	Case 2:17-mc-00145-RSL Docun	nent 1 Filed 11/15/17 Page 1 of 41
1		
2		
4		
5		
6		
7		TES DISTRICT COURT
8		STRICT OF WASHINGTON EATTLE
9		
10	IN RE PETITION OF INDEX NEWSPAPERS LLC D/B/A THE	MISC. CIVIL ACTION NO. <u>2:17-mc-00145 RS</u> L
11	STRANGER TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS,	PETITION TO UNSEAL ELECTRONIC SURVEILLANCE
12 13	APPLICATIONS, AND ORDERS	DOCKETS, APPLICATIONS, AND ORDERS
13		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24 25		
20		
	PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS	Dorsey & Whitney LLP Columbia Center 701 Fifth Avenue, Sutte 6100 Seattle, WA 98104-7043 Phone: (206) 903-8800 Fax: (206) 903-8820

		Cas	e 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 2 of 41
1			TABLE OF CONTENTS
2	I. INTRODUCTION		
3	I. II.		DICTION AND VENUE
4			GROUND
5	III.		
6		A.	The Stranger
7		B.	Legal Bases for Electronic Surveillance
8			1. The Pen Register Act
9			2. The Stored Communications Act
10	3. The Wiretap Act7		
11 12	4. The All Writs Act		
12	C. Docketing Practices for Electronic Surveillance Cases in This District		
13	D. Petitions Seeking To Unseal Surveillance Cases in Other Districts		
15	IV. LEGAL STANDARDS		
16	A. The First Amendment Right of Access to Judicial Records and Proceedings		
17		B.	The Common Law Right of Access to Judicial Records
18	V.	ARGU	JMENT
19		A.	Petitioner Has a Right to Access Basic Docketing Information Regarding
20			Electronic Surveillance Cases in This District15
21		В.	Petitioner Has a Right to Access Electronic Surveillance Applications and Orders Filed in This District, Once Secrecy is No Longer Necessary
22			
23			1. Petitioner Has a Right to Access the Requested Pen Register Act Materials
24			2. Petitioner Has a Right to Access the Requested Stored
25			Communications Act Materials22
	SURV		UNSEAL ELECTRONIC CE DOCKETS, APPLICATIONS, - i DORSEY & WHITNEY LLP COLUMBIA CENTER 701 FIFTH AVENUE, SUITE 6100 SEATTLE, WA 98104-7043 PHONE: (206) 903-8800 FAX: (206) 903-8820

	Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 3 of 41
1 2 3	<ul> <li>3. Petitioner Has a Right to Access the Requested Wiretap Act Materials</li></ul>
4 5	C. Redaction Is an Appropriate Mechanism to Address Privacy Interests and Other Concerns with Petitioner's Request to Unseal Judicial Records27
6	VI. SPECIFIC RELIEF REQUESTED
7	VII. CONCLUSION
8	
9	
10 11	
12	
13	
14	
15	
16	
17	
18	
19 20	
21	
22	
23	
24	
25	
	PETITION TO UNSEAL ELECTRONIC       Columbia Center         SURVEILLANCE DOCKETS, APPLICATIONS,       Seartle, WA 98104-7043         AND ORDERS - ii       PHONE: (206) 903-8820□

	Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 4 of 41
1	TABLE OF AUTHORITIES
2	Page(s) CASES
3	
4	Application of Newsday, Inc., 895 F.2d 74 (2d Cir.1990)
5	
6	Associated Press v. U.S. Dist. Court, 705 F.2d 1143 (9th Cir. 1983)
7	
8	Baltimore Sun Co. v. Goetz, 886 F.2d 60 (4th Cir. 1989)
9	CBS, Inc. v. U.S. Dist. Ct.,
	765 F.2d 823 (9th Cir. 1985)
10	Co. Doe v. Public Citizen,
11	749 F.3d 246 (4th Cir. 2014)
12	Ctr. for Auto Safety v. Chrysler Group, LLC,
13	809 F.3d 1092 (9th Cir. 2016)
14	Dhiab v. Trump,
15	852 F.3d 1087 (D.C. Cir. 2017)
16	EEOC v. Nat'l Children's Ctr., Inc.,
17	98 F.3d 1406 (D.C. Cir. 1996) 15
18	<i>Fed. Trade Comm'n v. Standard Fin. Mgmt. Corp.</i> , 830 F.2d 404 (1st Cir. 1987)
19	Foltz v. State Farm Mut. Auto. Ins. Co.,
20	331 F.3d 1122 (9th Cir. 2003)
21	Glaxo Grp. Ltd. v. Leavitt,
22	481 F. Supp. 2d 437 (D. Md. 2007)
23	Globe Newspaper Co. v. Superior Court,
24	456 U.S. 596 (1982)
25	Hagestad v. Tragesser, 49 F.3d 1430 (9th Cir. 1995)15
	PETITION TO UNSEAL ELECTRONIC COLUMBIA CENTER 701 EIETH AVENUE SUITE 6100
	Year in the constant for onstant field in the constant for onstant field in the constant field in the

	Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 5 of 41
1 2 3 4	Hartford Courant Co. v. Pellegrino, 380 F.3d 83 (2d Cir. 2004)
5 6 7 8	In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 5KGD203, No. 15-mj-0451, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016)
9 10	In re Application and Affidavit for a Search Warrant, 923 F.2d 324 (4th Cir. 1991)
<ol> <li>11</li> <li>12</li> <li>13</li> </ol>	Records, 585 F. Supp. 2d 83 (D.D.C. 2008)
14 15	In re Copley Press, Inc., 518 F.3d 1022 (9th Cir. 2008)
16 17 18	<i>In re Motion for Release of Court Records</i> , 526 F. Supp. 2d 484 (FISA Ct. 2007)
19 20	<i>In re N.Y. Times Co.</i> , 828 F.2d 110 (2d Cir. 1987)
21 22	In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued By this Court, 149 F. Supp. 3d 341 (E.D.N.Y. 2016)
<ul><li>23</li><li>24</li><li>25</li></ul>	<i>In re Order Requiring XXX, Inc.</i> , No. 14-mj-2258, 2014 U.S. Dist. LEXIS 154743 (S.D.N.Y. Oct. 31, 2014)
	PETITION TO UNSEAL ELECTRONIC       Columbia Center         SURVEILLANCE DOCKETS, APPLICATIONS,       SEATTLE, WA 98104-7043         AND ORDERS - iv       Fax: (206) 903-8820

	Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 6 of 41
1	In re Petition of Jennifer Granick and Riana Pfefferkorn to Unseal
2	<i>Technical-Assistance Orders and Materials</i> , No. 16-mc-80206-KAW (N.D. Cal.)
3	<i>In re Sealed Case</i> ,
4	199 F.3d 522 (D.C. Cir. 2000)16
5	<i>In re Sealing &amp; Non-Disclosure</i> ,
6	562 F. Supp. 2d 876 (S.D. Tex. 2008) 17, 20, 21, 28
7	In re Search Warrant for Secretarial Area Outside Office of Gunn,
8	855 F.2d 569 (8th Cir.1988)
9	<i>In re Special Proceedings</i> ,
10	842 F. Supp. 2d 232 (D.D.C. 2012)
11	<i>In re State-Record Co., Inc.,</i> 917 F.2d 124 (4th Cir. 1990)
12	In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns,
13	349 F.3d 1132 (9th Cir. 2003)
14	In re Wash. Post,
15	807 F.2d 383 (4th Cir. 1986)
16	<i>Kamakana v. City &amp; Cnty. of Honolulu,</i>
17	447 F.3d 1172 (9th Cir. 2006)14
18	Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)
19	Media Gen. Operations, Inc. v. Buchanan,
20	417 F.3d 424 (4th Cir. 2005)16
21	Nebraska Press Ass'n v. Stuart,
22	427 U.S. 539 (1976)
23	Nixon v. Warner Commc'ns, Inc.,
24	435 U.S. 589 (1978)2, 12
25	<i>Oregonian Publ'g Co. v. U.S. Dist. Court</i> , 920 F.2d 1462 (9th Cir. 1990)
	DORSEY & WHITNEY LLP         PETITION TO UNSEAL ELECTRONIC       Columbia Center         SURVEILLANCE DOCKETS, APPLICATIONS,       Seattle, Wa 98104-7043         AND ORDERS - v       Fax: (206) 903-8820

	Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 7 of 41
1 2 3 4 5	Pepsico, Inc. v. Redmond,         46 F.3d 29 (7th Cir. 1995)
6	Richmond Newspapers, Inc. v. Virginia,
7	448 U.S. 555 (1980)
8	<i>Times Mirror Co. v. United States</i> ,
9	873 F.2d 1210 (9th Cir. 1989)13, 14, 19
10	United States v. Appelbaum, 707 F.3d 283 (4th Cir. 2013)
11	United States v. Bus. of Custer Battlefield Museum and Store,
12	658 F.3d 1188 (9th Cir. 2011) passim
13 14	United States v. Chow, No. 14-cr-00196, 2015 U.S. Dist. LEXIS 114802 (N.D. Cal. Aug. 28, 2015)
15	United States v. Denedo,
16	556 U.S. 904 (2009)
17	United States v. El-Sayegh,
18	131 F.3d 158 (D.C. Cir. 1997)14
18	United States v. Espudo, 954 F. Supp. 2d 1029 (S.D. Cal. 2013)
20	United States v. Index Newspapers LLC,
21	766 F.3d 1072 (9th Cir. 2014)
22	United States v. Loughner,
23	769 F. Supp. 2d 1188 (D. Ariz. 2011) passim
24	United States v. Mendoza,
25	698 F.3d 1303 (10th Cir. 2012)17
	PETITION TO UNSEAL ELECTRONIC       COLUMBIA CENTER         SURVEILLANCE DOCKETS, APPLICATIONS,       SEATTLE, WA 98104-7043         AND ORDERS - vi       PHONE: (206) 903-8820□

	Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 8 of 41
1 2	United States v. New York Telephone Company, 434 U.S. 159 (1977)26
3	United States v. Ochoa-Vasquez, 428 F.3d 1015 (11th Cir. 2005)16, 17
4 5	United States v. Ressam, 221 F. Supp. 2d 1252 (W.D. Wash. 2002)25
6 7	United States v. Ring, 47 F. Supp. 3d 38 (D.D.C. 2014)
8 9	United States v. Tillman, No. 07-cr-1209, 2009 U.S. Dist. LEXIS 35400 (S.D.N.Y. Apr. 6, 2009)
10	United States v. Valenti, 987 F.2d 708 (11th Cir. 1993)16
11 12	Wash. Legal Found. v. United States Sentencing Comm'n, 89 F.3d 897 (D.C. Cir. 1996)15
13	STATUTES
14	18 U.S.C. §§ 2510-2522
15	18 U.S.C. § 2511(2)(a)(ii)
16 17	18 U.S.C. § 2518(8)(b)
18	18 U.S.C. §§ 2701-2712 passim
19	18 U.S.C. § 2703 passim
20	18 U.S.C. § 2705(b)
21	18 U.S.C. §§ 3121-3127 passim
22	18 U.S.C. § 3123
23	18 U.S.C. § 3124
24	18 U.S.C. § 3127
25	28 U.S.C. § 1331
	Dorsey & Whitney LLP

