, after the Court's extension of the third-party doctrine to "ordinary business records" in *Smith* and *Miller*? How long is the "long term" over which one's data is collected before one's expectation of privacy becomes "reasonable" or "legitimate"? Why shouldn't all digital information be subsumed by the doctrine if analog information is? How sensitive is sensitive? What constitutes the "meaningful" sort of voluntary sharing, and why? And so on.[2]

The Supreme Court should have used the opportunity presented in *Carpenter* to overturn *Smith* and *Miller* and return the third-party doctrine to its original scope: sharing information with government agents in the course of criminal activity. *See, e.g.*, *U.S. v. White*, 401 U.S. 745 (1971). Although the lack of a bright line beyond this scope is one sign of a problem, there's a much more important one: in *Miller*, the first case in which the Court extended the doctrine beyond the criminal context, it never justified its decision to do so.[3]

Such justification is due because, although one can hardly expect to retain a legitimate expectation of privacy in information shared with third parties in the course of *criminal* activity, the same does not hold true with respect to Americans sharing information during normal activities of daily life. The distinction lies in the common-law doctrine of *illegal contract*, which says that courts will not uphold any agreement the purpose of which is to achieve an illegal end.

---

[2] Justice Kennedy, in his dissent, makes precisely this sort of argument. He would not, however, take it to the logical conclusion that CLP does. *See Carpenter*, 138 S.Ct. at 2232–33.

[3] In *Miller,* the only thing the Court offered by way of justification was to note that the Bank Secrecy Act, a useful tool for investigating criminal activity, required the keeping of the records at issue. 425 U.S. at 443. Ironically, the Court later noted in *Smith* that the government should not be able, via regulation or otherwise, to destroy citizens' "reasonable expectation of privacy." 442 U.S. at 740 n.5.

See 5 SAMUEL WILLISTON & RICHARD A. LORD, A TREATISE ON THE LAW OF CONTRACTS § 12:1 (4th ed. 2009).

If an American makes an "arrangement" with a "business associate" to commit a crime, it's unenforceable—including any promise made, as part of the arrangement, to keep it a secret. But simply to share things on—and therefore with—Facebook, is not to engage in activity aimed to achieve a criminal purpose. Therefore, such sharing (other than, perhaps, sharing something publicly on Facebook) should not be deemed a renunciation of Fourth Amendment protection, regardless of what a user's "expectation" might be.

Using a model for the legal protection of privacy based upon common-law rights to property and contract, CLP's president has argued that the doctrine of illegal contract makes the third-party doctrine, as originally conceived, superfluous. *See* Amy L. Peikoff, *Of Third-Party Bathwater: How to Throw Out the Third-Party Doctrine While Preserving Government's Ability to Use Secret Agents*, 88 ST. JOHN'S L. REV. 349 (2014), *available at* https://scholarship.law.stjohns.edu/lawreview/vol88/iss2/3. But the model explicated in that article need not be adopted in total to be useful. One need only recognize that common-law doctrine provides courts with a principled reason—one firmly rooted in our legal traditions—to limit the scope of the third-party doctrine to criminal contexts, and to stop treating all Americans like criminals.

This approach would also be consistent with the property-based conception of the Fourth Amendment that Justice Scalia began developing in the years before his death, a development continued by some of the Justices in *Carpenter*.

III. The Assumption Made in the Stipulated Order is Particularly Unjustified in Light of *Carpenter v. United States*

The Supreme Court did not use the opportunity presented in *Carpenter* to reconsider *Smith* and *Miller*. Instead, the majority declined to extend *Smith* and *Miller* to apply to "the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls," given the records' "unique nature." *Carpenter*, 138 S.Ct. at 2214, 2217. The Court's reasoning rests on an analogy to the 2012 case, *United States v. Jones*, but does so only insofar as the two cases involve similar kinds of data records. *See* 132 S.Ct. 945 (2012). The majority explicitly declined to adopt the property-based approach that had been revived by the late Justice Scalia in *Jones* and other cases: "Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Carpenter*, 138 S.Ct. at 2217. It was the "product of a search," not because of specific actions performed, with respect to specific types of entities, in order to obtain the data, but rather because of the type of data obtained. *Id.*

Even this pragmatic majority holding in *Carpenter* is enough to call into question the reasonableness of the assumption made by the Stipulated Order in the instant case. True, one could argue that the sharing users do on Facebook is voluntary in a way that the sharing of location data with one's cellular service provider is not. *See id.* at 2220. But the data one knowingly, voluntarily shares on and with Facebook is not all the data Facebook collects and retains about users. Recall that even the Stipulated Order refers to metadata associated with data that a Facebook user has chosen to delete, and specifically grants permission to (requests?) Facebook to retain such metadata. Dkt. 2-1 at 14. Moreover, whatever Facebook data might be said to lack in the "voluntariness of sharing" prong, it more than makes up for in the "exhaustive

chronicle" of "personal information" prong. *Carpenter*, 138 S.Ct. at 2219. Ask any of Facebook's 1.56 billion daily active users. *See* Mariel Soto Reyes, *Scandals and teen dropoff weren't enough to stop Facebook's growth*, BUSINESS INSIDER, Apr. 26, 2019, https://www.businessinsider.com/facebook-grew-monthly-average-users-in-q1-2019-4.

