# *Notes*

# Appealing to Reason-able Expectations of Privacy: Increasing Appellate Review Under ECPA

ANDREW TYLER OHLERT*

*The Snowden revelations of 2013 sparked widespread, public discussion about the amount of government surveillance performed on American citizens under the Foreign Intelligence Surveillance Act. This dialogue often sidesteps the Electronic Communications Privacy Act, however, which is the primary statute that governs the government's ability to obtain the electronic communications of everyday citizens. The vast majority of requests for information under ECPA are pursued ex parte, and often without notice to a targeted individual that the government has obtained her information. This secrecy regime leaves targeted individuals unable to oppose the government or appeal adverse decisions. Moreover, if a magistrate judge disagrees with the government and denies its request for an individual's information, the government can simply apply to other judges until a judge grants access to the information.*

*This Note examines the resulting lack of appellate precedent that has developed from a system where the government has no opposition, and American citizens have no opportunity to be heard. This Note suggests three solutions to increase opposition to the government and incentivize the development of binding, appellate precedent under ECPA.*

* J.D. Candidate, 2015, University of California Hastings College of the Law; B.S. in Computer Science, 2012, Virginia Tech. I would like to thank Professor Evan Tseng Lee for his invaluable assistance with this Note, as well as Susan Freiwald for inspiring this topic. I would also like to thank my Father for teaching me chess.

## Table of Contents

## Introduction

The Snowden revelations in June of 2013 recently revealed to the American public how extensively the U.S. government has engaged in widespread and mass surveillance.[1] Secret courts under the Foreign Intelligence Surveillance Act ("FISA") hear approximately 1000 secret cases a year.[2] But that number pales in comparison to the number of ex parte applications filed under the Electronic Communications Privacy Act ("ECPA") that seek to collect targeted online information of American citizens.[3]

A conservative estimate of sealed ECPA applications estimated that over 30,000 ECPA applications were filed to magistrate judges in 2006 alone.[4] And a survey of just five technology companies in the first six months of 2014 verifies that estimate.[5] During that time, Microsoft received 6919 requests for user information from the government, targeting 15,730 user accounts for information;[6] Google received a total number of 12,539 requests for user information, targeting 21,576 user accounts;[7] Yahoo! received 4865 total government requests, targeting 9752 user accounts;[8]

1. *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian, (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (discussing just one aspect of the National Security Agency's domestic surveillance program).

2. Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harv. L. & Pol'y Rev. 313, 313 (2012).

3. *Id.* at 315, 320–22.

4. *Id.* at 320–22; *see also* Tim Reagan & George Cort, Fed. Judicial Ctr., Sealed Cases in Federal Courts (2009), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf (providing the sealed case information on which Judge Smith based his estimations).

5. *See* Microsoft, Law Enforcement Requests Report 2014: January-June, 2014, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (last visited Aug. 5, 2015) [hereinafter Microsoft]; *see also* Apple, Report on Government Information Requests (Jan. 1–June 30, 2014), https://www.apple.com/privacy/docs/government-information-requests-20140630.pdf (last visited Aug. 5, 2015) [hereinafter Apple]; *Transparency Report*, Google, http://www.google.com/transparencyreport/userdatarequests/data/ (last visited Aug. 5, 2015) [hereinafter Google]; *Transparency Report: Government Data Requests*, Yahoo!, https://transparency.yahoo.com/government-data-requests/index.htm (last visited Aug. 5, 2015) [hereinafter Yahoo!]; *United States Information Requests*, Twitter, https://transparency.twitter.com/country/us (last visited Aug. 5, 2015) [hereinafter Twitter].

6. Microsoft, Law Enforcement Requests Report 2014: July-December, 2014, at 2, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/. The data contained within this Note focuses exclusively on requests for information made by the U.S. government.

7. Google, *supra* note 5, at 9. In the United States, Google received 8211 subpoenas, 165 pen register orders, 171 emergency disclosure requests, 3187 search warrants, 7 wiretap orders, and 798 "other" court orders. *Id.*

8. Yahoo!, *supra* note 5. Of these 4865 requests, Yahoo disclosed "content" information in 1157 requests, and it disclosed "non-content" information in 2887 requests. *Id.*

Apple received 789 requests targeting 1739 user accounts;[9] and Twitter received 1257 requests for account information targeting 1918 user accounts.[10] Together, these five technology companies alone received 26,369 requests in just six months. In 2013, these same companies received a combined total of 55,689 requests for account information targeting 128,005 user accounts.[11] But in spite of the incredible number of requests received by Internet Service Providers ("ISPs"),[12] there is almost zero guidance on the proper standards required under ECPA.[13]

This Note seeks to reinvigorate privacy law within the United States by increasing appellate review of ex parte ECPA applications and fostering an adversarial system that will encourage courts to develop binding law within the realm of privacy law. Part I discusses the statutory history of ECPA and explains how each branch of government has, thus far, failed to elaborate on the standards required under ECPA. Part II discusses ECPA's statutory structure to explain why courts have been unable to address the constitutional issues surrounding new technologies. Part III reviews existing case law under ECPA and the Fourth Amendment to demonstrate the lack of guiding precedent for lower courts. Part IV suggests three potential solutions to increase appellate review of ex parte ECPA orders, including that Congress allow courts to appoint a "Constitutional Advocate" to oppose the government in ex parte hearings under these statutes.[14] And Part V discusses the Article III standing implications that such a Constitutional Advocate would have to overcome.

## I. BACKGROUND OF ECPA

As it stands now, every branch of government has refused to elaborate on the standards required by the Fourth Amendment under ECPA. First, the executive branch has actively sought to expand its ability to gather

9. APPLE, *supra* note 5, at 5. These numbers only include the number of account requests and do not include National Security Letters or requests for device information.

10. TWITTER, *supra* note 5.

11. *See* MICROSOFT, *supra* note 5; s*ee also* GOOGLE, *supra* note 5, at 6–7; YAHOO!, *supra* note 5; APPLE, *supra* note 5; TWITTER, *supra* note 5.

12. For simplicity, this Note refers to Internet Service Providers ("ISPs"), but it is important to note that ECPA does not distinguish between ISPs and general Service Providers. *See* 18 U.S.C. § 2702(a) (2014). ECPA does state, however, that a "provider" is any person or entity that provides an "electronic communication service" or "computing service" to the public. *Id.* So, while Google or any other public provider of electronic or computing services would qualify as a "provider" limited by the statute, a private employer would not. *Id.*

13. For example, it is often unclear whether subsections of ECPA or the Fourth Amendment require probable cause in the context of the specific technology at issue. *See infra* Part III.A.

14. Intelligence Oversight and Surveillance Reform Act, S. 1551, 113th Cong. § 402(b) (1st Sess. 2013) (enacted) (establishing within the judiciary a Constitutional Advocate to review each application submitted to and decision of the Foreign Intelligence Surveillance Court ("FISA Court"), and authorizing the advocate to participate in FISA Court proceedings or a petition review pool proceeding and to appeal any decisions of such bodies).

information and avoid judicial review.[15] A decision by a magistrate judge is not binding on other magistrate judges, and thus, if one magistrate denies the government's request, the government can simply apply to another magistrate who might be more sympathetic to its case.[16] Given that the executive branch is "chiefly responsible for law enforcement,"[17] it makes sense that prosecutors "tend to gravitate toward a judge who is known to view their requests less critically."[18] And because the executive branch has the flexibility to apply to various judges that endorse its own interpretation of the law, it would understandably avoid appealing cases and risking the establishment of contrary binding precedent by an appellate judge.[19]

Second, while Congress has amended ECPA five times,[20] only one of those amendments—the Communications Assistance for Law Enforcement Act ("CALEA") of 1994[21]—has actually attempted to modernize the standards that should apply to information under ECPA.[22] ECPA is no

15. *See, e.g.*, *In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 580 n.5 (E.D.N.Y. 2010), *rev'd* (Nov. 29, 2010) (discussing *Hearing on Elec. Commc'ns Privacy Act Reform & the Revolution in Location Based Techs. & Servs. Before the Subcomm. On the Constitution, Civil Rights, and Civil Liberties*, S. Comm. on the Judiciary, 111th, Cong. (statement of Stephen Wm. Smith, U.S. Mag. J., at 3–7 & n.14) (June 24, 2010), *available at* http://judiciary.house.gov/_files/hearings/pdf/Smith100624.pdf) [hereinafter *ECPA Reform Committee*]).

16. Smith, *supra* note 2, at 328; *see also* RLJCS Enters. Inc. v. Prof'l Ben. Trust Multiple Emp'r Welfare Ben. Plan & Trust, 487 F.3d 494, 499 (7th Cir. 2007).

17. Stephen Wm. Smith, *Standing Up for Mr. Nesbitt*, 47 U.S.F. L. REV. 257, 258 (2012).

18. *ECPA Reform Committee*, *supra* note 15, at 12.

19. *See infra* Part II.C.

20. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510–2522 (2014), *available at* https://it.ojp.gov/default.aspx?area=privacy&page=1285 (last updated July 30, 2013) (discussing the history of amendments to ECPA).

21. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, § 103(a)(2)(B), 108 Stat. 4279, 4281 (1994) (codified at 47 U.S.C. §§ 1001–1021 (2014)). The Communications Assistance for Law Enforcement Act ("CALEA") amended the Stored Communications Act ("SCA") to differentiate between customer information and "record[s] or other information . . . (not including the contents of communications)." 18 U.S.C. § 2703(c)(1)–(2) (2014). To obtain customer information, CALEA simply required the government to obtain an administrative subpoena. *Id.* § 2703(c)(2). But to obtain "other information," CALEA required the government to obtain a warrant pursuant to the Federal Rules of Criminal Procedure, a § 2703(d) court order, or the consent of the target. *Id.* § 2703(c)(1); *see also id.* § 2703(d); Fed. R. Crim. P. 41(d)(1). CALEA also prohibited the use of pen registers to obtain phone location data. 47 U.S.C. § 1002(a)(2)(B) (2014).

22. Other amendments have failed to address other common critiques of ECPA. For example, the SCA allows law enforcement officials to obtain e-mails stored for more than 180 days, at which point the e-mail is considered abandoned. 18 U.S.C. § 2703(a). When ECPA was enacted, it was routine for service providers to only store e-mail until it could be transmitted to the recipient, and it made sense that the e-mail could be collected if it was still on the ISP's servers after 180 days because that delay signaled that the recipient had essentially abandoned the e-mail. A common criticism of the SCA, which has remained unaddressed by Congress, is that this distinction is outdated because modern e-mail services, such as Gmail or Hotmail, will now store e-mails indefinitely, at least partly because of this statute. Interview with Eric Schmidt, CEO, Google, Inc. (Oct. 2, 2009, 4:11 PM), *available at* http://www.npr.org/templates/transcript/transcript.php?storyId=113450803. Instead of allowing the government to collect *abandoned* e-mails that users have no interest in collecting, the statute actually facilitates another way for the government to access everyday communications. *See* 18 U.S.C. § 2703(f) (requiring ISPs to preserve records pending the issuance of a court order).

exception to the legislative trend that "[h]istorically, Congress has dragged its heels in protecting communications privacy until the courts have demanded it."[23]

Third, the judicial branch has remained unable to exercise appellate review of these cases because there is little binding precedent and parties rarely appeal cases.[24] For example, although CALEA was enacted in 1994, the law continues to be unclear as to whether cell site location information ("CSLI") qualifies as "location data" subject to the "specific and articulable facts" standard of § 2703(d) of the Stored Communications Act ("SCA"),[25] or whether the Fourth Amendment requires the government to produce "probable cause"[26] to obtain CSLI.[27] In the intervening twenty-one years, the lack of appellate precedent has left this issue largely unsettled and lower courts have been left without a binding interpretation of the standards required under ECPA.[28]

The most direct way for this area of the law to reflect modern privacy expectations is to allow courts to develop binding precedent by interpreting the Constitution. But the question then turns to *why* appellate review of these proceedings is so anemic.