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - vii

## Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 9 of 41

1	1 28 U.S.C. § 1391(b)(2)		
2	28 U.S.C. § 1651 passim		
3	Judiciary Act of 1789, 1 Stat. 73, § 14 (Sept. 24, 1789)25		
4	Other Authorities		
5	U.S. Const. amend. I passim		
6 7	Fed. R. Crim. P. 41 5, 6, 30		
8	LCR 3(e)		
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21 22			
22			
24			
25			
	DORSEY & WHITNEY LLPPETITION TO UNSEAL ELECTRONICCOLUMBIA CENTERSURVEILLANCE DOCKETS, APPLICATIONS,701 FIFTH AVENUE, SUITE 6100SURVEILLANCE DOCKETS, APPLICATIONS,SEATTLE, WA 98104-7043PHONE: (206) 903-8800FAX: (206) 903-8820 []		

1

#### I. INTRODUCTION

Index Newspapers LLC d/b/a The Stranger, a Seattle-based newspaper, respectfully petitions the Court for an Order (1) unsealing certain judicial records in electronic surveillance cases filed in the Western District of Washington and (2) changing the Court's docketing practices to allow public access to these types of records in future cases, consistent with the public's constitutional and common law rights of access to judicial proceedings and records.

7 The judicial records sought by Petitioner authorize various forms of electronic surveillance
8 of individuals and compel service providers to assist with government surveillance and to disclose
9 user data and customer records.

Petitioner cannot access these judicial records without the Court's assistance because they are maintained under seal and not publicly docketed in the Court's Case Management/Electronic Case Files (CM/ECF) system. In many instances, these judicial records are completely and indefinitely hidden from public view, preventing the public from knowing how the Court is interpreting and applying the law in electronic surveillance cases.

Petitioner seeks access to these judicial records to better understand and inform the public about how the government is using current laws to gain access to individuals' private information, including how often law enforcement officers seek and obtain orders from this Court allowing access to such information.

Going forward, publicly docketing electronic surveillance cases and unsealing the
applications, orders, and other judicial records in those cases, after there is no longer any need for
secrecy, will similarly further the public's understanding of the law and the judicial process in
electronic surveillance cases, and serve the deep-seated American principle of open access to the
courts.

The legal and factual bases for Petitioner's request are explained in detail below. Additionally, this Petition is supported by the declarations of Steven J. Hsieh and Aaron D.

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 1

Mackey, filed herewith. Petitioner respectfully requests that the Court issue an order providing the
 specific relief identified in Section VI of this Petition and in the accompanying proposed order.

3

#### II. JURISDICTION AND VENUE

The Court has jurisdiction over this Petition because "[e]very court has supervisory power
over its own records and files." *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978); *accord In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 487 (FISA Ct. 2007) (footnote
omitted) (courts have "jurisdiction in the first instance to adjudicate a claim of right to [their] very
own records and files. . . . [T]his Court's inherent power over its records supplies the authority to
consider a claim of legal right to release of those records"). Jurisdiction is also proper under 28
U.S.C. § 1331.

Venue within this District is proper under 28 U.S.C. § 1391(b)(2) because the actions or omissions giving rise to the action occurred within this District, namely, the sealing of the specified judicial records of this Court to which Petitioner requests access.

Petitioner seeks District-wide relief, namely public docketing and unsealing of the sealed
judicial records specified herein, wherever they may be within this District. Therefore, under LCR
3(e), assignment to any division is proper. Petitioner maintains its principal place of business in
Seattle and therefore requests assignment to the Seattle Division.

18

19

# III. BACKGROUND

A. The Stranger

Petitioner Index Newspapers LLC d/b/a The Stranger is a Seattle-based Pulitzer Prize
winning newspaper that has been a voice in the community since 1991. Declaration of Steven J.
Hsieh ("Hsieh Decl.") ¶¶ 1-3. The Stranger prides itself in covering important stories overlooked
by other publications in Seattle, and is known for its investigations that shake up the status quo
and lead to significant policy changes. *Id.* ¶ 3. One of The Stranger's major reporting objectives is
to publish stories that contribute to the principles of transparency and open government. *Id.* ¶ 4.

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 2

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 12 of 41

Law enforcement surveillance practices are of significant interest to The Stranger's 1 journalists in their mission to inform citizens and ensure government transparency and 2 accountability. Id. ¶ 5. As part of The Stranger's efforts to increase public knowledge and 3 awareness regarding the activities of local, state, and federal government, The Stranger has 4 published numerous articles reporting on law enforcement electronic surveillance activities. Id. ¶¶ 5 5-10. For example, in 2013, The Stranger was the first local media organization to thoroughly 6 report on the surveillance devices installed by the Seattle Police Department that were capable of 7 tracking people's digital devices around the city. Id.  $\P$  6. The Stranger was also the first to report 8 that the Seattle Police Department purchased software that allowed officers to monitor social g media users without informing city officials—a violation of local laws. Id. ¶ 7. 10