The majority in *Carpenter* at least declined to extend *Smith* and *Miller* to certain other types of data not originally encompassed by those holdings, thereby affirming that the doctrine is limited in scope. Unfortunately, the Court did so by focusing on the type of data, and the voluntariness of its sharing, rather than on the validity of the means by which it was obtained. The latter is what Scalia was inviting future Justices to do when he wrote the majority opinion in *United States v. Jones*. And it is what other Justices in *Carpenter* chose to do, to varying degrees, in their dissents.

Justice Kennedy, in his dissent, said that while a property interest in the information at issue is not dispositive, it is relevant. Relying, perhaps ironically, on *Smith* and *Miller*, he wrote, "individuals often have greater expectations of privacy in things and places that belong to them, not to others." *Carpenter*, 138 S.Ct. at 2229 (Kennedy, J., dissenting). He noted that customers' contracts with their cellular service providers give them little control over the records, records created by the companies: "Customers do not create the records; they have no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed. Even their right to request access to the records is limited." *Id.* He rejected the majority's pragmatic, "balancing test" approach to the doctrine, insofar as it relies upon the personal nature of the information, or the degree of voluntariness of the sharing: "the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in [*Miller and Smith*] lacked a reasonable expectation of privacy." *Id.* at 2232. And he

said that, even using that sort of balancing test, the majority applied it incorrectly: "[T]he Court errs . . . when it concludes that cell-site records implicate greater privacy interests—and thus deserve greater Fourth Amendment protection—than financial records and telephone records." *Id.* In *Carpenter*, then, where the records in question were not owned, created, or controlled by the petitioner—i.e., were not the modern equivalent of petitioners' "papers and effects"—Justice Kennedy would hold that a subpoena is sufficient. *Id.* at 2228. In conclusion Kennedy noted that the majority opinion left open questions like the one raised here, in which a government agency stands to collect a "new form[] of information" using "processes that deviate from traditional warrant procedures." *Id.* at 2235. One can imagine Kennedy being sympathetic to CLP's argument here, given that Facebook user data, most of which is created and uploaded by the users themselves, is the perfect modern equivalent of an individual's "papers and effects." Moreover, Facebook's Terms of Service give users considerable control over their data. *See Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php (last accessed Oct. 13, 2019).

In his dissent Justice Thomas categorically rejected the *Katz* "reasonable expectation of privacy" test, which has been used by the Court for decades to determine whether a "search" occurred within the meaning of the Fourth Amendment.

> The more fundamental problem with the Court's opinion, however, is its use of the "reasonable expectation of privacy" test, which was first articulated by Justice Harlan in *Katz* . . . . The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence.

Id. at 2236 (Thomas, J., dissenting) (internal citations omitted). For Thomas, the issue in the case is not "'whether' a search occurred," but rather "*whose* property was searched." *Id.* at 2235. And he thinks the CSLI at issue in *Carpenter* was simply not Carpenter's property: "He did not create

the records, he does not maintain them, he cannot control them, and he cannot destroy them. Neither the terms of his contracts nor any provision of law makes the records his. The records belong to MetroPCS and Sprint." *Id.*

After an historical critique of the *Katz* test,[4] Thomas turns to Carpenter's argument that the cell-site records at issue in *Carpenter* were his "papers." *Carpenter,* 138 S.Ct. at 2242. He notes that Carpenter does not attempt to argue on the basis of "property, tort or contract law," any of which he would have considered to be valid. *Id.* Instead, Carpenter based his argument on a statute, the federal Telecommunications Act of 1996, and finds Carpenter's interpretation of that act unpersuasive. *Id.* at 2242–43. "[T]he Telecommunications Act is insufficient because it does not give Carpenter a property interest in the cell-site records." *Id.* at 2242. Justice Thomas concludes with a thorough explanation as to why the *Katz* test was not only wrong, from an historical perspective, but also unworkable, and counts *Carpenter* among those cases in which the Court has used the test to "expand the Fourth Amendment beyond its original scope." *Id.* at 2246. In his view, errors in "either direction"—whether expanding or narrowing the amendment's original scope—"should not [be] tolerate[d]". *Id.*