## II. Secret Courts with No Opportunity or Incentive to Appeal

> Every year 15,000 employment discrimination cases are filed in federal court, and based on innumerable Supreme Court and circuit precedents, every trial court knows what the plaintiff's burden of proof is. Inconceivable that it could be otherwise, most would agree. Yet, every year more than twice that number of electronic surveillance cases are filed and decided, with literally no binding precedent to specify the government's burden of proof when tracking your cell phone location. How is that conceivable?[29]

There are three primary reasons why ex parte ECPA orders are not appealed. First, the secrecy measures surrounding ECPA and the SCA

---

23. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 687 (2011); *see also* Smith, *supra* note 2, at 313 ("Although the ECPA has often been amended, most changes have been technical tweaks to the existing framework.").

24. *See infra* Part II.C.

25. 18 U.S.C. § 2703.

26. *In re* Application of U.S. For An Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 579 (E.D.N.Y. 2010), *rev'd* (Nov. 29, 2010).

27. *Compare* United States v. Davis, 754 F.3d 1205, 1211 (11th Cir. 2014), *aff'd in part, rev'd in part en banc*, 785 F.3d 498 (11th Cir. 2015), *with In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010) (holding that the government was only required to articulate "specific and articulable facts" under § 2703(d), but that magistrate judges could require "probable cause" in their discretion).

28. *Nesbitt*, *supra* note 17 ("Like an absentee landlord, Congress has all but ignored this widening breach since the problem first came to its attention in 1994."); s*ee also* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 103(a)(2)(B), 108 Stat. 4279, 4281 (1994) (codified at 47 U.S.C. §§ 1001–1021 (2014)).

29. *Nesbitt*, *supra* note 17, at 262.

rarely provide notice to targeted individuals that the government has obtained their electronic communications. Second, even where individuals are given notice, that notice is not given until after the information is obtained, creating excessively high barriers to the suppression of that information. And third, once the government has obtained the information, the only actual parties to the action have no incentive to appeal: (1) the targeted individual must reach a prohibitively high burden to suppress the information; (2) ISPs do not want to engage in a costly legal battle; and (3) the government can simply sidestep rulings against it and apply to other judges that are more likely to grant the ex parte order.[30] The result is a dearth of appellate precedent and little guidance as to the proper standards required under ECPA and the Fourth Amendment.[31]

ECPA governs the interception of electronic communications,[32] and ultimately is comprised of three titles. The first title, the Wiretap Act, governs the "intercept[ion]" of communications, a term defined as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[33] The second title, the SCA, regulates the privacy of stored communications.[34] Stated more simply, the Wiretap Act governs the interception of "communications while in transit," whereas the SCA governs communications once they have been stored.[35] The third title, the Pen Register Act, addresses "pen register and trap and trace devices," which capture the dialed numbers and related information from outgoing or incoming calls or communications.[36]

ECPA provides four standards upon which government requests for information must be based, each standard increasing in scrutiny based upon how invasive the order is[37]: (1) pen registers and trap and trace

30. *In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 584 n.5 (E.D.N.Y. 2010), *rev'd* (Nov. 29, 2010) ("The result . . . has been an unpredictable legal regime . . . . It is a regime in which prosecutors, rather than seeking to establish predictable legal norms, understandably 'tend to gravitate toward a judge who is known to view their requests less critically.'" (quoting *ECPA Reform Committee*, *supra* note 15, at 12)).

31. Freiwald, *supra* note 23, at 682; *see also* Smith, *supra* note 2, at 326 ("During its twenty-five year history, the ECPA has been the subject of only two Supreme Court decisions. By comparison, over a similar period the Supreme Court decided thirty-seven cases involving the Employee Retirement Income Securities Act of 1974, a statute of comparable range and complexity but generating far fewer cases filed.").

32. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2014).

33. The Wiretap Act, 18 U.S.C. § 2510(4).

34. Stored Communications Act, 18 U.S.C. §§ 2701–2712 ; *see also id.* § 2510(17).

35. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 815 (2003).

36. Pen Register Act, 18 U.S.C. §§ 3121–3127.

37. *ECPA Reform Committee*, *supra* note 15, Ex. B.

devices only demand "certified relevance";[38] (2) stored communications and account records require *at least* "specific and articulable facts";[39] (3) tracking device warrants require a Rule 41 "probable cause" standard;[40] and (4) wiretap orders require a "super-warrant"[41] standard.[42] In determining whether information is protected from the government, courts engage in two primary inquiries: (1) which of these four standards is required under ECPA to obtain that specific type of information, and (2) whether the Fourth Amendment requires a higher standard. But without binding appellate precedent, a magistrate or district judge's answer to these inquiries is irrelevant outside of that specific case because the decision is not binding on other judges.

### A. The Secrecy Provisions Within ECPA Diminish Notice and Render Targeted Individuals Unaware That the Government Has Obtained Their Information

ECPA's secrecy regime is a prime reason why appellate review of ECPA applications is so scarce. Without proper notice, targeted individuals rarely understand that the government has obtained their information, and thus, cannot contest adverse court rulings that favor the government. As stated by Magistrate Judge Stephen William Smith, "excessive secrecy effectively shields electronic surveillance orders from appellate review, thereby depriving the judiciary of its normal role in shaping, adapting, and updating legislation to fit changing factual (and technological) settings over time."[43] This Subpart briefly outlines the statutory authority within the Wiretap Act and the SCA that allows the government and courts to withhold notice from targeted individuals that they are being surveilled.

Under the Wiretap Act, wiretap orders "shall be sealed by the judge"[44] until a showing of "good cause."[45] Because no time limit is given for how long the order will be sealed, the effect is to "close files to public scrutiny long after any need for secrecy has passed."[46] Although the statute requires the government to provide notice to the target after surveillance, notice is only required after ninety days, and that period

38. 18 U.S.C. § 3122(b)(2). The statute simply requires the court to find that the law enforcement official has "certified to the court that the information likely to be obtained" is "relevant to an ongoing criminal investigation." *Id.* § 3123(a)(1)–(2).

39. *Id.* § 2703(d).

40. *Id.* § 3117; *see also* Fed. R. Crim. P. 41(d)(1).

41. Freiwald, *supra* note 23, at 748.

42. *See generally* 18 U.S.C. § 2518 (discussing the requirements that the government must meet to obtain a wiretap order).

43. Smith, *supra* note 2, at 326.

44. *In re* United States, 10 F.3d 931 (2d Cir. 1993) (quoting 18 U.S.C. § 2518(8)(b)); *see also* 18 U.S.C. § 2510(9)(a).

45. 18 U.S.C. § 2518(8)(b).

46. Smith, *supra* note 2, at 323 (quoting James G. Carr & Patricia L. Bellia, The Law of Electronic Surveillance § 4:72 (2012)).

may be extended if there is "good cause."[47] Moreover, the statute has no notice requirement for individuals who are ancillary to the investigation, and those individuals will rarely be notified of any surveillance against them.[48]

Under the SCA, the government can obtain court orders through § 2703(d) to compel access to stored wire and electronic communications, as well as subscriber and customer account information.[49] Although the statute does not have a provision for sealing such orders, the government is not required to provide notice to the subscriber or customer if it obtains the information using a warrant.[50] The government may obtain information through an administrative subpoena or a § 2703(d) order if it first provides notice to the individual,[51] except that notice may be delayed indefinitely in ninety-day increments if it fits one of five exceptions.[52] The practical effect of this secrecy scheme is that defendants can be surveilled for years without receiving notice,[53] hindering their ability to both contest the government in the first place and appeal adverse decisions to higher courts.

The secrecy of these proceedings has allowed issues under ECPA to go relatively unexamined for years.[54] As a result, there is almost zero guidance on the proper scope of the law, despite the incredible number of requests received by ISPs each year.[55]

### B. Even If Notified, ECPA Lacks Adequate Remedies for Individuals to Oppose the Government Once Their Information Has Been Obtained

Even where an individual receives notice of surveillance under ECPA, the targeted individual has little incentive to bring a claim under the

47. *Id.* ("In practice, the ninety-day maximum period has come to be seen as a minimum, and further postponements are granted as a matter of routine.").

48. *Id.*

49. *Id.* at 324; *see also* 18 U.S.C. § 2703(d).

50. 18 U.S.C. § 2703(b)(1)(A).

51. *Id.* § 2703(b)(1)(B).

52. *Id.* § 2705(a)(2) (listing the exceptions as: "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial").

53. *See* United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010). In October 2004, the government formally requested that the ISP preserve Warshak's e-mails, pursuant to 18 U.S.C. § 2703(f). *Id.* In January 2005, the government obtained a subpoena for those e-mails, pursuant to 18 U.S.C. § 2703(b). *Id.* In May 2005, the government served the ISP with an ex parte court order for any additional e-mails, pursuant to 18 U.S.C. § 2703(d). *Id.* "In all, the government compelled [the ISP] to reveal the contents of approximately 27,000 e-mails. Warshak did not receive notice of either the subpoena or the order until May 2006." *Id.*

54. Smith, *supra* note 2, at 326.

55. *See infra* Part III.

statute for the improper interception of their electronic communications.[56] As a result, targeted individuals are even less likely to oppose the government because they are unable to remedy the situation once the government has improperly obtained their information. And although ECPA authorizes civil remedies, defendants are rarely willing to pursue these when faced with criminal charges.[57]

The largest obstacle targeted individuals face is that ECPA does not provide an exclusionary remedy to suppress information in a criminal proceeding once the government has improperly obtained the information.[58] Rather, information obtained in violation of ECPA can only be excluded from a criminal proceeding if: (1) the court concludes the search violated the Fourth Amendment, and (2) the court finds that law enforcement officials did not act in good faith.[59] Yet courts are often unwilling to consider the constitutional merits if they first find that the officials acted in good faith,[60] resulting in an impressive lack of precedent.

### C. The Practical Implication of ECPA's Statutory Scheme Is That Only a Small Percentage of ECPA Applications Are Ever Opposed and Appealed

Only a few courts of appeals have considered the standards necessary for the collection of information under ECPA.[61] Magistrate Judge Smith's explanation is that none of the three parties aggrieved—the targeted

56. Freiwald, *supra* note 24, at 681.

57. Kerr, *supra* note 35. Individuals have a cause of action against the government for *willful* violations and may recover the greater of actual or statutory damages, plus reasonable litigation costs. 18 U.S.C. § 2512(a). Because the majority of ECPA cases are litigated within the civil context, courts have not elaborated on the statute's application within the criminal context and have largely ignored Fourth Amendment application.

58. *But see id.* § 2515 (prohibiting the use of improperly intercepted *wire or oral* communications, or any evidence obtained resulting from it, but not prohibiting the use of electronic communications); *see also* Kerr, *supra* note 35, at 809 ("[A suppression remedy] would clarify the law, inform the public, and influence the law's doctrinal development.").

59. Freiwald, *supra* note 24, at 682; *see also* United States v. Leon, 468 U.S. 897, 922 (1984) (recognizing a good faith exception to the suppression of improperly obtained evidence).

60. *Leon*, 468 U.S. at 922. Interestingly, the Supreme Court has considered a similar issue within the realm of qualified immunity. *See* Pearson v. Callahan, 555 U.S. 223, 236 (2009). Qualified immunity does not apply where (1) the plaintiff has sufficiently alleged violation of a constitutional right, and (2) that right was "clearly established" at the time of the defendant's alleged misconduct. *Id.* at 232. Previously, the Court mandated that courts were required to first determine whether a constitutional right was violated, in order to support the "law's elaboration from case to case." Saucier v. Katz, 533 U.S. 194, 201 (2001). The goal was to allow constitutional rights to become "clearly established" through such determinations. *Id.* The Court has since overturned this mandate, however, and lower courts may avoid the constitutional merits by simply concluding that the constitutional right has not been clearly established. *Pearson*, 555 U.S. at 236. The result is that these types of rights are rarely further established. *See id.*

61. *See infra* Part III.B.

individual, the ISP, or the government—has any real incentive to appeal decisions.[62]

First, the targeted individual has no opportunity to oppose an ex parte motion until a court has already granted access to the government.[63] Because of the unique nature of electronic communications, targeted individuals have no way to challenge an order before its execution.[64] Whereas a traditional search requires law enforcement officials to enter the premises of the targeted individual to conduct the search, electronic communications are generally obtained from ISPs and other third-party communications companies.[65] Moreover, ISPs are not allowed to notify the customer or subscriber of the ECPA order for as long as the "court deems appropriate."[66] By the time individuals obtain notice of these requests and are able to contest them, the government has already collected the information. Because ECPA has no suppression remedy, this essentially eliminates any incentive the individual would have to appeal,[67] assuming the targeted individual even knows of the order used to obtain the evidence in the first place.[68]

As a rare example of when a defendant *was* incentivized to appeal a lower court's ruling, consider the case of *United States v. Warshak*, where the Sixth Circuit ultimately concluded that the defendant possessed a reasonable expectation of privacy in his e-mails.[69] There, the defendant had substantial financial incentives to appeal his case—not including ECPA's meager statutory remedy—because his alleged fraudulent activities centered on his incredibly profitable company, which served as the distributor of the male-enhancement drug Enzyte.[70] Moreover, the defendant was only able to appeal "after a magistrate judge unsealed the underlying ECPA orders," revealing the source of the government's evidence.[71] But targeted individuals rarely possess the types of financial resources available to the defendant in *Warshak*, and thus, defendants are rarely in a position to appeal these cases and mount a constitutional

62. Smith, *supra* note 2, at 327.

63. *See supra* Part II.B.