The Stranger seeks public docketing and unsealing of certain electronic surveillance 11 applications and orders filed in this District as part of its continuing efforts to report on and better 12 inform the public regarding law enforcement surveillance activities. The Stranger aims to bring 13 greater transparency to law enforcement's electronic surveillance activities in this District. For 14 example, The Stranger wants to report the number of electronic surveillance orders sought and 15 obtained by law enforcement in this Court; which law enforcement agencies are seeking electronic 16 surveillance orders; the legal authorities cited to support such orders; the types of electronic 17 surveillance permitted; and the identities of companies compelled to provide technical assistance 18 for government surveillance and to disclose user data and customer records. Id. ¶¶ 11-13. 19

If the public cannot locate surveillance case dockets and records, it risks having an incomplete and inaccurate understanding of the government's electronic surveillance practices in this District. The public docketing and unsealing of electronic surveillance cases as requested in this Petition would enable The Stranger and other members of the public to search in CM/ECF for these records, and to obtain a more complete understanding of surveillance practices in this District, enabling the propriety of those practices to be discussed and debated. *Id.* ¶ 14. "Secrecy

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 3

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 13 of 41

of judicial action can only breed ignorance and distrust of courts and suspicion concerning the
 competence and impartiality of judges; free and robust reporting, criticism, and debate can
 contribute to public understanding of the rule of law." *Nebraska Press Ass'n v. Stuart*, 427 U.S.
 539, 587 (1976) (Brennan, J., concurring).

Beginning in August 2017, The Stranger, through its counsel, met and conferred
telephonically and by email with the United States Attorney's Office for the Western District of
Washington ("USAO"). In early September 2017, The Stranger's counsel provided a draft of The
Stranger's requested relief (proposed order) to the USAO. Counsel and the USAO discussed The
Stranger's requested relief during teleconferences on September 15 and October 13, 2017. No
agreement was reached before the filing of this Petition. Declaration of Aaron D. Mackey
("Mackey Decl.") ¶ 16.

12

#### B. Legal Bases for Electronic Surveillance

Law enforcement can invoke a number of statutory authorities when seeking authorization to conduct electronic surveillance or otherwise obtain personal information about individuals in this District. These authorities include for example the Pen Register Act, 18 U.S.C. §§ 3121-3127, the Stored Communications Act, 18 U.S.C. §§ 2701-2712, the Wiretap Act, 18 U.S.C. §§ 2510-2522, and the All Writs Act, 28 U.S.C. § 1651. These statutes allow law enforcement to obtain a wide range of personal data, including the content of communications, geographic locations, lists of websites visited, email addresses, phone numbers, and customer account records.

20 Petitioner seeks public docketing and unsealing of electronic surveillance applications and
21 orders relating to each of these statutory authorities, which are described in further detail below.

22

#### 1. The Pen Register Act

Title III of the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§ 3121-3127, is known as the Pen Register Act ("PRA"). The PRA establishes rules governing telephone companies' and Internet service providers' compelled collection and disclosure of users'

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 4

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 14 of 41

1 dialing, routing, signaling, and addressing information to law enforcement.

Pen register and/or trap and trace ("PR/TT") devices record routing information, such as telephone numbers, and e-mail addresses transmitted by wire or electronic communications carriers. 18 U.S.C. § 3127. A court "shall enter" an order authorizing the installation and use of a PR/TT device if it "finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation," 18 U.S.C. § 3123(a)(1), a showing lower than the "probable cause" standard required to obtain a search warrant under Federal Rule of Criminal Procedure 41.

A court order authorizing the installation and use of a PR/TT device must direct that the
order be sealed until further order of the court. 18 U.S.C. § 3123(d). Though the PRA contemplates
unsealing of PR/TT applications and orders when "ordered by the court," *id.*, unsealing is in
practice uncommon. As a result, judicial records regarding PR/TT devices, including basic docket
information, are typically shielded from public scrutiny indefinitely.

Law enforcement uses PR/TT devices to collect information about the communications of 14 thousands of individuals each year. A U.S. Department of Justice report on the use of PR/TT 15 devices by four federal law enforcement agencies showed that in 2011, 43,576 people were 16 affected by those agencies' use of pen registers and 46,565 people were affected by their use of 17 trap and trace devices on telephone facilities; 837 pen registers and 824 trap and trace devices were 18 authorized for use on e-mail and/or Internet networks. See Mackey Decl., Ex. A. These numbers 19 reflect only PR/TT devices judicially authorized for use by the four agencies included in the report. 20From 2008 through 2016, in a single district, the District of Columbia, the USAO alone filed 2,248 21 applications for judicial authorization to use a PR/TT device—approximately 250 applications per 22 year. See Mackey Decl., Exs. B-D. 23

24

25

#### 2. The Stored Communications Act

Title II of ECPA, 18 U.S.C. §§ 3121-3127, is known as the Stored Communications Act

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 5

("SCA"). The SCA provides government entities with mechanisms to compel third-party
 electronic communication service or remote computing service providers to disclose the contents
 of stored wire and electronic communications, as well as records and other information pertaining
 to subscribers. The mechanisms available under the SCA include Section 2703(d) orders, *see* 18
 U.S.C. § 2703(d), and search warrants, *see* 18 U.S.C. § 2703(a), (b)(1)(A), and (c)(1)(A).

Like PR/TT orders, Section 2703(d) orders may be issued on a showing lower than that
required to obtain a warrant under Fed. R. Crim. P. 41: The government seeking a Section 2703(d)
order must "offer[] specific and articulable facts showing that there are reasonable grounds to
believe that the contents of a wire or electronic communication, or the records or other information
sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Search warrants issued under the SCA must be "issued using the procedures described in
the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant
procedures)." 18 U.S.C. § 2703(a), (b)(1)(A), and (c)(1)(A).

