Where Have All the Emails Gone: A Journalist's Fight to Expose Use of PATRIOT Act Tools on US Citizens

Claire Cahoon[1]

I. INTRODUCTION

Jason Leopold, a journalist ominously known to government officials as the "FOIA Terrorist," is more familiar than most with rejection from the United States government.[2] A 2018 Pulitzer finalist and industry-celebrated expert on the Freedom of Information Act (FOIA), Leopold has filed more FOIA lawsuits than any other journalistic entity except the New York Times, and usually, the courts side with the government and refuse his requests for disclosure.[3] A notable exception is a lawsuit he initially believed to be innocuous but resulted in the release of Hillary Clinton's emails before the 2016 presidential election.[4]

In 2013, Leopold ventured beyond his typical FOIA requests and filed a request for disclosure of materials related to pen registers, trap and trace devices, and Stored Communications

---

1. Claire Cahoon is a 2020 candidate for Juris Doctor from SMU Dedman School of Law. She received a Bachelor of English from the University of Southern California in 2017.

2. Michael Morisy, *Requester's Voice: Jason Leopold*, MUCKROCK (July 12, 2013), https://www.muckrock.com/news/archives/2013/jul/12/jason-leopold-foia-terrorist-shares-his-transparen/.

3. *Jason Leopold*, BUZZFEED, https://www.buzzfeed.com/jasonleopold (last visited Oct. 23, 2018); Benjamin Mullin, *BuzzFeed News hires 'FOIA terrorist' Jason Leopold from VICE News*, POYNTER (Jan. 3, 2017), https://www.poynter.org/news/buzzfeed-news-hires-foia-terrorist-jason-leopold-vice-news; Interview with Jason Leopold, Senior Investigative Reporter, BuzzFeed News (Sept. 26, 2018).

4. Jason Leopold, *How I Got Clinton's Emails*, VICE NEWS (Nov. 4, 2016), https://news.vice.com/en_us/article/j5vevy/clinton-email-scandal-foia; Interview with Jason Leopold, *supra* note 3; Complaint, Leopold v. Dep't of State, No. 1:15-cv-00123 (D.D.C. 2018).

Act (SCA) materials.[5] The D.C. District Court (D.D.C.) left the matter virtually untouched until 2016, when U.S. District Judge Richard Roberts, facing allegations of sexual assault and predatory misbehavior, stepped down from the D.D.C.[6] Judge Howell, Robert's replacement, quickly picked the case up. Leopold, with support from the Reporters Committee for the Free Press, has spent the last two years negotiating the release of these materials with the US Attorney's Office (USAO).[7]

In the latest iteration of this saga, the D.D.C. incorrectly held that the SCA does not create a First Amendment right of access to records related to SCA warrants in closed cases.[8] To come to this conclusion, the court engaged in a misguided debate about whether an SCA warrant ought to be treated as a traditional warrant or a subpoena.[9] To this end, the court determined that: (1) SCA warrants function more like subpoenas than warrants and (2) the SCA's use of the term "warrant" does not indicate that SCA warrants ought to be treated like traditional warrants.[10] The court came to these conclusions despite the CLOUD Act, which amended the SCA to create a framework for extraterritorial access to stored data.[11]

---

5. Petition at 1, In re Leopold (*Leopold II*), 327 F. Supp. 3d 1 (D.D.C. 2018) (No. 1:13-mc-00712).

6. Carrie Johnson, *Federal Judge Retires As 'Bad Lapse In Judgment' With 16-Year-Old Surfaces*, NPR (Mar. 18, 2016), https://www.npr.org/2016/03/18/470852225/federal-judge-retires-as-bad-lapse-in-judgment-with-16-year-old-surfaces.

7. *See* Memorandum of Points and Authorities In Support of the Motion to Intervene and Petition to Unseal of the Reporters Committee for Freedom of the Press, In re Leopold, 327 F. Supp. 3d 1 (D.D.C. 2018) (No. 1:13-mc-00712).

8. *See generally Leopold II*, 327 F. Supp. 3d at 1.

9. *Id.* at 8–16.