64. Smith, *supra* note 2, at 327.

65. Kerr, *supra* note 35, at 808–09.

66. 18 U.S.C. § 2705(b) (2006).

67. Smith, *supra* note 2, at 330–31.

68. The targeted individual is unlikely to even know of the order because it is submitted "*ex parte*, without notice, and subject to the sealing and gag orders." *Id.* at 327. The government would additionally need to disclose the order in pretrial discovery or trial, which is unlikely given that few of these orders are ever unsealed. *Id.* at 327–28.

69. 631 F.3d 266, 288 (6th Cir. 2010).

70. *See id.* at 318.

71. Smith, *supra* note 2, at 327 (citing Warshak v. United States, 490 F.3d 455, 460–61 (6th Cir. 2007), *vacated in part*, 532 F.3d 521 (6th Cir. 2008) (en banc), *appeal after remand*, 631 F.3d 266 (6th Cir. 2010)).

challenge whenever the government has improperly obtained their information.

Second, ISPs have little incentive to oppose the government against such orders: they are compensated for the costs of complying, and the cost of a legal battle would far outweigh simply providing the information.[72] Additionally, many of those ISPs do not want to oppose the government because they market identical services to the public for profit.[73] And because there is no binding precedent from higher courts, an ISP's efforts may have diminishing returns: the government can simply apply to different magistrate judges until one of them grants the order.[74] Although larger ISPs have significant resources to oppose the government, the reality is that they rarely appeal those decisions.[75]

Finally, the government has no incentive to appeal decisions. The government applies for these orders ex parte, so there are only two possible outcomes: the magistrate judge will either grant or deny the order. If the former, the government will simply collect the information and move on. If the latter, the government will not risk an appeal that could establish binding, unfavorable law. Instead, the government will simply apply to another magistrate judge, as the opinion of one magistrate has no binding effect on others.[76] Neither of these outcomes encourages the government to appeal because it either received a positive outcome or risk the establishment of binding law against its position. Moreover, because of the ex parte nature of these proceedings, the government is the sole party to define the issues before the court and can guide the court's analysis accordingly. Looking to CSLI as an example, the government has characterized this information as "historical," even where the data is milliseconds old and can enable contemporaneous tracking.[77] The result is that the government is in complete control over the ex parte proceedings and has no incentive to appeal and create potentially adverse precedent.

This discussion highlights just one explanation for the simple fact that few, if any, of these ex parte orders under ECPA are ever appealed.[78] Assuming charges are even filed against the targeted individual, it is not

72. *Id.* at 328.

73. Albert Gidari, *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535, 546 (2007). As a concrete example, while a consumer may not want the government to be able to track them using their phone, a consumer does want Apple to be able to locate their phone in case it is lost or stolen. *See iPhone Support: Find My iPhone*, APPLE, https://www.apple.com/support/iphone/find/ (last visited Aug. 5, 2015).

74. Gidari, *supra* note 73, at 546–47.

75. Smith, *supra* note 2, at 328; *see also* Gidari, *supra* note 73, at 550 ("How does that sit when you are a multipurpose phone company and your general counsel is the former Attorney General of the United States . . . ? Verizon is likely not going to see these issues the same as [privacy groups].").

76. Gidari, *supra* note 73, at 547.

77. Government Reply Brief, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866620.

78. Smith, *supra* note 2, at 326–27.

clear that the government discloses that the evidence was obtained from an ECPA order.[79] And even if the targeted individual was aware that the information stemmed from an ECPA order, the impending criminal charges overshadow any potential opposition to or appeal of the ECPA order itself. The inevitable result is that magistrate judges are forced to respond to thousands of these requests each year with "literally no binding precedent" to guide their decisions or create uniform outcomes.[80]

## III. Lack of Appellate Precedent Under ECPA

Magistrate Judge Smith has argued that the Supreme Court's difficulty in clarifying ECPA standards stems from the "relative paucity of cases involving electronic surveillance under ECPA."[81] This Part details the inevitable outcome of ECPA's secrecy regime: the sincere lack of both Supreme Court and circuit court precedent under the Act.

### A. The Supreme Court Has Provided No Guidance as to the Standards Required by ECPA

The Supreme Court has only had the opportunity to consider two cases under ECPA,[82] neither of which was within the criminal context.[83] Ultimately, neither case elaborated on the standards required under ECPA or the Fourth Amendment.

*Bartnicki v. Vopper*, the Supreme Court's first case on the issue, only considered the First Amendment implications of ECPA's disclosure requirements,[84] and thus, it is largely irrelevant to the question of what standards are required by ECPA or the Fourth Amendment. And while the Supreme Court's second decision—*City of Ontario, California v. Quon*—directly addressed the standards required under ECPA, the Court did not provide any guidance as to what protections might exist.[85]

79. *Id.* at 327–28.

80. *Nesbitt*, *supra* note 17, at 262.

81. *Id.* at 261.

82. *See* City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010); *see also* Bartnicki v. Vopper, 532 U.S. 514 (2001).

83. The Supreme Court has acknowledged that Fourth Amendment protections extend beyond just criminal investigations, including when the government acts in its capacity as an employer. *See, e.g.*, Camara v. Mun. Court, 387 U.S. 523, 530 (1967); Treasury Emps. v. Von Raab, 656, 665 (1989). The Court has not clarified, however, whether a different Fourth Amendment standard applies where the government acts as an employer, as opposed to its law enforcement capacity. *Quon*, 560 U.S. at 757 (discussing the plurality opinion in O'Connor v. Ortega, 480 U.S. 709 (1987)).

84. Specifically, § 2511(1)(c) prohibited the intentional disclosure of illegally intercepted communications. 18 U.S.C.A. § 2511 (2008). The Court had to determine (1) whether this was a "content-neutral" law of general applicability, and (2) whether application to the defendants violated their First Amendment rights, where the defendants had obtained the information lawfully and did not realize it had originally been obtained illegally. *Bartnicki*, 532 U.S. at 517. Ultimately the Court held that this was a content-neutral law, but that it did violate the defendants' First Amendment rights because they had not taken part in the interception of the information. *Id.* at 526, 535.

85. 560 U.S. 746.

There, the Court determined whether the Fourth Amendment prohibited the city from reading a government employee's text messages sent using a pager.[86] Although the factual record in *Quon* was *eight years old* and the technology focused primarily on a pager, the Supreme Court—in 2010—stated that it "risk[ed] error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[87] Rather, the Court assumed *arguendo* that Quon had a reasonable expectation of privacy in his text messages but ultimately held that the search was reasonable because it was "efficient and expedient" and not "excessively intrusive."[88] Neither *Bartnicki* nor *Quon* elaborated on the protections under ECPA or the Fourth Amendment.

As a result of continued ambiguity as to the standards required under ECPA, lower courts are left to grapple with Fourth Amendment precedent that was mostly decided in the 1970s and '80s. The seminal privacy case interpreting the Fourth Amendment is *Katz v. United States*, where the Supreme Court held that there was a reasonable expectation of privacy over a telephone conversation that occurred in a phone booth.[89] The Court focused on the fact that a user of a telephone booth shut the door, which entitled him "to assume that the words he utters into the mouthpiece will not be broadcast to the world."[90] But the third-party doctrine quickly limited any reasonable expectation of privacy in information revealed to third parties.[91] For example, in *Smith v. Maryland*, the Supreme Court refused to recognize an expectation of privacy in phone numbers dialed by an individual because "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company" in order to place calls.[92] The Supreme Court also distinguished between "envelope" information, such as the numbers dialed, and "content" information, such as the actual conversation itself,

86. *Id.* at 750. Importantly, Mr. Quon was a police officer working for the city, and the city had given him the pager to use for work purposes. *Id.* at 750–51.

87. *Id.* at 759. *But see* Freiwald, *supra* note 23, at 689 ("[I]f the courts take too long to address new technology, they create the risk not only that the technology they do address will be obsolete but also 'that the Fourth Amendment will never really catch up.'") (quoting Audio File: *Hearing Before S. Comm. on the Judiciary, The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age*, at 88:30-89:10 (2010) (oral statement of Brad Smith, Esq., General Counsel of Microsoft Corporation)), *available at* http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=judiciary092210&st=xxx).

88. *Quon*, 560 U.S. at 760–61.

89. 389 U.S. 347, 353 (1967). In order to demonstrate a reasonable expectation of privacy, an individual must show (1) a subjective expectation of privacy, and (2) that the expectation is "one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring).

90. *Id.* at 352; *see also id.* at 361 (Harlan, J., concurring) ("The critical fact in this case is that '[o]ne who occupies it, [a telephone booth] shuts the door behind him . . . .").

91. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (holding that a bank customer lost any expectation of privacy when she gave her information to a bank teller).

92. 442 U.S. 735, 742 (1979).

which might have been entitled to more protections.[93] While these factual examples may appear simple, scholars remain conflicted as to how applicable these "pre-modern precedents" are to the "constitutional minimums for modern communications."[94]

Two recent Supreme Court cases have cast doubt on the continued applicability of these older cases to modern Fourth Amendment jurisprudence. In *United States v. Jones*, where the Court unanimously held that the government's warrantless installation of a GPS tracking device violated the Fourth Amendment, five Justices expressed doubts about the applicability of the third-party doctrine in more modern cases.[95] The five-Justice majority reached its conclusion by relying on the government's physical trespass on the defendant's car to place a GPS and track the defendant.[96] While agreeing with the majority in this case, Justice Sotomayor's concurrence directly questioned the relevance of older legal frameworks, such as the third-party doctrine, for future cases.[97] Moreover, Justice Alito's four-Justice concurrence criticized the majority's trespass theory and directly applied the *Katz* test to conclude that GPS tracking for four weeks violated the defendant's reasonable expectation of privacy.[98] Thus, at least five Justices have expressed a willingness to discard the third-party doctrine as it applies to modern technologies.

Similarly, the second case—*Riley v. California*—distinguished *Smith* and rejected the government's argument that the third-party doctrine should apply. There, the Court unanimously held that the Fourth Amendment required police officers to obtain a warrant to search a defendant's cell phone for incriminating information.[99] In reaching its decision, the Court rejected third-party doctrine because the use of a pen

93. *Id.* at 743. *But see id.* at 748 (Stewart, J., dissenting) ("The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without 'content.'"); *see also* Freiwald, *supra* note 23, at 689 (labeling the content versus non-content interpretation as an "analytical short cut" that inhibits Fourth Amendment analysis).

94. *Compare* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 12 (2007) (arguing that courts should instead apply a "normative inquiry" of "whether users may rely on the privacy of the information because of the vital nature of that aspect of modern communications"), *with* Orin S. Kerr, *Internet Surveillance After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 612 (2003) (arguing that the principles of *Katz* and *Smith* translate well to e-mail, which easily distinguishes between e-mail headers and the body of the e-mail).

95. United States v. Jones, 132 S. Ct. 945, 951 (2012) (applying a trespass-based theory to render the GPS device unconstitutional because the GPS device was placed on the bottom of the defendant's vehicle).

96. *Id.*

97. *Id.* at 957 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach 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." (citations omitted)).