CLP would respectfully encourage Thomas to consider the common law of contract as an additional basis for the legal protection of privacy—under the Fourth Amendment and elsewhere—regardless of whether a particular contract creates, whether explicitly or implicitly, a property interest in the records or information at issue. Is not a contract an "effect" that individuals today use every day so as to protect their privacy, while still enjoying the life-

---

[4] A critique with which CLP is sympathetic in many respects, despite it being rooted in Originalism. *See* TARA SMITH, JUDICIAL REVIEW IN AN OBJECTIVE LEGAL SYSTEM 145–62 (2015).

enhancing technologies now made available to us? Or perhaps it is the data we allow third parties to collect about us that are the "effects," as Justice Gorsuch suggests. *Id.* at 2269 (Gorsuch, J., dissenting). But even if Thomas were not persuaded of this, it is reasonable to think that he might treat Facebook user data differently than the CSLI at issue in *Carpenter*, depending on his reading of Facebook's Terms of Service.

Justice Alito parts ways with the *Carpenter* majority on two main issues. First, he notes there is a "basic distinction between an actual search (dispatching law enforcement officers to enter private premises and root through private papers and effects) and an order merely requiring a party to look through its own records and produce specified documents." *Id.* at 2247 (Alito, J., dissenting). Only the former, Alito says, requires a showing of probable cause, because it "intrudes on privacy far more deeply" than a subpoena or other order to produce documents. *Id.* Second, he says it is "revolutionary" to "allow[] a defendant to object to the search of a third party's property." *Id.* The order in *Carpenter*, he wrote, was "the functional equivalent of a subpoena for documents," *id.* and, after reviewing the history of compulsory production of documents he concludes, "Neither this Court nor any of the parties have offered the slightest bit of historical evidence to support the idea that the Fourth Amendment originally applied to subpoena *duces tecum* and other forms of compulsory process." *Id.* at 2252.

Even the modern doctrine of the Fourth Amendment as applied to subpoenas, he argues, will not help Carpenter. Citing *Oklahoma Press Publishing Company v. Walling*, he writes, "the Fourth Amendment regulates the compelled production of documents, but less stringently than it does full-blown searches and seizures." *Carpenter*, 138 S.Ct. at 2254 (Alito, J., dissenting) (citing 327 U.S. 186, 202 (1946)). And applying that less stringent standard in *Carpenter*, Alito argues that the standard required by the Stored Communications Act is sufficient. *Id.* at 2255.

Regarding what he sees as the *Carpenter* majority's second error—allowing petitioner Carpenter to object to the search of a third person's property—Alito echoes the dissents of Justices Kennedy and Thomas:

> [Here] Carpenter indisputably lacks any meaningful property-based connection to the cell-site records owned by his provider. Because the records are not Carpenter's in any sense, Carpenter may not seek to use the Fourth Amendment to exclude them.

Id. at 2260.

What might Justice Alito think of the instant case? On the one hand, he mentions approvingly "document-production orders issued by administrative agencies," *id.* at 2247, and so he might think the sort of document production called for in the Stipulated Order is justified. On the other hand, he might agree with CLP that Facebook user data is often more comprehensive and personal than the CSLI at issue in *Carpenter* and also that the "property-based connection" users have to that data is much more "meaningful." *Id.* at 2260.

Justice Gorsuch's dissent could very well have been a concurrence. True, Gorsuch joined the other dissenters in criticizing *Katz* and its progeny, and he also joined them in looking for a property interest Carpenter might have in his cell-site records. *Id.* at 2264-67 (Gorsuch, J., dissenting). But while the other Justices failed to find or identify such an interest, Gorsuch thinks there is one. "It seems to me entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law." *Id*. at 2272. To show this, he analyzes §222 of the federal Telecommunications Act of 1996 in a way that departs from Justice Thomas's analysis, finding "substantial legal interests in this information, including at least some right to include, exclude, and control its use." *Id.* "Those interests," he concludes, "might even rise to the level of a property right." *Id.* Justice Gorsuch makes clear earlier in his opinion that it is not only statute that might give rise to a protectable interest under the Fourth Amendment:

> We know that if a house, paper, or effect is yours, you have a Fourth Amendment interest in its protection. But what kind of legal interest is sufficient to make something yours? And what source of law determines that? Current positive law? The common law at 1791, extended by analogy to modern times? Both? Much work is needed to revitalize this area and answer these questions.

Id. at 2268. In particular, CLP is hopeful that Justice Gorsuch, even on his Originalist approach, would consider CLP's argument here as an example of "[t]he common law at 1791, extended by analogy to modern times." *Id.* CLP is encouraged by Gorsuch's view that "the Court has never offered a persuasive justification" for the third-party doctrine, especially as his presentation of the doctrine's history begins with its unjustified expansion under *Miller* and *Smith*. *Id.* at 2263.