10. *Id.*

11. Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Div. V; *Leopold II*, 327 F. Supp. 3d at 12.

Even though the SCA specifically uses the term "warrant," many courts make the argument that SCA warrants might not truly be warrants as an escape mechanism from the presumption against extraterritoriality. However, using this escape mechanism is dangerous when applied to First Amendment rights, as it gives the government unprecedented ability to search and seize information without ever disclosing the circumstances surrounding those seizures. The D.D.C. improperly applied a Fourth Amendment analysis to the First Amendment issues presented by this case. Additionally, the court wildly misinterprets the legislative intent behind the SCA and subsequent amendments, including the CLOUD Act.

In this case note, I examine *In re Leopold* in the context of the history of the SCA, the implications of SCA extraterritoriality, the recent amendments to the SCA, and relevant case law. Whether an SCA warrant functions more like a warrant or a subpoena has been examined extensively by the DC Circuit and other courts, but not in the context of the right of access under the First Amendment.[12]

II. FACTUAL AND LEGAL BACKGROUND

A. Factual Background

In July of 2013, Jason Leopold, a journalist currently employed by BuzzFeed, filed an application with the United States District Court for the District of Columbia to: (1) "make public applications to and orders of the Court regarding pen registers, trap and trace devices, cell site location, stored email, telephone logs, and customer account records from electronic service

12. *See* Microsoft Corp. v. United States (*Microsoft II*), 829 F.3d 197, 214–15 (2d Cir. 2016); Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm'n, 715 F.3d 631, 646 (7th Cir. 2013); In re Info. Associated with @gmail.com, No. 16-mj-00757, 2017 U.S. Dist. LEXIS 130153, at *49–53 (D.D.C. July 31, 2017)

; In re Search Warrant No. 16-960-M-01, 232 F. Supp. 3d 708, 720–22 (E.D. Pa. 2017); Matter of 381 Search Warrants Directed to Facebook, Inc., 78 N.E.3d 141, 146–47 (N.Y. 2017).

providers"; (2) make public docket numbers, in closed investigations, associated with government applications and orders relating to PR/TT devices; and (3) prospectively compel disclosure after 180 days for all sealing of non-disclosure orders for such materials, extendable for ongoing investigations or exceptional circumstances.[13] This case note is primarily concerned with the requested SCA materials.

Leopold's motive in requesting these materials is twofold.[14] First, he seeks to make the frequency and purpose of these methods public.[15] From the minimal disclosure he has already seen, Leopold knows the government is using these methods to track ordinary people accused of ordinary crimes.[16] "Perhaps that's something that the legal community is like, of course it's used for that," Leopold says, "but I think when it comes to surveillance tools, the public is led to believe it's being used for reasons of national security."[17] Second, Leopold hopes to set a precedent for other courts to proactively post information relating to these materials on their websites.[18]

In response to Leopold's initial petition, the USAO expressed that request for relief was overbroad and presented too many obstacles.[19] When the case was revived in early 2016, Leopold's counsel, joined by counsel for the Reporters Committee, began lengthy negotiations

---

13. *See* In re Leopold (*Leopold I*), 300 F. Supp. 3d 61, 68 (D.D.C. 2018).

14. Interview with Jason Leopold, *supra* note 3.

15. *Id.*

16. *Id.*

17. *Id.*

18. *Id.*

19. This is a stance which Leopold "finds[s] to be bullshit, because it's not [his] problem." Interview with Jason Leopold, *supra* note 3. *See* United States' Response to Application to Unseal Records at 3; *In re Leopold*, 327 F. Supp. 3d at 1.

with the USAO.[20] Petitioners agreed to narrow their requests, and the USAO agreed to release very limited information on the total number of warrants, other orders, and limited docket information regarding these orders.[21] Despite these negotiations, the parties reached a stalemate and asked the D.D.C. to resolve the issue.[22]

The court's first Memorandum Opinion held that the common law afforded a limited prospective right of access to the information the USAO agreed to release.[23] However, the court held that the petitioners' First Amendment right of access claims fail, as does any claim of retrospective right of access under common law.[24] Notably, in this opinion, the court raised the issue of whether SCA warrants ought to be treated like warrants or subpoenas for First Amendment purposes sua sponte.[25] The court cited several cases which have addressed this SCA warrant/subpoena issue, but all those cases have addressed the issue from a Fourth Amendment extraterritoriality perspective.[26] Such cases have been contentious, to put it lightly, most recently

20. *See Leopold I*, 300 F. Supp. 3d at 69–79.