98. *Id.* at 964 (Alito, J., concurring).

99. Riley v. California, 134 S. Ct. 2473, 2485 (2014).

register in *Smith* did not qualify as a "search" under the Fourth Amendment.[100] Thus, it is even less clear what Fourth Amendment standard should guide lower courts as they wrestle with the privacy protections of electronic communications, other than the normative, case-by-case inquiry provided by *Katz*.[101]

### B. Only a Handful of Circuit Court Decisions Have Grappled with These Standards Required Under ECPA

Appellate interpretations of the standards required to obtain electronic communications have been relatively sparse as well. In recent years, the discussion of location data has received relatively greater discussion than other technologies that focus exclusively on electronic communications. For example, only one appellate court has addressed whether citizens enjoy a reasonable expectation of privacy in their e-mail, ultimately concluding that they do.[102] By contrast, several circuits had previously issued opinions discussing GPS location data[103] before the Supreme Court's opinion in *Jones* resolved the issue by requiring a warrant.[104]

There are three possible explanations for the disparate treatment of these types of information. The first is that location data, unlike electronic communications, often goes directly to a central element in a crime (that is, the defendant's whereabouts), and thus, the government is more likely to rely on this information at trial. Another possible explanation is that the government can plausibly claim that electronic communications were obtained in some way other than through ECPA or the SCA, such as by searching a defendant's computer after arrest. By contrast, the government will often need to detail the reliability of the defendant's location data, including how it was obtained, in order to persuade a jury in a criminal case. One final explanation is that GPS location data, one of the most popular forms of tracking until *Jones*, is not subject to ECPA[105] and the

100. *Id.* at 2492. The logical conclusion of this analysis is that any "search" of a defendant's information would never be subject to the third-party doctrine. *See id.*

101. Freiwald, *supra* note 94; *see also* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (requiring an individual to show (1) a subjective expectation of privacy, and (2) that the expectation is "one that society is prepared to recognize as 'reasonable'").

102. United States v. Warshak, 631 F.3d 631 F. 3d 266, 275, 288 (6th Cir. 2010) (holding that individuals had a reasonable expectation of privacy in e-mails when the ISP merely acted as an intermediary to facilitate their transmission).

103. United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011) *cert. granted and judgment vacated*, 132 S. Ct. 1534 (2012); United States v. Maynard, 615 F.3d 544, 568 (D.C. Cir. 2010) *aff'd in part sub nom. Jones*, 132 S. Ct. 945; United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010*) cert. granted and judgment vacated*, 132 S. Ct. 1533 (2012).

104. *Jones*, 132 S. Ct. at 954 (affirming that the government's warrantless installation of a GPS tracking device violated the Fourth Amendment).

105. GPS location data is not generally governed by ECPA because it relies on a tracking device, and not necessarily electronic communications stored by an ISP. *See id.* at 949; *see also In re*

corresponding secrecy regime that diminishes appellate review. Regardless of the ultimate reason, the reality is that appellant precedent under ECPA remains scarce.

Now that the Supreme Court has held that GPS surveillance requires a warrant,[106] warrantless cell phone tracking has become a de facto method to snoop on criminals.[107] As a result, this is one of the few technologies governed by ECPA that has received at least moderate appellate attention in the past few years. By way of background, law enforcement officials perform this cell phone tracking by monitoring CSLI, defined as information about calls made using cell sites or cell towers.[108] CSLI will reflect the direction of the user from the tower and will normally connect to the closest cell tower, allowing law enforcement to extrapolate the approximate location of the cell phone user at the time and date of the call record.[109] Only three appellate courts have considered SCA and Fourth Amendment standards for obtaining cell site information.[110] Moreover, each of these circuits have articulated different standards required under ECPA to obtain a defendant's cell site information.

The Third Circuit did not address the legal standard for cell site information until 2010.[111] In *In re Application of the U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, the Third Circuit rejected the argument that historical cell site information constituted a "tracking device," which would have required a probable cause standard, largely because "the privacy interests at issue are confined to the interior of the home" and there was no evidence that historical cell site information "extend[ed] to that realm."[112] Thus, the court concluded that a § 2703(d) order only

Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 133 n.15 ("Again, the Court sees little resemblance between the tracking devices in [GPS location cases] and the retrieval of stored electronic records here.").

106. *Jones*, 132 S. Ct. at 95 (affirming that the government's warrantless installation of a GPS tracking device violated the Fourth Amendment).

107. David Kravets, *NSA Wrongly Says Warrantless Mobile-Phone Location Tracking is Legal*, WIRED (Dec. 6, 2013, 6:30 AM), http://www.wired.com/2013/12/nsa-cell-site-data/.

108. *See* United States v. Davis, 754 F.3d 1205, 1210–11 (11th Cir. 2014), *aff'd in part, rev'd in part en banc*, 785 F.3d 498 (11th Cir. 2015).

109. *Id.* at 1211.

110. *See id.*; *see also In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010) (holding that the government is only required to show "specific and articulable facts" that historical cell site data is reasonably related to an ongoing criminal investigation, but that a magistrate judge has discretion to require a warrant and probable cause); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding that there was not a reasonable expectation of privacy in regards to historical cell site data because the information sought was a business record and voluntarily given to a third party).

111. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d at 313.

112. *Id.* at 312–13 (citing United States v. Knotts, 460 U.S. 276 (1983) and United States v. Karo, 468 U.S. 705 (1984) for the proposition that "tracking devices" only implicate Fourth Amendment concerns to the extent they "reveal a critical fact about the interior" of the home).

required "specific and articulable facts" that the information was "relevant and material to an ongoing criminal investigation."[113] The Third Circuit proceeded, however, to hold that a magistrate judge possesses discretion to require a warrant showing probable cause pursuant to 18 U.S.C. § 2703(c)(1)(A),[114] so long as she made "fact findings and [gave] a full explanation that balances the Government's need (not merely desire) for the information with the privacy interests of cell phone users."[115]

The Fifth Circuit agreed that § 2703(d) only required the "specific and articulable facts" standard, but disagreed that a magistrate judge possessed discretion to require a probable cause warrant under the SCA.[116] Although the Eleventh Circuit ultimately agreed with the Fifth Circuit in the en banc decision *United States v. Davis*, a panel decision in the same case merits additional discussion.[117]

The panel ultimately disagreed with both the Third and Fifth Circuits and held that the Fourth Amendment required the government to produce probable cause to obtain a defendant's cell site information.[118] The Eleventh Circuit relied heavily on the Supreme Court's decision in *Jones*, arguing that the factual differences between GPS location data and cell site information actually "operate[d] against the government's case rather than in favor of it."[119] *Jones* involved the movements of a defendant's automobile in public, and the Supreme Court ultimately concluded that a "reasonable expectation of privacy had been established by the aggregation of the points of data, not by the obtaining of individual points."[120] The Eleventh Circuit reasoned that this "mosaic theory" was unnecessary to establish an expectation of privacy in cell site information, where one's cell phone "can accompany its owner anywhere" and automatically convert "a private event into a public one."[121] Thus, while GPS location data would only be protected in the aggregate, the court held that "even one point" of cell site information could be within

113. *Id.* at 313.

114. Section 2703(c)(1) of the SCA states that "a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record . . . when the governmental entity (A) *obtains a warrant* issued using the procedures described in the Federal Rules of Criminal Procedure . . ." or "(B) *obtains a court order* for such disclosure under subsection (d) of this section[.]" 18 U.S.C.A. § 2703 (emphasis added).

115. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d at 319.

116. *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d at 607 ("[W]e conclude that the 'may be issued' language is permissive—it grants a court the authority to issue the order—and the 'shall issue' term directs the court to issue the order if all the necessary conditions in the statute are met.").

117. *See* United States v. Davis, 754 F.3d 1205 (11th Cir. 2014), *aff'd in part, rev'd in part en banc*, 785 F.3d 498 (11th Cir. 2015).

118. *Id.*

119. *Id.* at 1215.

120. *Id.* (discussing United States v. Jones, 132 S. Ct. 945, 951 (2012)).

121. *Id.* at 1215–16.

a reasonable expectation of privacy.[122] Notably, the en banc majority of the Eleventh Circuit relied heavily on the third party doctrine to reverse the panel's decision, despite more recent Supreme Court precedent casting doubt on the doctrine's applicability to more modern technology.[123]

These cases demonstrate that there is little guidance as to the proper standards required under ECPA or the Fourth Amendment. While the courts have engaged in some discussion of the standards required to obtain a § 2703(d) order for CSLI, there is still little agreement across circuits.[124] Moreover, a court's discussion is often technology specific and rarely applies outside of the context of that specific technology.[125] The best way to increase appellate discussion of technology under ECPA is for parties to increase opposition to the government and appeal adverse judgments.

## IV. The Solution: Increasing ECPA Appeals to Create Binding Precedent

Ex parte proceedings already go against our adversarial judicial structure in that they allow one party to petition the court without opposition from another party.[126] There are three avenues to increase appellate review of ex parte ECPA orders and foster the development of binding standards under the Act. First, given the political climate surrounding developments in privacy law after the Snowden revelations of 2013, ISPs should be more willing to oppose government requests for information. Second, district courts should be willing to appoint counsel in federal criminal cases where it would be appropriate to do so. And third, Congress could amend ECPA to allow courts to appoint Constitutional Advocates in cases where significant constitutional questions are presented, reinstating the adversarial nature of these proceedings.

---

122. *Id.* at 1216.

123. *See* United States v. Davis, 785 F.3d 498, 511–15 (11th Cir. 2015) ("If anything, Justice Alito's concurrence, joined by three others, suggests that a legislative solution is needed."); *see also supra* Part III.A (discussing the Supreme Court's more recent disregard of the third party doctrine).

124. *Compare Davis*, 754 F.3d at 1217, *with In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d at 607.

125. *See Davis*, 754 F.3d at 1215 (accepting as relevant the government's distinction between GPS location data and cell site information); *see also In re* Application of the U.S. for an Order Pursuant to § 18 U.S.C. 2703(d), 830 F. Supp. 2d 114, 133 n.15 ("Again, the Court sees little resemblance between the tracking devices in [GPS location cases] and the retrieval of stored electronic records here.").

126. *Nesbitt*, *supra* note 17, at 262 ("[T]he ex parte nature of ECPA applications does present a major procedural challenge for magistrate judges. These are not adversary proceedings with opposing counsel present to argue the constitutional, statutory, or procedural rights of . . . other targeted parties.").

## A. ISPs Should Increase Opposition to the Government and Appeal Cases

ISPs do not want to be "middle men" between citizens and the government,[127] but there is no realistic alternative under a statutory scheme that requires ISPs to track customer information in order to provide it to the government.[128] If ISPs opposed the government's ECPA orders and appealed adverse decisions to higher courts, then appellate courts would be able to establish binding precedent that would guide lower courts as to the proper legal process required under ECPA and the Fourth Amendment. With that guiding precedent, the focus can turn away from ISPs and toward the appropriate standard that should be applied to a particular technology.

### *1. The NSA Revelations Provide Background as to Why ISPs Have Recently Pushed for Legislative Reform*

The Internet industry's push for privacy reform is an overt reaction to the Snowden revelations of 2013, which accused many of these same technology companies of directly enabling the mass surveillance of American citizens without a warrant.[129] Two specific programs are directly relevant to large communications companies: MUSCULAR and PRISM.[130]

MUSCULAR was a joint operation between the NSA and its British counterpart, the Government Communications Headquarters ("GCHQ").[131] The operation performed "upstream collection," which refers to the direct copying of entire data flows over fiber-optic cables.[132] Using this type of collection, the NSA copied any and all information sent between Google and Yahoo! datacenters[133] across the world without the companies' knowledge.[134]

---

127. Gidari, *supra* note 73, at 535 ("I do not tend to think about it that way—being 'in the middle'—I think it is just way too polite a term, way too generic, under-descriptive, and under-informed. Instead, I think 'Service Providers As Piñatas' would be a better title because service providers get beat up by all sides all the time.").

128. *See* 18 U.S.C. § 2703(f) (2006) (requiring ISPs to preserve records pending the issuance of a court order); *see also* Interview with Eric Schmidt, *supra* note 22 (discussing how Google stored information longer than otherwise necessary to provide it to the government for these types of requests).