Although the SCA does not require sealing of warrants or orders issued under its 14 provisions, such records are frequently sealed and kept under seal indefinitely. As a result, the 15 public lacks information as to the number of SCA search warrants and Section 2703(d) orders 16 issued by district courts in any given time period. However, there is reason to believe those 17 numbers are high. Google, Inc. reported that during the first six months of 2017, it received 5,201 18 search warrant requests, 9,320 subpoena requests, and 1,533 "other court order" requests from the 19 U.S. government. See Mackey Decl., Ex. E. Microsoft Corporation reported that during the first 20six months of 2017, it received 5,401 U.S. law enforcement requests for customer data from 12,936 21 accounts/users. See Mackey Decl., Ex. F. 22

Information released by the U.S. District Court for the District of Columbia indicates that the number of applications for Section 2703(d) orders filed in that District averaged around 100 per year from 2008 to 2013, and then increased rapidly, with 1,136 such applications filed in 2016.

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 6

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 16 of 41

See Mackey Decl., Ex. G. Writing about the ECPA dockets of federal district courts, Magistrate
 Judge Stephen W. Smith noted that "the number of ECPA cases filed in a single year surpasses the
 entire output of the FISA court since its creation in 1978," and, in one sample year (2006), "federal
 magistrate judges were presented with over 30,000 secret ECPA applications." Mackey Decl., Ex.
 H at 315 & 322.

In October 2017, the Department of Justice (DOJ) issued a new policy regarding protective
orders under § 2705(b) of the SCA. *See* Mackey Decl., Ex. I. The new DOJ policy ends the routine
imposition of nondisclosure orders of indefinite duration barring service providers like Google and
Microsoft from notifying their customers that their email or other records have been turned over
in response to legal demands by the government under the SCA. The new DOJ policy provides
that "[b]arring exceptional circumstances, prosecutors filing § 2705(b) applications may only seek
to delay notice for one year or less." *Id.* at 2.

Nothing in the new DOJ policy, however, requires prosecutors to request that courts
publicly docket and unseal the applications, orders, and other documents filed in SCA cases, even
after one year has passed. Thus, these judicial records remain indefinitely sealed and inaccessible
to Petitioner and the public at large in this District.

17

#### 3. The Wiretap Act

Title I of ECPA, 18 U.S.C. §§ 2510-2522, amended the Wiretap Act to permit interception
of electronic communications. The Wiretap Act enables law enforcement to obtain, among other
things, an order requiring third parties to provide technical assistance to law enforcement to
intercept wire, oral, or electronic communications or to conduct electronic surveillance. 18 U.S.C.
§ 2511(2)(a)(ii). No time limit for sealing is stated in the Wiretap Act.

Judicial interpretation of the technical-assistance provisions of the Wiretap Act may be
enabling surveillance of oral communications via smart TVs and other home consumer products.
In a 2003 decision, the Ninth Circuit reviewed a district court decision to issue several *ex parte*

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 7

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 17 of 41

orders under the Wiretap Act, requiring an unnamed company to assist in intercepting 1 conversations occurring in a vehicle equipped with an on-board system that listened to occupants' 2 voice commands and gave directions and other assistance according to request. The district court 3 granted a government technical-assistance application to force the unnamed company to 4 surreptitiously turn on the microphone in the automobile's communication system. Though the 5 Federal Bureau of Investigation had a court-issued warrant to conduct a wiretap, the Ninth Circuit 6 ultimately reversed the district court for a fact-specific reason. The Court held that the technical 7 assistance demanded was not authorized by the Wiretap Act because it would disable the service 8 entirely. In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns, 349 F.3d 9 1132, 1144-46 (9th Cir. 2003). 10

Today, the public does not know whether law enforcement has sought to use the Wiretap
Act's technical-assistance provisions to turn home appliances into eavesdropping equipment, for
example, by requiring manufacturers to turn on the microphones in televisions and smart speakers. *See* Mackey Decl., Ex. J at 13-15.

15

#### 4. The All Writs Act

The All Writs Act ("AWA") authorizes federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a).

In recent years, the government has sought orders under the AWA compelling smartphone
companies to circumvent the encryption on their devices. For example, in October 2014, a
magistrate judge in the Southern District of New York issued an order under the AWA compelling
an unnamed cellphone manufacturer to bypass the lock screen on—and extract intelligible data
from—an encrypted phone for which law enforcement had a search warrant. *In re Order Requiring XXX, Inc.*, No. 14-mj-2258, 2014 U.S. Dist. LEXIS 154743 (S.D.N.Y. Oct. 31, 2014).

25

In 2015, another magistrate judge in the Eastern District of New York unsealed a similar

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 8

AWA application (which he ultimately denied), this time directed at iPhone manufacturer Apple. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued By this Court*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (denying AWA application). During that case, the
public learned that courts have granted at least 70 other government applications for AWA orders
compelling manufacturers to bypass smartphone passcodes in sealed proceedings. *See* Mackey
Decl., Ex. K.