21. *Id.*

22. *Id.* at 79.

23. *See generally id.* at 69–79.

24. *Id.* at 108.

25. *Id.*

26. *See, e.g.*, *Big Ridge, Inc.*, 715 F.3d at 631, 646; In re Info. Associated with @gmail.com, 2017 U.S. Dist. LEXIS 130153, at *49–53; In re A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. (*Microsoft I*), 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

causing the legislature to intervene and amend the SCA before the Supreme Court could rule on the issue.[27]

B. Stored Communications Act

The Stored Communications Act was enacted in 1986 to "update and clarify Federal privacy protections and standards."[28] The legislature found an update to be especially urgent because advances in communication and surveillance had "expanded dramatically the opportunity for . . . [government] intrusion into the 'houses, papers, and effects' protected by the Fourth Amendment."[29] In its original iteration, 18 U.S.C. § 2703(b)(1)(A) described a SCA warrant as "a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant."[30] Following the terrorist attacks of September 11, 2001, the legislature amended § 2703(b)(1)(A) through the PATRIOT Act to read, "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of State court, issued using State Warrant procedures)" to mitigate "investigative delays caused by the cross-jurisdictional nature of the Internet."[31]

The SCA was amended again by the CLOUD Act on March 23, 2018, barely three weeks before the Supreme Court was set to determine whether the Second Circuit properly held that SCA

---

27. Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Div. V; United States v. Microsoft Corp. (*Microsoft III*), 138 S. Ct. 1186 (2018); Sarah Aitchison, Comment, *Privacy in the Cloud: The Fourth Amendment Fog*, 93 Wash. L. Rev. 1019, 1027–28 (2018).

28. S. REP. NO. 99-541, at 1 (1986).

29. *Id.* at 2.

30. *Id.* at 38.

31. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, sec. 212, 115 Stat. 272, 284–85 [hereinafter PATRIOT Act].

warrants do not apply extraterritorially.[32] Instead of waiting for the Court to rule, Congress created an exception to the presumption against extraterritoriality for all SCA orders.[33] In addition to creating a comity analysis for sharing data between foreign countries, the Act provides:

> "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter . . . regardless of whether such communication, record, or other information is located within or outside of the United States."[34]

C. D.C. District Court Arguments in *In Re Leopold* Memorandum Opinion

The D.D.C.'s most recent Memorandum Opinion regarding *In Re Leopold* was released in August 2018, after the CLOUD Act's enactment.[35] In its opinion, the court addresses many issues regarding the First Amendment right of access analysis, the Privacy Protection Act, and other matters that are mostly beyond the scope of this case note.[36] However, the analysis for the First Amendment right of access must be briefly explained to understand why the court raises the warrant vs. subpoena argument. Whether materials are subject to a First Amendment right of access is analyzed through a two-part "experience and logic" test.[37] The D.D.C. has previously

---

32. Consolidated Appropriations Act, Div. V; *Microsoft Corp.* (*Microsoft III*), 138 S. Ct. at 1187–88.

33. Consolidated Appropriations Act, Div. V.

34. *Id.*

35. *Leopold II*, 327 F. Supp. 3d at 12.

36. *See generally Leopold II*, 327 F. Supp. 3d 1.

37. *See* Press-Enterprise II, 478 U.S. 1, 8–9 (1986); United States v. Brice, 649 F.3d 793 (D.C. Cir. 2011).

held that warrants meet the "experience" requirement.[38] In this case, the court held that because SCA warrants are not traditional warrants, they are subject to an "experience and logic" analysis of their own, and because there is no historic right of access to these materials, SCA warrants have no First Amendment right of access.[39] To establish that SCA warrants are not traditional warrants for First Amendment purposes, the court uses the same analysis that it and other courts have used to determine whether SCA warrants may be applied extraterritorially for Fourth Amendment purposes.

i. Warrants are more akin to subpoenas than traditional warrants.