129. *NSA Slides Explain the PRISM Data-Collection Program*, Wash. Post (last updated July 10, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ [hereinafter *Prism Slides*] (identifying Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple as providers for the NSA's PRISM program).

130. *Id.*; *see also* Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

131. *See Prism Slides*, *supra* note 129.

132. *Id.*

133. Google and Yahoo! each have since encrypted the data sent between data centers, so as to make it more difficult for the NSA to make widespread use of the data. Matthew Panzarino, *Yahoo Will Follow Google in Encrypting Data Center Traffic, Customer Data Flow by Q1'14*, TechCrunch

By contrast, PRISM allowed the NSA to collect information from *participating* companies based on "targeting selectors," so long as there was a "reasonable belief"[135] that the specified target was a "foreign national who is overseas at the time."[136] Depending on the provider, the NSA received e-mail, chat (video and voice), videos, photos, stored data, Voice over Internet Protocol ("VoIP"), file transfers, video conferencing, notifications of the targets activity (for example, logins), and online social networking details.[137] A heavily redacted Foreign Intelligence Surveillance Court ("FISC") ruling from October 2011 at least confirms the existence of "the targeting of non-United States persons reasonably believed to be located outside the United States"[138] and "Upstream Collection,"[139] the latter of which was declared unconstitutional in that same FISC ruling.[140]

Meanwhile many of these companies have been vehemently outspoken that they only provide information to the government if it is a

(Nov. 18, 2013), http://techcrunch.com/2013/11/18/yahoo-will-follow-google-in-encrypting-data-center-traffic-all-traffic-between-company-and-customers-by-q1-14/. While the NSA can presumably still copy the information, the agency would need to conduct targeted decryption in order to access the data, which is far less effective than opportunistic decryption.

134. Gellman & Soltani, *supra* note 130. In response to the revelation of this program, Google's chief legal officer said, "We are outraged at the lengths to which the government seems to have gone to intercept data from our private networks, and it underscores the need for urgent reform." *Id.* It would be difficult to believe that Google or Yahoo! were completely unaware that this could happen on their servers, as the Electronic Frontier Foundation ("EFF") had initiated a legal battle as early as 2006 over the same type of surveillance on AT&T systems. Declaration of Mark Klein, 4–7, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D.C.A. 2006), *available at* https://www.eff.org/files/filenode/att/Mark%20Klein%20Unredacted%20Decl-Including%20Exhibits.PDF (detailing the installation of a fiber-optic splitter to enable to duplication of all data packets sent across the cable). Although in that instance, AT&T voluntarily cooperated with the government. *Id.*

135. "Reasonable belief" is defined as a fifty-one percent confidence. *See Prism Slides*, *supra* note 129.

136. *Id.* According to these internal slides, the following technology companies were complicit with PRISM surveillance: Microsoft, Yahoo!, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple. *Id.* Moreover, the NSA's General Counsel, Rajesh De, stated that Silicon Valley's tech giants knew about both "the internet collection program known as Prism and for the so-called 'upstream' collection of communications across the internet." DJ Pangburn, *Tech Giants Knew About Prism All Along, the NSA's Top Lawyer Says*, VICE (Mar. 19, 2014, 4:15 PM), http://motherboard.vice.com/read/tech-giants-knew-about-prism-all-along-says-the-nsas-top-lawyer.

137. Pangburn, *supra* note 136.

138. Presumably, the court's discussion of the targeting of non-U.S. persons refers to the targeting selectors used within PRISM. *See Prism Slides*, *supra* note 129.

139. The court's discussion of upstream collection refers to Project MUSCULAR. *See id*.

140. [Redacted], 2011 WL 10945618, at *1, *28 (FISA Ct. Oct. 3, 2011). It is difficult to estimate the current state of Project MUSCULAR, as the court's holding left open the possibility that the government could more narrowly tailor the "Upstream Collection." *Id.* at *28. Moreover, it is unclear whether GCHQ was involved at the time, whether the NSA avoided the constitutional concerns by simply having GCHQ perform this collection, or whether subsequent secret decisions have overturned this ruling. *Id.* What is clear is that the government received at least eight approvals of this program until it "clarified" the proper scope of its surveillance. *Id.* at *11 ("The Court now understands, however, that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications.").

"lawful, specific order[] about individuals" that is consistent with "tech company lawyers scrutinizing each [PRISM] request before complying with it."[141] For example, Google has claimed that it requires "an ECPA search warrant" before divulging the content of subscribers' information,[142] but this is problematic for two reasons. First, Google's resistance only applies to "content" information and accepts the government's outdated distinction of content and non-content data.[143] Google still readily divulges "non-content" information,[144] which alone can reveal significant personal information of targeted individuals.[145] In fact, using just your name and zip code—both of which are routinely included in account non-content information[146]—private companies have advertised the ability to identify customers with one hundred percent accuracy.[147] Second, it is unclear what an "ECPA search warrant" is or the proper legal standard required to obtain it.[148] Alone, these measures are not enough to oppose the government's over-invasive surveillance techniques.

---

141. Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST WONKBLOG (June 12, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ (responding to denials made by Google Chief Architect, Yonatan Zunger, on his public Google Plus page).

142. David Kravets, *Google Tells Cops to Get Warrants for User E-Mail, Cloud Data*, WIRED (Jan. 23, 2013, 5:29 PM), http://www.wired.com/threatlevel/2013/01/google-says-get-a-warrant.

143. *See* Smith v. Holder, 442 U.S. 735, 737, 741 (1979) (rejecting a Fourth Amendment challenge to the use of a pen register on telephone company equipment that captured information concerning telephone calls, but not the content or identities of the parties). *But see* Freiwald, *supra* note 23, at 689 (labeling the content versus non-content interpretation as an "analytical short cut" that inhibits Fourth Amendment analysis).

144. For example, Google will hand over the IP addresses associated with a particular e-mail, as well as the "non-content" portions, such as the "from," "to," and "date" fields. Freiwald, *supra* note 23, at 689.

145. Researchers sourced 5000 phone numbers and were able to identify 27.1% of those numbers using one automated program and three publicly available directories: Yelp, Google Places, and Facebook. Gregory Ferenstein, *Stanford Researcher Proves NSA Can Probably Identify Individuals From Phone Records*, TECHCRUNCH (Dec. 25, 2013), http://techcrunch.com/2013/12/25/stanford-researcher-proves-nsa-can-probably-identify-individuals-from-phone-records/. To conservatively approximate human analysis, the researchers randomly sampled one hundred numbers and were able to associate sixty of the numbers with an individual or business in just an hour using Google alone. *Id.*

146. For example, Microsoft has disclosed that its non-content information includes a user's login, personal user ID, first and last name, state, zip code, country, time zone, registered IP address, date of registration, gender, and last login IP address. *Law Enforcement Requests Report*, MICROSOFT, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (last visited Aug. 5, 2015).

147. Adam Tanner, *Never Give Stores Your ZIP Code. Here's Why*, FORBES (June 19, 2013, 8:19 AM), http://www.forbes.com/sites/adamtanner/2013/06/19/theres-a-billion-reasons-not-to-give-stores-your-zip-code-ever/.

148. *ECPA Reform Committee*, *supra* note 15, n.1, Ex. B. Essentially, ECPA demands four standards, each increasing in scrutiny based upon how invasive the order is: (1) pen registers and trap and trace devices only demand "certified relevance"; (2) stored communications and account records at least require "specific and articulable facts"; (3) tracking device warrants require a "probable cause" standard of Rule 41 of the Federal Rules of Criminal Procedure; and (4) wiretap orders require a "super-warrant" standard. *Id.* Thus, it is unclear what Google is specifically referring to when it

### 2. *The Same Rationale Underlying ISPs' Recent Political Opposition to the Government Supports Increased Judicial Opposition*

ISPs have the direct power to enable judicial review of ex parte ECPA orders by simply resisting the government's request for consumer information and appealing cases that are decided in favor of the government. It is especially strange, then, that many companies with this appellate right have chosen instead to petition the legislative and executive branches to reform ECPA directly.[149]

For example, in January 2013, Google, AT&T, and other technology companies "urged Congress to clarify when they need to give the government access" to user communications.[150] Similarly, in December of that year, Google actively supported an online petition for the Obama Administration to support ECPA reform, which reached the requisite 100,000 signatures to "mandate" an official response.[151] While making these public complaints to the government, technology companies have continued to enable governmental surveillance of American citizens. Google, Microsoft, Yahoo!, LinkedIn, and Facebook dropped a lawsuit seeking increased transparency about government requests for consumer information in exchange for the NSA's permission to disclose FISA orders in increments of 1000.[152] These "first world responses" pale to the direct

---

requires an "ECPA search warrant," as this could be a wiretap "super-warrant," a traditional search warrant, or simply a § 2703(d) order.

149. Allison Grande, *Google, Others Breathe New Life Into ECPA Reform*, LAW360 (Jan. 29, 2013, 10:10 PM), http://www.law360.com/articles/410977/google-others-breathe-new-life-into-ecpa-reform.

150. *Id.*

151. The administration has yet to respond. Tim Cushing, *ECPA Reform Petition Passes 100K Signature Threshold with a Last-Minute Surge*, TECHDIRT (Dec. 12, 2013, 2:02 PM), http://www.techdirt.com/articles/20131212/08533525546/ecpa-reform-petition-passes-100k-signature-threshold-with-last-minute-surge.html; *see also* Letter to President Barack H. Obama, Email Privacy and Reform of the Electronic Communications Privacy Act (ECPA) (Apr. 28, 2014), *available at* https://www.aclu.org/files/assets/ecpa_reform_coalition_letter.pdf (listing eighty-one organizations that support reforming ECPA to require a warrant based on probable cause).

152. Jeremy Hsu, *Tech Giants' NSA Deal Leaves Start-Ups in the Shadows*, INST. FOR ELECTRICAL & ELECTRONICS ENGINEERS (Jan. 29, 2014, 5:49 PM), http://spectrum.ieee.org/tech-talk/telecom/internet/tech-giants-nsa-deal-leaves-startups-in-the-shadows (discussing how the agreement still eliminates disclosures from new services that are less than two years old). ISPs want to disclose more information to the public for two reasons: (1) to create public awareness as to the extent of governmental surveillance, and (2) to shift the blame off of these companies (for complying with the government) to the government itself (for mandating their compliance in the first place). *See AT&T Transparency Report*, AT&T, http://about.att.com/content/dam/csr/transpreport/ATT_Transparency%20Report.pdf (last visited Aug. 5, 2015); *Verizon Transparency Report*, VERIZON, http://publicpolicy.verizon.com/blog/entry/verizon-releases-transparency-report-for-second-half-2014 (last visited Aug. 5, 2015); Jeremy Kessel, *Fighting for More #Transparency*, TWITTER (Feb. 6, 2014), https://blog.twitter.com/2014/fighting-for-more-transparency ("Unfortunately, we are currently prohibited from providing this level of transparency . . . [T]ransparency is critical for building and maintaining user trust and trust from the larger public, and for fostering a healthy and vibrant global community committed to defending free expression.").

measures that these companies *could* take by opposing ex parte ECPA applications directly and appealing adverse decisions.

Not all technology companies have decided to play ball with the Obama Administration or respond to government requests for information. For example, Twitter filed a lawsuit to increase transparency about government requests for consumer information.[153] Similarly, a small privacy-focused company, Lavabit, unsuccessfully resisted the government's request for its encryption keys, arguing that the keys would grant the government access to all of Lavabit's 400,000 customers.[154] After Lavabit's lawsuit was unsuccessful, another privacy-focused start-up, Silent Circle, closed its e-mail operations rather than be forced to comply with future government requests for information.[155] These companies exemplify the lengths to which ISPs could go to oppose the government's request for consumer information.