In fact, CLP would have been momentarily tempted to encourage Justice Gorsuch to adopt a concurring position—to use the property interest he believed existed to find that Carpenter had a "reasonable expectation of privacy"—even though, as he notes, Carpenter failed to "invoke the law of property, or any analogies to the common law," at the requisite times. *Id.* at 2272. Of course, had Gorsuch done so, he would have failed to encourage litigants to frame their demands for Fourth Amendment protection in terms other than the hopelessly pragmatic "reasonable expectation of privacy" test of *Katz*. *See* Amy L. Peikoff, *Pragmatism and Privacy*, 5 N.Y.U. J. L. & LIBERTY 638, 655–61 (2010). Gorsuch himself minces no words when it comes to *Katz*: "*Katz* has yielded an often unpredictable—and sometimes unbelievable—jurisprudence." *Carpenter*, 138 S.Ct. at 2266. So long as Facebook users asserted a protectable interest in their data, whether in terms of property or other common-law doctrines—or even an interest created by statute—it seems Justice Gorsuch would be sympathetic.

The understanding of the third-party doctrine proffered here by CLP—which asks only whether information is shared for a limited purpose within the context of a legally enforceable contractual arrangement—is something many Justices might be receptive to in a case like

Carpenter, as well as the instant case. But even if not, as argued above, *Carpenter* on its own terms raises the issue whether the assumption apparently made in the Stipulated Order—that it is permissible for Facebook to be required to hand over user data to government agencies, "without further leave of court"—is justifiable. Certainly many Facebook users believe they continue to own the data they create and share on and with the platform—even if they have given Facebook permission to use this data to sell them things, or to entice them and others to spend more time on Facebook. And if more Facebook users were aware of the implications of the Stipulated Order for the privacy of the information they've created and shared on and with Facebook, they would be arguing as CLP is here.

CONCLUSION AND RECOMMENDATION

CLP has a limited mission. Accordingly, this brief does not address other issues raised by the specter of government—as a "remedy" for legitimate concerns about the conduct of a private corporation with access to vast troves of personal data—taking control of said corporation in a way that would make George Orwell think he was reading *The Onion*.

CLP's mission is to "legalize privacy" generally: to allow individuals, once again, to use the tools the Common Law put at their disposal to create and protect states of privacy for themselves, according to their own tastes and preferences. An individual should not lose the protection of our Fourth Amendment's warrant requirement simply because he or she shares information, for a limited purpose, in order to enjoy any number of life-enhancing technologies now made available to us.

Full legalization of privacy will require, as argued above, that the third-party doctrine either be eliminated or narrowed to its original scope. CLP is aware that such a ruling by this Court would likely be overbroad given the narrow scope of the decision it's been asked to make. CLP urges, at least, that any final order approved by this court specify that no identifiable

Facebook user data be given to any government agent or agency—including the Commission, the Department of Justice, and anyone appointed at their pleasure (who are arguably de facto government agents)—without a warrant based on probable cause and particularized suspicion *regarding that individual user*. "Relevance" to the question of whether Facebook is or has been violating its contractual obligation to protect user privacy in a way that runs afoul of any number of FTC regulations, consent decrees, stipulated orders, etc., does not justify warrantless access to personal information about the individual citizens who are its customers. Not in a free country.

Amy Peikoff, counsel for CLP, respectfully requests permission to participate in any oral argument regarding the Stipulated Order to further address the third-party doctrine concerns and the egregious threat to privacy posed by this settlement.

Respectfully submitted,

The Center for the Legalization of Privacy

by counsel,

/s/ Amy Peikoff
Amy Lynn Peikoff (*Pro hac vice*)
THE CENTER FOR LEGALIZATION OF PRIVACY
3024 E. Chapman Ave. #129
Orange, CA 92869
Telephone: (714) 409-8275
legalizeprivacy@icloud.com

/s/ Stephen R. Klein
Stephen R. Klein (Bar No. 177056)
STATECRAFT PLLC
1629 K Street NW, Suite 300
Washington, DC 20006
Telephone: (202) 804-6676
steve@statecraftlaw.com
Local counsel to amicus curiae

CERTIFICATE OF COUNSEL

This brief complies with the page limitation established by Local Civil Rule 7(o)(4), because it contains 18 pages, exclusive of those parts of the brief exempted by Federal Rule of Appellate Procedure 32(f). This brief complies with the typeface requirements of Local Civil Rule 5.1(d) because it has been prepared in a 12-point font and double-spaced.

/s/ Stephen Klein
Stephen R. Klein

CERTIFICATE OF SERVICE

I CERTIFY that on October 15, 2019, I served the foregoing brief through the Court's electronic filing system which served a copy on all counsel of record.

/s/ Stephen Klein
Stephen R. Klein