In 2016, a magistrate judge in the Central District of California issued an AWA order 7 compelling Apple to write new software code to allow law enforcement to "brute force" guess the 8 password protecting an encrypted iPhone used by one of the San Bernardino terrorists. In the 9 Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a 10Black Lexus IS300, California License Plate 5KGD203, No. 15-mj-0451, 2016 U.S. Dist. LEXIS 11 20543 (C.D. Cal. Feb. 16, 2016). Although the FBI dropped the matter after accessing the phone's 12 data by other means, that case sparked discussion of whether compelling such access is within the 13 courts' authority. See Mackey Decl., Ex. L. 14

15

#### C. Docketing Practices for Electronic Surveillance Cases in This District

Beginning in July 2017, Petitioner communicated with the Chief Deputy Clerk for the Western District of Washington to learn more about how applications for electronic surveillance orders and search warrants are handled in this District, including the extent to which court records relating to such requests are publicly accessible. Hsieh Decl. ¶ 15. Based on those communications, Petitioner developed the following understanding regarding docketing practices for electronic surveillance cases in this District.

When a new case is filed in this District, the case is docketed in the Court's CM/ECF system and assigned a case number and a case type designation, such as Criminal (CR), Civil (CV), Magistrate Judge (MJ), Grand Jury (GJ), or Miscellaneous (MC). *Id.* ¶¶ 16-17. Applications seeking a search warrant or a non-warrant order for electronic surveillance are filed manually (*i.e.*,

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 9

in paper) and later scanned by the Court into its CM/ECF system. Id. ¶ 18. This procedure applies 1 to all of the types of electronic surveillance cases addressed in this Petition. Id. 2

3

This Court uses the Magistrate Judge (MJ) case type designation for cases seeking a search warrant for electronic surveillance and the Grand Jury (GJ) case type designation for cases seeking 4 a non-warrant order for electronic surveillance. Id. ¶¶ 19-20. The Court uses the Grand Jury (GJ) 5 case type designation for non-warrant surveillance cases—even though they are not connected 6 with any grand jury proceedings—as a way to prevent those cases from becoming inadvertently 7 unsealed, since cases having the Grand Jury (GJ) case type designation cannot be unsealed in the 8 Court's CM/ECF system. Id. ¶ 20. 9

In cases seeking a search warrant or a non-warrant order for electronic surveillance, all 10 documents are filed under seal, and the docket sheet and all documents remain under seal unless 11 the Court orders otherwise. When such a case is sealed, even the existence of the case (e.g., the 12 case number) is not publicly disclosed and not publicly discoverable, either electronically through 13 the Court's Public Access to Court Electronic Records (PACER) service or in person by visiting 14 the Clerk's office at the Court. Id. ¶ 21. 15

Under this Court's current docketing practices, which Petitioner understands have been in 16 effect since at least 2010, the public has no way to access even basic docket sheet information 17 regarding non-warrant electronic surveillance cases, much less the applications, orders, and other 18 documents filed in these cases assigned the Grand Jury (GJ) case type designation. These cases 19 remain sealed indefinitely. The very existence of individual non-warrant electronic surveillance 20cases in this District is kept secret from the public and, at present, there is no way Petitioner can 21 make a particularized request to unseal information in specific cases. Id. ¶ 22. 22

23 Unlike the non-warrant cases described above, cases involving search warrants for electronic surveillance are sometimes unsealed, for example, after an executed search warrant has 24 been returned to the Court. Petitioner understands that the Court sends periodic reports to the 25

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 10

USAO identifying cases in which an executed search warrant has not been returned, and that the 1 USAO responds to those reports by filing a motion requesting that the warrant-related materials 2 either remain sealed or be unsealed. Id. ¶ 23. Petitioner does not know what portion of cases in this 3 District involving a search warrant for electronic surveillance have been unsealed. Nor does 4 Petitioner know how long on average it takes for such cases to be unsealed in this District, although 5 on information and belief it can take years for search warrant materials to be unsealed. After a 6 search warrant case has been unsealed, the public can access the case docket sheet and the unsealed 7 materials electronically through PACER. Id. 8

9

#### D. Petitions Seeking To Unseal Surveillance Cases in Other Districts

In the District of Columbia, journalist Jason Leopold and the Reporters Committee for
Freedom of the Press petitioned the court seeking increased public access to judicial records in
cases involving electronic surveillance under the Pen Register Act and the Stored Communications
Act. See In the Matter of the Application of Jason Leopold to Unseal Certain Electronic
Surveillance Applications and Orders, No. 13-mc-00712-BAH (D.D.C.) ("Leopold").

A recent filing in *Leopold* details efforts by the district court, its clerk's office, the DOJ, 15 and the petitioners to unseal applications and orders in certain electronic surveillance cases. See 16 Mackey Decl., Ex. M. To date, the *Leopold* petition has resulted in the release of lists identifying 17 PR/TT applications filed by the United States Attorney's Office for the District of Columbia 18 between 2008 and 2016 (approximately 700 pages), the approximate number of matters filed under 19 section 2703(d) of the SCA, extraction charts for the PR/TT applications (approximately 50 pages), 20and total or partial unsealing of PR/TT matters where the application was denied or a substantive 21 opinion issued. See id. at 2-3. As for prospective relief, the D.D.C. Clerk's Office will now permit 22 23 electronic filing and public reporting of caption information in certain surveillance cases. *Id.* at 3. The *Leopold* case is still pending, but already the government has acknowledged that "[b]y filing 24 this lawsuit, petitioners have been instrumental in prompting a sea change in how the Court and 25

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 11

the USAO-DC handle the filing of sealed matters under the Pen Register Statute and the SCA." *Id.* at 42.

In the Northern District of California, researchers Jennifer Granick and Riana Pfefferkorn
petitioned the court seeking the public docketing and unsealing of judicial records in that District
involving electronic surveillance under the Pen Register Act, the Stored Communications Act, the
Wiretap Act, and the All Writs Act. *See In re Petition of Jennifer Granick and Riana Pfefferkorn to Unseal Technical-Assistance Orders and Materials*, No. 16-mc-80206-KAW (N.D. Cal.). The
case is still pending. A Joint Status Report was filed on August 22, 2017, *see* Mackey Decl., Ex.
N, and a status conference is scheduled for December 7, 2017.