Other companies have followed suit and actually removed the technological capability for the government to access user information. For example, Apple made headlines when it announced that it would no longer enable its phones to remotely obtain customer data.[156] Within three hours of Apple's announcement, Google followed suit and announced that they would similarly encrypt their future phones.[157] Law enforcement officials were highly critical of these decisions, arguing that the protective measures would hinder investigators even where they possessed probable

153. Ellen Nakashima, *Twitter Sues U.S. Government Over Limits on Ability to Disclose Surveillance Orders*, WASH. POST (Oct. 7, 2014), http://www.washingtonpost.com/world/national-security/twitter-sues-us-government-over-limits-on-ability-to-disclose-surveillance-orders/2014/10/07/5cc39ba0-4dd4-11e4-babe-e91da079cb8a_story.html.

154. *In re* Under Seal, 749 F.3d 276, 281 (4th Cir. 2014); *see also* Ladar Levison, *Secrets, Lies and Snowden's Email: Why I Was Forced to Shut Down Lavabit*, GUARDIAN (May 20, 2014, 7:30 AM), http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email. The government also refused Levison's offer to modify the code of his servers so that the government could use the encryption key without accessing all 400,000 of Lavabit's customers. *Id.* The government's request was issued shortly after Snowden first revealed the NSA's campaign of warrantless surveillance, and commentators have heavily speculated that the government sought access to Snowden's actual e-mail address. Glenn Greenwald, *Email Service Used by Snowden Shuts Itself Down, Warns Against Using US-Based Companies*, GUARDIAN (Aug. 9, 2013), http://www.theguardian.com/commentisfree/2013/aug/09/lavabit-shutdown-snowden-silicon-valley.

155. Parmy Olson, *Encryption App Silent Circle Shuts Down E-Mail Service 'To Prevent Spying'*, FORBES (Aug. 9, 2013, 12:41 PM), http://www.forbes.com/sites/parmyolson/2013/08/09/encryption-app-silent-circle-shuts-down-e-mail-service-to-prevent-spying/ (discussing how "Silent Circle" preemptively shut down its e-mail application after Lavabit's legal troubles).

156. *Privacy*, APPLE, http://www.apple.com/privacy/government-information-requests/ (last visited Aug. 5, 2015) ("So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8.").

157. Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

cause to properly conduct the search.[158] But given the uncertain standards behind these types of warrants and the government's relentless pursuit of security at the cost of privacy, this is just one example of the new Internet regime, by which the Internet industry actively *opposes* the government intelligence community, rather than working with them.[159]

The development of the standards required under ECPA also cuts in favor of law enforcement. When technology companies feel backed into a corner, they have demonstrated a willingness to completely remove the government's ability to obtain this information in the first place.[160] Rather than eliminating access to customer information altogether, the government should favor the development of clear precedent that allows prosecutors, ISPs, and users to understand what is necessary to obtain customer information.

The same reasons that justify ISPs in politically opposing the government also support ISPs opposing the government in the courts. The most direct way to change the standards required under ECPA—short of congressional intervention—is to appeal to the courts and develop binding law that endorses more stringent protections of user information. If these companies truly want reform, of both online privacy law and their own reputations, then they should actively oppose the government to create binding precedent under ECPA. If ISPs continue to remain complicit with government surveillance, however, then courts should look to other ways to encourage an adversarial system and create binding precedent.

### B. JUDGES CAN APPOINT COUNSEL IN SITUATIONS WHERE THE INTERESTS OF JUSTICE SO REQUIRE

Judges are responsible for appointing counsel in federal criminal cases when defendants are unable to pay for representation.[161] Prior to 1964, judges had to rely on the "professional obligation of lawyers" to provide pro bono representation to such defendants.[162] In order to establish a structured and comprehensive system for appointing and

158. Mike Masnick, *Law Enforcement Freaks Out Over Apple & Google's Decision To Encrypt Phone Info By Default*, TECHDIRT (Sept. 23, 2014, 11:18 AM), https://www.techdirt.com/articles/20140923/07120428605/law-enforcement-freaks-out-over-apple-googles-decision-to-encrypt-phone-info-default.shtml.

159. Mike Masnick, *Thank Snowden: Internet Industry Now Considers the Intelligence Community An Adversary, Not A Partner*, TECHDIRT (Feb. 13, 2015, 10:30 AM), https://www.techdirt.com/articles/20150213/07100730015/thank-snowden-internet-industry-now-considers-intelligence-community-adversary-not-partner.shtml.

160. *See* Masnick, *supra* note 158.

161. *Appointment of Counsel*, U.S. COURTS, http://www.uscourts.gov/FederalCourts/AppointmentOfCounsel.aspx (last visited Aug. 5, 2015).

162. *Id.*

compensating lawyers in these cases, Congress enacted the Criminal Justice Act ("CJA").[163]

The CJA states that if magistrate judges determine that the "interests of justice so require," they may appoint counsel for any "financially eligible person" who "is charged with a Class B or C misdemeanor, or an infraction for which a sentence to confinement is authorized."[164] A "financially eligible person" is defined as someone whose "net financial resources and income are insufficient to obtain qualified counsel."[165] In making such a determination, courts should resolve "any doubt" in that individual's favor, and erroneous determinations can be corrected after the fact.[166]

At least one magistrate judge has interpreted this language within the context of ex parte ECPA orders to grant authority to appoint CJA counsel for unnamed defendants, so as to provide a proper adversarial system.[167] That court decided to appoint CJA counsel—with government consent—for two reasons: (1) the standard to be applied in granting access to real time or prospective cell site information was an unsettled legal issue, and (2) that legal issue would continue to arise "each time the government submits an ex parte application for cell site information."[168] The court ultimately held that the government was not entitled to the sought data, but that the court would issue a warrant for "real time cell location information" if the government could show probable cause.[169] Likely for the reasons discussed above,[170] the government did not appeal.

Unfortunately, the court did not elaborate on its precise interpretation of how the CJA allowed it to appoint counsel.[171] One explanation is that the CJA creates a presumption that counsel may be appointed.[172] Because of the ex parte nature of the proceeding, the court was unable to inquire into the defendant's financial status to determine if she was "financially eligible" for CJA appointment of counsel.[173] But the CJA requires "any doubts" as to the defendant's finances to be resolved

163. *Id.*

164. 18 U.S.C. § 3006(A)(a)(2)(A) (2006).

165. Guide to Judiciary Policies and Procedures, Volume VIIA, Chapter II, § 210.40.30(a), Standards for Eligibility (2015).

166. *Id.*

167. *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register, 415 F. Supp. 2d 211, 212 (W.D.N.Y. Feb. 15, 2006) [hereinafter *In re Pen Register*].

168. Order at 1–2, *In re Pen Register*, 415 F. Supp. 2d 211 (No. 06-MJ-506).

169. *In re Pen Register*, 415 F. Supp. 2d at 219.

170. *See supra* Part II.C.

171. Order at 1, *In re Pen Register*, 415 F. Supp. 2d 211(No. 06-MJ-506).

172. *Id.* (considering the "interests of justice"); *see also* Guide to Judiciary Policies and Procedures, Volume VIIA, Chapter II, § 210.40.30(b) ("Any doubts as to a person's eligibility should be resolved in the person's favor; erroneous determinations of eligibility may be corrected at a later time.").

173. *In re Pen Register*, 415 F. Supp. 2d 211.

in favor of the defendant.[174] The court, therefore, was able to appoint counsel in this special circumstance. Although the court took the additional step of obtaining the government's consent to appoint counsel, this step was likely nothing more than the court's attempt to eliminate a possible future objection, not a requirement before appointing CJA counsel in the first place.[175] Congress should consider updating the language of ECPA to explicitly allow or deny CJA appointments in such cases.[176]

Until Congress explicitly resolves the matter, other judges should consider appointing CJA counsel to oppose the government in similar ex parte ECPA proceedings, when the interests of justice so require. In *In re Pen Register*, the court only appointed counsel after seven magistrate judges had already considered the issue with conflicting outcomes.[177] Moreover, the court took action because it expected the issue to continue to arise *each time* the government applied for one of these ex parte ECPA orders until a binding decision could be reached.[178] The goal of this appointment was not to eliminate such ex parte proceedings altogether, but rather it was to provide a proper adversarial relationship to consider the issue.[179] Thus, there should be no concern that the limited use of CJA appointments in these types of cases would swallow the rule.

The appointment of CJA counsel would remedy the main deficiency under ECPA, which is that targeted individuals do not receive notice of the government's ECPA application until it is too late to properly oppose it. CJA counsel would be able to oppose the government at the relevant time—before the application is granted—and would possess the procedural tools necessary to develop the law, including the right to appeal an adverse decision. More judges should consider appointing CJA counsel as a helpful solution to deal with recurring issues under ECPA.

### C. Congress Could Allow Courts to Appoint a Constitutional Advocate to Oppose the Government in Significant Cases

Within the context of FISA, members of the Senate Intelligence Committee recommended amending the Act to allow for the appointment

174. Guide to Judiciary Policies and Procedures, Volume VIIA, Chapter II, § 210.40.30(b).

175. Nothing in the CJA refers to the government's consent to appoint counsel, and there would likely be a conflict of interest if courts relied on the government when appointing counsel to oppose it.

176. Such an amendment is highly unlikely, given Congress' refusal to update the statutory scheme of ECPA. *See* Smith, *supra* note 17, at 259 ("Like an absentee landlord, Congress has all but ignored this widening breach since [geolocation monitoring] first came to its attention in 1994.").

177. *In re Pen Register*, 415 F. Supp. 2d at 212 (noting that at least seven prior decisions had considered the issue, of which five courts had rejected the government's request for real time cell site data and two courts had granted access to it).

178. Order at 1, *In re Pen Register*, 415 F. Supp. 2d 211(No. 06-MJ-506).

179. *In re Pen Register*, 415 F. Supp. 2d at 212–13. With the consent of the government, a "fictional" version of the government's application was used to ground the dispute. *Id.* at 213 n.2. This fictional application retained identical legal issues to the real application, and, presumably, it was only meant to avoid concerns about improperly notifying the targeted individual. *Id.*

of a Constitutional Advocate to oppose the government in secret proceedings before FISC.[180] Congress should consider establishing a similar Constitutional Advocate under ECPA who would be able to oppose the government and appeal adverse decisions.

Senator Patrick Leahy's proposal for a Constitutional Advocate under FISA ultimately produced the USA FREEDOM Act, which the House of Representatives passed in an attempt to reform portions of FISA in light of the Snowden revelations of 2013.[181] Although the bill was ultimately voted down in the Senate, it required FISA Courts to appoint an amicus curiae when, "in the opinion" of the court, the government request raised a "novel or significant interpretation of the law."[182] Had it passed, the USA FREEDOM Act would have certainly been at least one incremental step closer to the proper development of the law under FISA.

Critics of the USA FREEDOM Act, however, argued that it did not go far enough to enable adversarial opposition to the government in cases under FISA. For example, Judge James G. Carr argued that "an amicus participates solely for the court's benefit" and that the only way to achieve true reform was to appoint an attorney to represent the target directly.[183] His primary rationale was that "[u]nlike an amicus, an attorney would have standing on behalf of the target to appeal to the Foreign Intelligence Surveillance Court of Review."[184] These procedural difficulties are precisely why Senator Leahy's original proposal sought a Constitutional Advocate, and not simply the appointment of an amicus curiae.

The same problems outlined by critics under the USA FREEDOM Act already exist under ECPA's current statutory scheme. As is, courts have the discretion to invite amicus curiae to oppose the government in cases where they would like to hear additional arguments.[185] But there are many procedural hurdles that restrict these amici from truly opposing the government: amici cannot pursue discovery, access sealed filings, or raise claims that are not asserted by the parties.[186] Most importantly, amici cannot appeal when the court rules against them.[187]

---

180. Senators Mark Udall, Ron Wyden, Richard Blumenthal, and Rand Paul introduced the legislation. Intelligence Oversight and Surveillance Reform Act, S.1551, 113th Cong. (2013).

181. USA FREEDOM Act, H.R. 3361, 113th Cong. (2014).

182. *Id.*

183. James G. Carr, *Fixing What Ails the FISA*, HILL (July 24, 2014, 11:00 AM), http://thehill.com/blogs/congress-blog/judicial/213137-fixing-what-ails-the-fisa.

184. *Id.* Judge Carr also argued that if Congress was unwilling to authorize counsel before FISA courts, then it should instead consider an alternative procedure that would enable an amicus to certify questions for FISCR review. *Id.*

185. *See* Linda Sandstrom Simard, *An Empirical Study of Amici Curiae in Federal Court: A Fine Balance of Access, Efficiency, and Adversarialism*, 27 REV. LITIG. 669, 687 (2008).