Arguing that providers' ability to challenge SCA warrants is a sufficient stand-in for targets' ability to challenge, the court holds that SCA warrants are more functional to subpoenas than to traditional warrants.[40] According to the court, providers' risk of civil liability, if they fail to challenge an insufficient SCA warrant, place providers in the target's shoes, thereby negating the target's interest in challenging an improper warrant.[41] The court acknowledges that this is not a perfect solution but bafflingly allows this argument to factor in favor of treating an SCA warrant like a subpoena.[42]

The court then runs through what it sees as a multitude of differences in the execution of SCA warrants and traditional warrants.[43] First, the court says SCA warrants always require third-

38. *See* In re New York Times Co., 585 F. Supp. 2d 83, 88 (D.D.C. 2008).

39. *Leopold II*, 327 F. Supp. 3d at 17–18.

40. *Id.* at 13–17.

41. *Id.* at 14–15.

42. *Id.*

43. *Id.* at 11, 13.

party compliance, which makes them different from traditional warrants.[44] Next, conceding that an agent's physical presence is not precluded by the SCA, the court claims traditional search warrants always require the physical presence of an agent, while SCA warrants do not.[45] Additionally, pointing to § 2705(b), which says the government may preclude service providers from notifying customers of an SCA warrant's existence, the court says notice is required after a search in a traditional warrant, but not for an SCA warrant.[46]

Lastly, the court notes that while SCA warrants do import a traditional warrant's probable cause standard, SCA warrants do not have the characteristics that justify such a standard for a traditional warrant.[47] Specifically, the court's reasoning is because SCA warrants are subject to pre-exclusion challenges by the provider and because they are not executed in the same fashion as traditional warrants.[48] This circular argument essentially holds that the court does not care that SCA warrants have a probable cause standard because the court believes they should not merit a probable cause standard.

ii. The SCA does not use "warrant" as a term of art.

The court's second contention is that the SCA does not use "warrant" as a term of art.[49] The court says that the legislative history presented by the petitioners proves only that Congress

44. *Id.* at 13.

45. *Leopold II*, 327 F. Supp. 3d at 13.

46. *Id.* at 11.

47. *Id.* at 11–12.

48. *Id.*

49. *Id.* at 9–12.

intended the probable cause requirement to apply to SCA warrants.[50] The D.D.C. has previously held that the amendments made to the SCA through the PATRIOT Act indicate that an SCA warrant is a distinct procedural warrant that imports some, but not all, requirements of Rule 41.[51] In regards to the CLOUD Act, the court holds that Congress just as likely enacted the CLOUD Act to clarify that the SCA warrant is functionally analogous to a subpoena.[52] To support this argument, the court merely claims that Congress feared SCOTUS would reach a contrary opinion and treat SCA warrants like warrants.[53]

III. ANALYSIS

A. Functionally, an SCA Warrant is Analogous to a Traditional Warrant.

The court was incorrect when it held that the SCA does not create a First Amendment right of access because SCA warrants are more functionally akin to a subpoena than a warrant. In fact, an SCA warrant fits well within the bounds of a traditional warrant. Treating SCA warrants as subpoenas, especially for First Amendment purposes, allows the government's unprecedented seizures of American data to remain hidden. The court's arguments supporting the notion that an SCA warrant is functionally dissimilar to a warrant are, at best, mischaracterizations of precedent and, at worst, blatantly circular or baseless.

i. SCA warrants do not allow for pre-execution challenges.

The concept that a provider can quash an SCA warrant is not remotely sufficient to claim that the SCA provides for a pre-execution challenge. A provider's pre-execution challenge is not

50. *Id* at 10, n.4.

51. *See In re Info. Associated with @gmail.com*, 2017 U.S. Dist. LEXIS 130153, at *61, n.24.

52. *See Leopold II*, 327 F. Supp. 3d at 12–13.