10

#### IV. LEGAL STANDARDS

The United States "has a long history of distrust for secret proceedings," which "are the exception rather than the rule in our courts." *United States v. Index Newspapers LLC*, 766 F.3d 1072, 1084 (9th Cir. 2014) (citations omitted). The documents Petitioner requests the Court unseal are subject to qualified rights of access to judicial proceedings under both the First Amendment and under the common law. *Press-Enter. II*, 478 U.S. at 8-9 (First Amendment); *Nixon*, 435 U.S. at 597 (footnotes omitted) (common law).

Petitioner has standing to unseal judicial records. "Members of the public have standing to 17 move to unseal criminal proceedings." United States v. Ring, 47 F. Supp. 3d 38, 41 (D.D.C. 2014) 18 (citing Press-Enter. Co. v. Superior Court, 478 U.S. 1 (1986) (Press-Enterprise II)). The sealing 19 of the requested materials constitutes "an injury [to Petitioner] that is likely to be redressed by a 20favorable decision" to unseal those materials. In re Wash. Post, 807 F.2d 383, 388 n.4 (4th Cir. 21 1986) (internal quotation marks and alteration omitted); see also Lujan v. Defenders of Wildlife, 22 23 504 U.S. 555, 560-61 (1992). Petitioner has sufficiently alleged (1) an injury to its right to access the court documents it seeks, that is (2) fairly traceable to the Court's sealing of those documents, 24 and is (3) likely to be redressed by a Court decision to unseal them and change its docketing 25

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 12

1 practices going forward.

A.

2

### The First Amendment Right of Access to Judicial Records and Proceedings

The First Amendment establishes a presumptive right of access to the Court's proceedings 3 and records. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 580-81 (1980); Associated 4 Press v. U.S. Dist. Court, 705 F.2d 1143, 1145 (9th Cir. 1983) (pre-trial documents); In re Special 5 Proceedings, 842 F. Supp. 2d 232, 239 (D.D.C. 2012) (collecting cases); Oregonian Publ'g Co. v. 6 U.S. Dist. Court, 920 F.2d 1462, 1465 (9th Cir. 1990) (citing Press-Enter. Co. v. Superior Court, 7 464 U.S. 501, 510 (1984) (*Press-Enterprise I*). This right of access "ensure[s] that th[e] 8 constitutionally protected 'discussion of governmental affairs' is an informed one." Globe 9 Newspaper Co. v. Superior Court, 456 U.S. 596, 604-05 (1982) (quotation omitted). The right is 10based on the history of open criminal trials in the American and English legal systems and on 11 policy grounds including the potential for public scrutiny to "enhance[] the quality and safeguard[] 12 the integrity of the factfinding process," the "appearance of fairness," and the opportunity for "the 13 public to participate in and serve as a check upon the judicial process." Id. at 605-06 (footnotes 14 omitted). As Chief Justice Burger famously wrote: "People in an open society do not demand 15 infallibility from their institutions, but it is difficult for them to accept what they are prohibited 16 from observing." Richmond Newspapers, 448 U.S. at 572. 17

Courts employ a two-part inquiry, commonly called the experience and logic test, to 18 determine whether the First Amendment right of access applies to particular judicial proceedings 19 or records. Press-Enter. II, 478 U.S. at 8-9; Times Mirror Co. v. United States, 873 F.2d 1210, 201213 n.4 (9th Cir. 1989) (applying the same test to the disclosure of "documents generated as part 21 of a judicial proceeding"). First, courts ask, "whether the place and process have historically been 22 23 open to the press and general public." Press-Enter. II, 478 U.S. at 8-9 (citation omitted). Second, courts ask, "whether public access plays a significant positive role in the functioning of the 24 particular process in question." Id. Importantly, in the Ninth Circuit, "logic alone, even without 25

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 13

experience, may be enough to establish the right" of access. *In re Copley Press, Inc.*, 518 F.3d
1022, 1026 (9th Cir. 2008) (citations omitted).

The public's presumptive First Amendment right of access to judicial proceedings and records can only be overcome by proof that limiting access satisfies a "compelling governmental interest" and that the restrictions are "narrowly tailored to serve that interest," *Globe Newspaper*, 457 U.S. at 606-07. The party seeking to override the public's right of access must show a "substantial probability" of harm if such restrictions are not present; even a "reasonable likelihood" of harm is insufficient under the First Amendment. *Press-Enter. II*, 478 U.S. at 14.

Further, any judicial decision to restrict the public's right of access must be "based on
[specific] findings that closure is essential to preserve higher values." *Press-Enter. I*, 464 U.S. at
510; *Oregonian Publ'g Co.*, 920 F.2d at 1465.

12

#### B. The Common Law Right of Access to Judicial Records

The common law right of access similarly presumes that a broad range of judicial records
must be public. Only "a narrow range of documents" is exempt from the common-law right of
public access, *Kamakana v. City & Cty. of Honolulu*, 447 F.3d 1172, 1178 (9th Cir. 2006), namely,
those which have "traditionally been kept secret for important policy reasons." *Times Mirror Co.*,
873 F.2d at 1219.