186. Smith, *supra* note 2, at 330.

187. *Id.*

For example, in *In re Application of the U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, the government originally claimed that it only sought "single-tower and sector [] records," which the government clarified did not include GPS, "triangulation," registration, or duration information because that information was rarely available "for past time periods."[188] At oral arguments, the government stated that location data would only be recorded when actual calls were placed.[189] But in fact, the precise nature of *what* the government sought—that is, whether the location data was available only when calls were placed or whether it was continuously available—was at issue from the start of the ex parte proceedings.[190] Because the amici had no procedural rights, however, the most they could do was argue that the Third Circuit should remand for an evidentiary hearing.[191] And when the Third Circuit's opinion focused on "historical cellular tower data . . . (including, without limitation, call initiation and termination . . . call handoffs, *call durations, registrations, and connection records*)," there was no way for the amici to appeal the court's holding.[192] This example demonstrates the procedural shortfalls that ultimately restrict the development of binding appellate decisions.[193]

Although the USA FREEDOM Act was ultimately not adopted under FISA, Congress should consider a similar amendment in the context of ECPA to foster the development of binding precedent. A Constitutional Advocate could oppose the government and assert the

188. Gov't Memorandum of Law in Support of Request for Review at 25, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (No. 08-4227) 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008); Brief for the United States at 15, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*,* 620 F.3d 304 (No. 08-4227), 2009 WL 3866620 ("No Global Positioning System ('GPS') data or other more precise location information (such as 'triangulation' data) is contained in the historical records pursuant to the application.").

189. Oral Argument at 30:30-31:00, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (No. 08-4227), *available at* http://www2.ca3.uscourts.gov/oralargument/audio/08-4227-ApplicationofUSA.wma.

190. *In re* Application of the U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 590 (W.D. Pa. Feb. 19, 2008) (noting that cell phones will scan for the "strongest signal/best reception," known as "registration," which can provide location data *every seven seconds*); *see also* Freiwald, *supra* note 23, at 711 (noting that carriers often store location data to help manage their networks and facilitate location applications, and that ISPs are not obligated to filter out this data when providing information to the government).

191. Brief of Amici Curiae Electronic Frontier Foundation, et al. at 22, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (No. 08-4227), 2009 WL 3866619.

192. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*,* 620 F.3d at 308 (emphasis added). The Third Circuit's holding was ultimately a middle ground. Although ECPA did not *mandate* a warrant for all § 2703(d) orders seeking cell site information, magistrate judges could, in their discretion, require a warrant before granting such orders. *Id.* at 319.

193. *See supra* Part III.B.

third-party rights of a targeted individual in cases that involve a significant issue under ECPA. Congress would need to identify how many of these positions would be necessary to properly oppose the government, but the advocate would be a governmental officer who steps in to represent the third-party interests of targeted individuals when the court deems it appropriate, similar in this way to the appointment of a public defender.[194] A Constitutional Advocate would remedy the procedural shortcomings faced by amici that lack the ability to appeal adverse decisions.

Moreover, given that the House of Representatives proposed such an advocate in the context of FISA, Congress should be even more willing to allow a Constitutional Advocate to oppose to the government under ECPA. Whereas FISA deals with significant issues of national security that require increased secrecy,[195] ECPA is a general privacy statute that applies outside of the national security context. Thus, while increased opposition might decrease the level of secrecy surrounding ECPA proceedings, this concern is less relevant to the ultimate purpose of the Act.

To the extent Congress would be concerned that a Constitutional Advocate would unduly burden ECPA's statutory scheme, Congress could look to two examples to narrow when courts should appoint a Constitutional Advocate. First, Congress could simply use the House of Representative's own language under the USA FREEDOM Act, which required a court to be faced with a "novel or significant interpretation of the law" before it could invoke a Constitutional Advocate. Second, Congress could direct courts to the same principles that prompted the judge in *In re Pen Register* to appoint CJA counsel, meaning that an unsettled legal issue would "continue to arise each time the government submits an ex parte application" for that type of information.[196] Under either approach, the Constitutional Advocate would reinvigorate the adversarial nature of these proceedings, where important constitutional questions are likely to recur, without unduly bogging down ex parte applications.

Further, a Constitutional Advocate would have all of the procedural tools that are necessary to create a proper adversary system. Most importantly, as a direct party to the action, this Constitutional Advocate

194. A public defender, like CJA counsel, is the actual attorney for the targeted individual. By contrast, a Constitutional Advocate would be a government position that steps in to oppose the government and represent the third-party interests of the targeted individual. But Congress could consider the structure of how public defenders are assigned in order to determine how Constitutional Advocates are assigned to particular cases and how many advocates would be necessary.

195. [Redacted], 2011 WL 10945618, at *24 (holding that the acquisition of foreign intelligence information pursuant to § 702 of FISA falls within the "foreign intelligence exception" to the Fourth Amendment because "national security" goes beyond garden-variety law enforcement objectives).

196. Order Appointing Counsel at 2, *In re Pen Register*, 415 F. Supp. 2d 211 (No. 06-MJ-506).

would have the ability to appeal decisions and foster the development of binding interpretations of the Fourth Amendment as it relates to electronic communications. But as the next Part will discuss, there are Article III standing requirements that would need to be satisfied in order for a Constitutional Advocate to represent third-party rights of a targeted individual.

## V. A CONSTITUTIONAL ADVOCATE COULD ASSERT *JUS TERTII* STANDING FOR TARGETED INDIVIDUALS

If such a Constitutional Advocate were appointed to oppose the government in these types of proceedings, courts should determine that they have standing to represent the interests of targeted individuals.[197] Ex parte proceedings already go against the general structure of our judicial system, and a Constitutional Advocate would only effectuate the guiding principles under the case or controversy limitations of Article III.

A party is entitled to be heard in federal court only when she has alleged a personal stake in the outcome of the controversy, ensuring an adversarial proceeding.[198] In order to establish this Article III standing, a litigant must satisfy both constitutional and prudential requirements. To satisfy the constitutional requirements, a litigant must show: (1) that she has suffered a concrete and particularized injury, (2) the cause of which is fairly traceable to the defendant's allegedly unlawful conduct, (3) which is likely to be redressed by the requested relief.[199] There is no doubt that targeted individuals would have standing to oppose the government, as their liberty interests are directly implicated by such proceedings.

The relevant issue, however, is whether such a Constitutional Advocate could represent the targeted individual in the context of an ex parte ECPA application. The prudential requirement relevant to a Constitutional Advocate is that of *jus tertii* standing, which provides that, generally, litigants cannot assert the legal rights of third parties not before the court.[200] The Supreme Court has allowed litigants to bring actions on behalf of third parties, provided three criteria are met: (1) the litigant must have suffered an injury-in-fact, (2) the litigant must have a close relation to the third party, and (3) a hindrance must exist, such that the third party cannot protect his or her own interests.[201] In order for a

197. *See* Matthew I. Hall, *Standing of Intervenor-Defendants in Public Law Litigation*, 80 FORDHAM L. REV. 1539, 1562 ("The standing to defend of intervenor-defendants thus becomes a determinative issue in a relatively small number of cases: primarily, those in which the intervenor seeks appellate review of a trial court judgment not appealed by the original defendant . . . .").

198. Flast v. Cohen, 392 U.S. 83, 99 (1968); *see also* U.S. CONST. art. III, § 3.

199. Allen v. Wright, 468 U.S. 737, 751 (1984).

200. Barrows v. Jackson, 346 U.S. 249, 255 (1953) ("Apart from the jurisdictional requirement, this Court has developed a complementary rule of self-restraint . . . which ordinarily precludes a person from challenging the constitutionality of state action by invoking the rights of others.").

201. Powers v. Ohio, 499 U.S. 400, 410–11 (1991).

court to find that the Constitutional Advocate can assert *jus tertii* standing, the advocate would need to be able to satisfy each of these three requirements.

Before addressing how a Constitutional Advocate would satisfy these requirements, it would be helpful to recognize an exception that *does not* apply here. Specifically, the Supreme Court's prohibition of one defendant asserting the Fourth Amendment rights of another would-be defendant.[202] When deciding a case against Defendant A, and presenting evidence obtained from Defendant B, the court need not determine whether evidence was obtained as part of an illegal search conducted upon Defendant B. The Court has explicitly stated that the analysis within these types of cases falls "under the heading of substantive Fourth Amendment doctrine," and does not fall under "the heading of standing."[203] In the context of this Note, however, the issue is purely whether Congress may appoint a Constitutional Advocate who can assert the rights of third parties. This is distinct from the issue of whether one *defendant* may question the validity of a search upon another would-be defendant.[204]

### A. A Constitutional Advocate Would Have the Requisite "Injury-In-Fact" for Purposes of Asserting the Rights of a Third Party

In order to assert *jus tertii* standing, the Supreme Court first requires that the litigant must have an injury-in-fact.[205] This requirement ensures a "concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination of difficult constitutional questions."[206] However, the Supreme Court has recognized injuries under *jus tertii* standing that would not typically satisfy a "particularized injury" under traditional Article III standing, suggesting the injury requirement is lower in this context.

As an example of this relaxed injury requirement, consider *Powers v. Ohio*. There, the Court held that improper jury selection caused a "cognizable injury" to the defendant, and therefore the defendant had a

202. *See* Rakas v. Illnois, 439 U.S. 128, 150 (1978) (affirming the defendant's conviction because it was unnecessary to decide whether the search violated the rights secured to someone else by the Fourth and Fourteenth Amendments). *But see Powers*, 499 U.S. at 411 ("These criteria have been satisfied in cases where we have permitted criminal defendants to challenge their convictions by raising the rights of third parties.").

203. *Rakas*, 439 U.S. at 140.

204. As Justice Scalia's dissent in *Powers* highlights, one party asserting the rights of another is distinct. *Powers*, 499 U.S. at 428 (Scalia, J., dissenting). To the extent there is overlap between the issues, the majority opinion in *Powers* has long favored allowing the assertion of a third party's rights, so long as the requisite elements are met. *Id.* at 410–11.

205. *Id*. at 411.

206. United States v. Windsor, 133 S. Ct. 2675, 2687 (2013) (quoting Baker v. Carr, 369 U.S. 186, 204 (1962)).

"concrete interest in challenging the practice."[207] It seems logical that a criminal defendant, whose ultimate liberty is at issue, would obviously have a "concrete interest" in asserting a juror's third-party rights. According to the Court, however, the injury did not stem from the juror's potential disposition in the case.[208] Rather, the injury existed because racial discrimination "casts doubt on the integrity of the judicial process" and places the "fairness of a criminal proceeding in doubt."[209] Such "doubt" would not usually be the type of "particularized injury" required under Article III,[210] and thus, the rationale underlying *Powers* is that the injury requirement is less substantial when asserting a third party's rights than if a litigant were simply asserting her own rights.[211]

Moreover, the Supreme Court has relaxed this prong in the context of Freedom of Information Act ("FOIA") requests, where there is no articulated injury at all, suggesting that the injury prong may be relaxed even further when appropriate.[212] FOIA allows individuals to petition the government for certain records, and the statute provides a cause of action if these records are not provided "in a timely manner."[213] The Supreme Court has repeatedly held that any litigant may petition the courts for such records, regardless of their reasons or justification for doing so.[214] One observer has noted that this precedent has led to a line of cases—the "birther" cases[215]—that would otherwise be considered a prohibited "generalized grievance."[216] This suggests that the injury threshold may be lowered when appropriate.

One example of where it would be appropriate to relax the injury prong is when a government official represents the interests of third

207. *Powers*, 499 U.S. at 411.

208. *Id.*

209. *Id.*

210. *See* Allen v. Wright, 468 U.S. 737, 751 (1984).

211. *See Powers*, 499 U.S. at 427 (Scalia, J. dissenting) ("[H]ow do these alleged perceptions of unfairness, these 'castings of doubt' and 'invitations to cynicism,' establish that the defendant has been injured *in fact*? They plainly do not." (quotations and emphasis in original)); *see also Windsor*, 133 S. Ct. at 2687 (quoting Warth v. Seldin, 422 U.S. 490, 500–01 (1975) ("In some circumstances, countervailing considerations may outweigh the concerns underlying the usual reluctance to exert judicial power when the plaintiff's claim to relief rests on the legal rights of third parties.")).