53. *Id.* at 13.

a legally sufficient substitute for an individual's pre-execution challenge.[54] Because the government can prevent the provider from disclosing the warrant's existence to the target, the target truly has no opportunity to challenge the warrant.[55] The court provides no substantive argument against this, merely claiming that these limitations do not make an SCA warrant analogous to an actual warrant.[56] The court's own language disputes this argument—in its discussion of this issue, the court refers to providers as the "recipient" of an SCA warrant and the person whose data is being searched as the "target."[57] Such language clearly demonstrates that there is only one party with a true interest in challenging the warrant: the target.

Any legal incentive providers have to challenge defective SCA warrants is insufficient to function similarly to pre-execution challenges to subpoenas. First, the target's ability to file a civil suit may be of little concern to large data storage companies such as Google or Facebook—at the time of this writing, Facebook has been a defendant in about 300 cases since 2016.[58] Second, the SCA provider subject to a cause of action from an individual aggrieved by an SCA violation can simply assert a "good faith reliance" on a court warrant or order as a defense.[59] Thus, suits by an

54. Reply in Support of Petitioners' Motion for Reconsideration at 3, *In re Leopold*, 327 F. Supp. 3d at 1.

55. *Id.*

56. *Leopold II*, 327 F. Supp. 3d at 15.

57. *Id.* at 13–15.

58. LEXIS ADVANCE RESEARCH, https://advance.lexis.com/search/?pdmfid=1000516&crid=5744de51-28c0-4d4a-af83-d89eb38f5768&pdsearchterms=facebook&pdstartin=hlct%3A1%3A1&pdtypeofsearch=searchboxclick&pdsearchtype=SearchBox&pdqttype=and&pdquerytemplateid=&ecomp=5gd6k&prid=f2cc9e55-e66a-4b04-b394-62b83a62a5e3 (last visited Nov. 9, 2018).

59. 18 U.S.C. § 2707(e) (2018).

individual are highly defensible and unlikely to induce providers to behave in a way that protects themselves from such suits.

ii. The method of execution for SCA warrants and traditional warrants is analogous.

The majority of execution methods which the court believes make an SCA warrant materially different from traditional warrants fall well within the scheme of traditional search warrants. Under 18 U.S.C. § 3105, private parties may aid in the execution of a search warrant.[60] Other circuits have held that an SCA search warrant is still a valid search warrant even when law enforcement is not present.[61] In line with such decisions, Congress specifically amended the SCA to clarify that private parties may execute SCA warrants without the presence of law enforcement officers.[62] When a private party executes an SCA warrant, that party is merely an agent of the government.[63] Therefore, the court's concerns regarding lack of officer presence and required third-party compliance in executing an SCA warrant are wholly irrelevant because private parties may independently execute an SCA search warrant—such searches need not be re-defined as "subpoenas" to allow their execution.

Additionally, although the court has yet to bring up this argument in *Leopold*, the D.D.C. has held that materials sought through SCA warrants are executed differently from traditional warrants because the materials they seek are not as private as those sought under traditional

60. 18 U.S.C. § 3105 (2018).

61. United States v. Bach, 310 F.3d 1063, 1066–67 (8th Cir. 2002); Bellville v. Town of Northboro, 375 F.3d 25, 34 (1st Cir. 2004).

62. 18 U.S.C. § 3105; *In re Info. Associated with @gmail.com*, 2017 U.S. Dist. LEXIS 130153, at *59.

63. *Microsoft II*, 829 F.3d at 214.

warrants.[64] The court claims that SCA materials fall under the third-party doctrine, which says individuals have less of a privacy interest in information they have knowingly shared with another, i.e., with a digital communications provider.[65] However, this argument is irrelevant in light of the Supreme Court's recent ruling in *United States v. Carpenter*.[66] In *Carpenter*, the Supreme Court determined that cell-site records were not obtainable through a court order under § 2703(d) of the SCA because of the pervasive use of cell phones and the incredible wealth of data that is automatically transmitted merely when the user turns on a phone.[67] The Court acknowledges prior holdings that pen registers and phone call logs may be sufficiently limited to be deemed "shared" with providers, but holds that Fourth Amendment protections apply to cell phone location information.[68]

The D.D.C.'s arguments in *@gmail* and *Leopold* are remarkably similar to Justice Kennedy's dissent in *Carpenter*, which argues compulsory disclosures of cell phone location information are governed by subpoena, not warrant, protections.[69] The *Carpenter* majority counters this argument quite strongly, noting that cell service location information is starkly different from information obtainable under subpoenas, such as bank records or payroll

64. *In re Info. Associated with @gmail.com*, 2017 U.S. Dist. LEXIS 130153, at *45–46.

65. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018); *In re Info. Associated with @gmail.com*, 2017 U.S. Dist. LEXIS 130153, at *45–46.

66. *See Carpenter*, 138 S. Ct. at 2206.

67. *Id.*

68. *Carpenter*, 138 S. Ct. at 2219 (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); Riley v. California, 573 U.S. 373, 400 (2014)).

69. *See generally Carpenter*, 138 S. Ct. at 2223–36 (Kennedy, J. dissenting)*; In re Info. Associated with @gmail.com*, 2017 U.S. Dist. LEXIS 130153; *Leopold II*, 327 F. Supp. 3d at 1.

information.[70] Put simply, "if the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement."[71] Katie Townsend, counsel for the Reporters Committee in *Leopold*, agrees, saying "I get that a subpoena for business records goes to a company, or a subpoena for phone records goes to the phone company. We're not talking about metadata, though – we're talking about opening someone's mail, it's fundamentally different."[72]

Lastly, that the government may apply for a notice preclusion order under 18 U.S.C. § 2705(b) does not render SCA warrants wholly different from traditional warrants.[73] The exception to notice under § 2705(b) actually implies that it should be presumed that notice is required under the SCA unless the government has a good reason to except the search from traditional notice requirements.[74] The notice exception under § 2705(b) indicates that Congress knew they needed to carve out the notice requirement from traditional warrant requirements, not that Congress intended to remove warrant protections from SCA warrants altogether.[75]

iii. Probable cause

The court's probable cause argument is also easily dismissed by understanding that private parties may independently execute an SCA search warrant. Put succinctly, the court says that the

70. *Carpenter*, 138 S. Ct. at 2222 (majority opinion).

71. *Id.*

72. Interview with Katie Townsend, Legal Director, Reporters Committee for Freedom of the Press (Oct. 5, 2018).

73. 18 U.S.C. § 2705 (2018).

74. *Id.*

75. *Id.*

identifying characteristic of a warrant, the requirement of probable cause, is irrelevant to the determination of whether an SCA warrant is a warrant because SCA warrants do not merit the probable cause standard.[76] This argument is incredibly circular because the arguments the court provides to substantiate this argument are the same arguments it makes to distinguish the execution of an SCA warrant from a traditional warrant.[77] Therefore, if private parties may execute SCA warrants without re-defining them as subpoenas, then whether or not the court thinks SCA warrants ought to have the probable cause standard is wholly irrelevant.

B. The SCA Uses "Warrant" as a Term of Art.

Even if an SCA warrant is executed differently from the court's traditional notions of warrants, the legislature's use of the word "warrant" in the SCA surely indicates that SCA warrants ought to trigger the same protections under the First Amendment. First, it is highly unlikely that Congress would use the specific term "warrant" to create an entirely new set of legal standards beyond those typically applying to that term.[78] Prior to the PATRIOT Act, when the language of the SCA read "a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant," the plain language of the statute quite clearly indicated that SCA warrants should be treated as warrants.[79] The Eighth Circuit agreed, noting in *United States v. Bach* that "while

76. *Leopold II*, 327 F. Supp. 3d at 11.

77. *Id.*

78. *See Microsoft II*, 829 F.3d at 211.