212. Evan Tsen Lee & Josephine Mason Ellis, *The Standing Doctrine's Dirty Little Secret*, 107 NW. U. L. REV. 169, 172 (2012) ("[Justice Scalia] could have cited even more devastating proof that Congress sometimes has the power to relax or eliminate other supposed minimum requirements of the Article III standing doctrine—including injury-in-fact.").

213. 5 U.S.C. § 552(a)(6)(E)(iii) (2006).

214. *See, e.g.*, NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 220 (1978) ("[U]nless the requested material falls within [a] statutory exemption[], FOIA requires that records and material in the possession of federal agencies be made available on demand to any member of the general public.").

215. Litigants have repeatedly attempted to use FOIA to petition the government for copies of President Obama's birth certificate. *See, e.g.*, Taitz v. Ruemmler, No. 11-1421, 2011 WL 4916936, at *1 (D.D.C. Oct. 17, 2011), *aff'd*, No. 11-5306, 2012 WL 1922284 (D.C. Cir. 2012) (per curiam).

216. Lee & Ellis, *supra* note 211, at 196–97 ("The 'birther' cases are a prime example of the generalized grievances that federal courts are willing to entertain in the name of FOIA.").

parties.[217] Consider the Supreme Court's decision in *United States v. Windsor*, where the Court upheld standing for the Bipartisan Legal Advisory Group—comprised of members of the House of Representatives—after the Obama Administration refused to defend the constitutionality of the Defense of Marriage Act.[218] The Court's holding was the exact opposite as that in its sister case, *Hollingsworth v. Perry*, where the Court held that presenters of a state ballot initiative did not have standing to defend the constitutionality of Proposition 8.[219] The primary difference between these two cases was that the litigants in *Windsor* were members of the government, whereas the litigants in *Hollingsworth* were little more than "concerned bystanders" that had brought the ballot initiative just as any citizen in California could.[220]

Here, these same considerations should weigh in favor of allowing a Constitutional Advocate to represent the interests of a targeted individual. Above all, a Constitutional Advocate is necessary to preserve the adversarial nature of ECPA orders and develop the law. Given that "integrity of the judicial process" and "fairness" drove the Court's decision in *Powers*,[221] the injury prong should similarly be satisfied here. Ultimately, a Constitutional Advocate is needed because of the inherent unfairness to defendants that are unable to adequately oppose ECPA applications before they are granted.[222] And without appellate review, the integrity of the judicial process in ex parte ECPA proceedings will inevitably be called into question.[223]

Like the litigants in *Windsor*, a Constitutional Advocate would be an official position within the government that could be appointed at the court's discretion in cases that focus on significant issues under ECPA.[224]

---

217. *Compare Windsor*, 133 S. Ct. at 2688–89 (holding that members of Congress had standing to defend the Defense of Marriage Act when the U.S. Executive Branch refused to defend it), *with* Hollingsworth v. Perry, 133 S. Ct. 2652, 2663 (2013) (holding that individuals who had first put forth a ballot initiative did not have standing to defend Prop 8 when the California Executive Branch refused to defend it).

218. *Windsor*, 133 S. Ct. at 2688–89.

219. *Perry*, 133 S. Ct. at 2663. Proposition 8 was a voter-enacted ballot initiative that amended the California Constitution to provide that only marriage between a man and a woman was valid, thereby eliminating the right of same-sex couples to marry. *Id.* at 2659.

220. *Compare Windsor*, 133 S. Ct. at 2688–89 (upholding standing for members of Congress to support § 3 of the Defense of Marriage Act), *with Perry*, 133 S. Ct. at 2663 (denying standing because "Petitioners here hold no office and have always participated in this litigation solely as private parties").

221. *See* Powers v. Ohio, 499 U.S. 400, 411 (1991).

222. *See supra* Part II.

223. *See supra* Part II.C; *see also* Smith, *supra* note 2, at 326 ("[E]xcessive secrecy effectively shields electronic surveillance orders from appellate review, thereby depriving the judiciary of its normal role in shaping, adapting, and updating legislation to fit changing factual (and technological) settings over time.").

224. As a point of comparison, consider Federal Public Defendant Organizations, which are "federal entities, and their staffs are federal employees." *Appointment of Counsel*, *supra* note 161 ("The chief federal public defender is appointed to a four-year term by the court of appeals of the circuit in which the organization is located."). Similarly, *ex relatione* cases most commonly allow the government

Courts have consistently made these types of discretionary decisions to either appoint counsel or call for amicus curiae briefs, which is an easy analogy courts can rely upon to identify situations in which this advocate should be invoked.[225] Thus, the same considerations that led the Supreme Court to relax this prong in *Windsor* should be persuasive here as well.

Courts should be willing to determine that such a Constitutional Advocate satisfies the injury-in-fact prong of this prudential prohibition because it would facilitate the adversarial process, which currently does not exist in ex parte ECPA proceedings. This injury prong is less relevant here, where the Constitutional Advocate would be an official government position.

### B. A Constitutional Advocate Would Have the Requisite "Close Relation" with the Targeted Individual

The second requirement of *jus tertii* standing is that the litigant must have a "close relation" with the third party, so that the litigant can effectively represent the third party.[226] This close relation has never been a high threshold to meet.[227] For example, in *Powers*, the Supreme Court found a close relation between a criminal defendant and an excluded juror whom he had *never met*.[228] This close relation was primarily because of their shared goal of eliminating racial discrimination from the courtroom.[229] Similarly, the Court found the close relation requirement was met between a beer vendor and his potential customers, when he asserted the rights of his male beer-consuming customers against an Oklahoma law that allowed men and women to purchase beer at different ages.[230] Because this factor focuses on the shared interests of the parties, and not necessarily their literal relationship, this requirement is a relatively low threshold to satisfy.

Here, a Constitutional Advocate's sole duty would be to oppose the government in otherwise-ex parte requests under ECPA, which she could do more effectively than the targeted individual. Similar to *Powers*, both the Constitutional Advocate and the third party would have the

---

to bring a claim for private parties with an interest in the matter. Black's Law Dictionary 248 (9th ed. 2009). This suggests that standing requirements are more relaxed when the government itself intervenes as a party. *See generally Windsor*, 133 S. Ct. 2688–89 (holding that members of Congress satisfied Article III standing to defend the Defense of Marriage Act).

225. *See* Simard, *supra* note 184, at 687.

226. *Powers*, 499 U.S. at 411.

227. *Id.* at 413 ("In certain circumstances, the relationship between the litigant and the third party may be such that the former is fully, or very nearly, as effective a proponent of the right as the latter." (quoting Singleton v. Wulff, 428 U.S. 106, 113 (1976) (internal quotation marks omitted))).

228. *Id.*

229. *Id.* at 413–14 ("Both the excluded juror and the criminal defendant have a common interest in eliminating racial discrimination from the courtroom . . . . This congruence of interests makes it necessary and appropriate for the defendant to raise the rights of the juror.").

230. Craig v. Boren, 429 U.S. 190, 197 (1976).

shared interest of opposing the government to ensure the requirements of ECPA and the Fourth Amendment were satisfied as well.

Because of the secrecy proceedings surrounding ECPA, it would be largely impossible for the Constitutional Advocate to establish a literal relationship with the targeted individual.[231] But that type of literal relationship has not been required by the Supreme Court under *Powers* or *Craig v. Boren*.[232] And more importantly, a Constitutional Advocate would be able to oppose the government without doing harm to the secrecy proceedings that Congress has deemed necessary to facilitate obtaining these electronic communications. For proponents of ECPA, this is a far more effective and efficient outcome than allowing targeted individuals to oppose the government themselves. As a result of the shared common goal between the Constitutional Advocate and the targeted individual, there would be enough of a "close relation" to satisfy *jus tertii* standing under *Powers*.

### C. Targeted Individuals Are "Hindered" from Representing Their Own Interests

The third requirement of *jus tertii* standing requires that some hindrance must exist, which prevents third parties from asserting their own interests.[233] This is still satisfied where the third party could, but as a practical matter usually does not, bring a suit.[234] In *Powers*, for example, although jurors who were improperly dismissed on account of their race had the "legal right to bring suit on their own behalf," the Court allowed the defendant to assert their interests because "[a]s a practical matter, [] these challenges are rare."[235] The Court found this especially persuasive because of "the small financial stake involved and the economic burdens of litigation."[236] Thus, this requirement does not require that third parties be completely barred from preventing their own rights, but rather only requires that some barrier exists that makes asserting those rights more difficult.

Here, as discussed above,[237] the targeted individual has no opportunity to oppose the government before these ECPA orders are granted. The entire reason a Constitutional Advocate would be helpful in ECPA proceedings stems from the fact that targeted individuals are unable to assert their own interests, as shown by the thousands of ECPA orders

231. *See supra* Part II.B.
232. *See Powers*, 499 U.S. at 411; *see also Craig*, 429 U.S. at 194.
233. *See Powers*, 499 U.S. at 411.
234. *Id.* at 414.
235. *See id.*
236. *Id.* at 415.
237. *See supra* Part II.B.

that go unopposed and unappealed each year.[238] Even though a targeted individual could theoretically assert her own defense against the government, the reality of ECPA's statutory scheme is that defendants will rarely be incentivized to mount a criminal defense or a civil claim.[239] As demonstrated by *Powers*, this type of hindrance is precisely what the Court had in mind when contemplating this requirement.[240]

As a result, each of the prudential requirements of *jus tertii* standing—(1) that the litigant suffers an injury-in-fact; (2) that the litigant shares close relation with the third party; and (3) that some hindrance exists to prevent the third party from asserting their own rights—would be satisfied to establish an exception to the general prohibition against representing the interests of third parties. First, a Constitutional Advocate would be an official position within the government, making it appropriate for courts to lower the injury-in-fact requirement. And similar to the injury upheld in *Powers*, the specific injury here would stem from the unfairness of ex parte ECPA proceedings and the resulting loss of integrity within the judicial system. Second, a Constitutional Advocate would share with the litigant an interest in opposing the government and adequately developing arguments in support of constitutional protections of the targeted individual's information. Third, a Constitutional Advocate would remedy the practical reality that targeted individuals are rarely able to mount a constitutional defense to oppose the government after their information has already been obtained. Because each of these three factors would be satisfied, a Constitutional Advocate would be able to assert *jus tertii* standing to represent the interests of targeted individuals in otherwise-ex parte ECPA proceedings.

## CONCLUSION

Privacy law in the United States has stagnated because the government has remained willfully ignorant as to how the Fourth Amendment relates to burgeoning electronic communications. A primary reason for this stagnation is because the government pursues ECPA orders ex parte, and there are few remedies to protect a targeted individual once the information is obtained.

The solution is to increase opposition to the government in these otherwise-ex parte proceedings. Whether that is achieved by ISPs resisting

238. *Id.*

239. When faced with criminal charges, a defendant will rarely pursue the civil remedies available for a violation of the statute. Kerr, *supra* note 35, at 818. Moreover, in order to suppress evidence obtained in violation of ECPA, the defendant would have to successfully demonstrate a violation of the Fourth Amendment and overcome a good faith defense from the law enforcement official in order to suppress the information. United States v. Leon, 468 U.S. 897, 922 (recognizing a good faith exception to the suppression of improperly obtained evidence). The practical outcome is that defendants rarely oppose the government under either avenue. *See supra* Part II.C.

240. *See Powers*, 499 U.S. at 414–15.

government applications for user information, by courts appointing CJA counsel to represent the targeted individual, or by the appointment of a Constitutional Advocate, the end result would be an adversarial proceeding that would help develop the issues before the courts. Moreover, each of these three parties has the key tool necessary to develop the law: the right to appeal adverse decisions.

The only way to incentivize the development of Fourth Amendment protections is to allow parties to oppose the government with full procedural rights and develop binding appellate precedent. Appointment of a Constitutional Advocate would restore the adversarial nature of these proceedings and protect against the wanton disclosure of targeted individuals' information.