79. S. REP. NO. 99-541, at 38 (1986); *see Matter of 381 Search Warrants Directed to Facebook, Inc.*, 78 N.E.3d at 147..

warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants and we find that Congress intended them to be treated as warrants."[80]

The amendments made thereafter do not change whether an SCA warrant is a warrant or not. In fact, it is most likely that Congress carved out specific exceptions to the traditional application of warrants specifically because an SCA warrant is a warrant. Whether an SCA warrant is a true warrant or not became an issue following the PATRIOT Act amendment to the SCA.[81] It was only because of the PATRIOT Act's seemingly minor change of § 2307(b)(1)(A)'s language to "using the procedures" that courts could argue that the SCA created its own form of warrant.[82] Congress clearly stipulated that the SCA amendments within the PATRIOT Act were intended to address "investigative delays caused by the cross-jurisdictional nature of the Internet" by creating an exception to the presumption that warrants do not apply extraterritorially.[83] Instead, courts manipulated the amended language to start an intense, misleading debate where courts are using the warrant/subpoena debate to justify applying SCA warrants abroad.[84]

This is particularly concerning for purposes of public disclosure. Because the amendment was made under the PATRIOT Act, citizens may believe that more relaxed warrants standards are being applied only to terrorists. For Leopold and Townsend, this concern is the crux of why these materials ought to be disclosed. "The example that we always point [to is] the James Rosen case,"

---

80. United States v. Bach, 310 F.3d 1063, 1066–67 (8th Cir. 2002).

81. PATRIOT Act, Pub. L. No. 107-56, sec. 212, 115 Stat. 272, 284–85 (2001).

82. *Id.*

83. H.R. REP NO. 107-236, at 57 (2001).

84. *Microsoft II*, 829 F.3d at 214–15; *In re Info. Associated with @gmail.com*, 2017 U.S. Dist. LEXIS 130153, at *49–53; *In re Search Warrant*, 232 F. Supp. 3d at 720–22; *Matter of 381 Search Warrants Directed to Facebook*, 78 N.E.3d at 146–47.

Townsend says.[85] "He didn't know that there was a search warrant that obtained the contents of his email until it appeared in the Washington Post. . . . These are tools that have become really ubiquitous."[86]

If nothing else, the CLOUD Act ought to put a final pin in the warrant/subpoena debate.[87] The CLOUD Act created an exception to the presumption against extraterritorial application of SCA warrants as a direct response to Microsoft.[88] This amendment renders previous arguments that SCA warrants are more similar to subpoenas because of their extraterritorial application completely moot.[89] If SCA warrants were more akin to subpoenas, such an exception would be unnecessary as "a company availing itself of the opportunity of doing business in the United States is subject to U.S. criminal laws and can be compelled to bring assets and evidence from abroad into the United States" through a subpoena.[90] Therefore, the court's argument that it could have just as easily meant that Congress intended to re-enforce that SCA warrants are more like a subpoena is baseless.

IV. CONCLUSION

The D.D.C.'s analysis in *In re Leopold* is a misguided continuation of the warrant vs. subpoena debate, which was created only to allow the extraterritorial application of the Stored

---

85. Interview with Katie Townsend, *supra* note 72.

86. *Id.*

87. Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Div. V.

88. *Id.*; *Microsoft III*, 138 S. Ct. 1186.

89. *See, e.g.*, *Microsoft II*, 829 F.3d at 214–15; *In re Info. Associated with @gmail.com*, 2017 U.S. Dist. LEXIS 130153, at *49–53; *In re Search Warrant*, 232 F. Supp. 3d at 720–22; *Matter of 381 Search Warrants Directed to Facebook*, 78 N.E.3d at 146–147.

90. *See In re Info. Associated with @gmail.com*, 2017 U.S. Dist. LEXIS 130153, at *38.

Communications Act. Because this case is a First Amendment case, the court's application of the Fourth Amendment subpoena escape mechanism is completely inappropriate. Additionally, the argument that SCA warrants are more akin to subpoenas is practically incorrect. Finally, because subsequent amendments to the Stored Communications Act clearly demonstrate the SCA's extraterritorial application, it is likely that the entire warrant vs. subpoena debate is entirely moot. Juxtaposing "SCA warrants" and "traditional warrants" is in itself misleading—SCA warrants are not an entirely different form of a court order from Rule 41 warrants, they are merely warrants with certain procedural requirements waived. Therefore, the *Leopold* court incorrectly denied relief to Jason Leopold and the Reporter's Committee for the Free Press. Without the disclosure that Leopold seeks, Americans will remain in the dark as the US government hides behind bright screens, seizing our emails.