The Ninth Circuit has held there is a common law right of access to judicial records. Ctr. 18 for Auto Safety v. Chrysler Group, LLC, 809 F.3d 1092, 1102 (9th Cir. 2016). This access promotes 19 the "public interest in understanding the judicial process itself and the bases or explanations for a 20court's decision." Id. (internal citations omitted). A strong presumption of access applies to any 21 court document that is "strongly correlative to the merits of a case." Id. at 1099; see also United 22 23 States v. El-Sayegh, 131 F.3d 158, 163 (D.C. Cir. 1997) ("[W]hat makes a document a judicial record and subjects it to the common law right of access is the role it plays in the adjudicatory 24 process."). For example, documents are judicial records if "the district court ma[kes] any decisions 25

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 14

about the [documents] or [] otherwise relie[s] on them." *Dhiab v. Trump*, 852 F.3d 1087, 1103
(D.C. Cir. 2017) (internal quotations, citation, and alterations omitted). Judicial orders and the
documents underlying them are indisputably judicial records. *EEOC v. Nat'l Children's Ctr., Inc.*,
98 F.3d 1406, 1409 (D.C. Cir. 1996) ("A court's decrees, its judgments, its orders, are the
quintessential business of the public's institutions."); *see also Wash. Legal Found. v. United States Sentencing Comm'n*, 89 F.3d 897, 905 (D.C. Cir. 1996).

"When the common law right of access applies to the type of document at issue in a 7 particular case, 'a "strong presumption in favor of access" is the starting point." United States v. 8 Bus. of Custer Battlefield Museum and Store, 658 F.3d 1188, 1194 (9th Cir. 2011) (quoting g Kamakana, 447 F.3d at 1178; further citation omitted). A party seeking to seal a judicial record 10must overcome this strong presumption by articulating compelling reasons for sealing that 11 outweigh the general history of access and the public policies favoring disclosure. The court must 12 "conscientiously balance[] the competing interests" of the public and of the party who seeks to 13 keep certain judicial records secret. Foltz v. State Farm Mut. Auto. Ins. Co., 331 F.3d 1122, 1135 14 (9th Cir. 2003). If the court decides to seal certain judicial records, it must "base its decision on a 15 compelling reason and articulate the factual basis for its ruling, without relying on hypothesis or 16 conjecture." Hagestad v. Tragesser, 49 F.3d 1430, 1434 (9th Cir. 1995) (citation omitted). 17

18

19 20

#### V. ARGUMENT

#### A. Petitioner Has a Right to Access Basic Docketing Information Regarding Electronic Surveillance Cases in This District

Petitioner has both constitutional and common law rights to access basic docketing information regarding cases filed in this Court. Under the Court's current docketing practices, however, even basic docket sheet information regarding electronic surveillance cases (*e.g.*, the case number) is sealed such that these cases are completely hidden from public view—in many instances indefinitely.

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 15

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 25 of 41

Operating a secret docket for certain surveillance cases while also maintaining a public
 docket for other criminal proceedings is "facially unconstitutional." *United States v. Ochoa- Vasquez*, 428 F.3d 1015, 1029 (11th Cir. 2005) (citing *United States v. Valenti*, 987 F.2d 708, 715
 (11th Cir. 1993)). It "violates the public and press's First Amendment right of access to criminal
 proceedings." *Co. Doe v. Public Citizen*, 749 F.3d 246, 268 (4th Cir. 2014) (citing *Valenti*, 987
 F.2d at 715).

A secret docketing system "can effectively preclude the public and the press from seeking
to exercise their constitutional right of access" to court records. *Valenti*, 987 F.2d at 715. In short,
a "district court . . . cannot employ . . . secret docketing procedures." *Ochoa-Vasquez*, 428 F.3d at
1030. *See generally In re Sealed Case*, 199 F.3d 522, 525 (D.C. Cir. 2000) (collecting federal
appeals court cases requiring public docketing in judicial proceedings other than grand jury
matters); *Media Gen. Operations, Inc. v. Buchanan*, 417 F.3d 424, 437 (4th Cir. 2005) (court clerk
must maintain a public docket of search warrant proceedings, once warrant has been returned).

The Court's current practice of docketing non-warrant electronic surveillance cases as 14 Grand Jury (GJ) cases violates Petitioner's constitutional and common law rights of access to 15 judicial proceedings and records in those cases. When the Court dockets non-warrant surveillance 16 cases as Grand Jury (GJ) cases, they are indefinitely sealed and inaccessible to the public. See 17 Hsieh Decl. ¶ 19-21. Because there is no public docket for these non-warrant surveillance cases, 18 there is no public record for when and how often law enforcement seeks them. Id. Further, because 19 there is no public docket indicating these records exist, the press and the public have no ability to 20monitor and make particularized requests to unseal information in specific cases. Id. 21

The First Amendment right of access requires this Court's non-warrant surveillance
 dockets be made public because such secrecy runs counter to both experience and logic.

First, the United States has a "centuries-long history of public access to dockets." *United States v. Mendoza*, 698 F.3d 1303, 1304 (10th Cir. 2012). This historic tradition counsels for

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 16

1 granting Petitioner access to the requested docket sheets.

Second, logic also supports unsealing the docket sheet information sought here. Public 2 docket sheets play a key role in the public's relationship with the courts. The docket sheet notifies 3 the public of the existence of a matter, and of activity in a matter. Ochoa-Vasquez, 428 F.3d at 4 1029 n.15 (citation omitted). Docket sheets provide an index to judicial proceedings and 5 documents, and endow the public and press with the capacity to exercise their rights of access 6 guaranteed by the First Amendment. Hartford Courant Co. v. Pellegrino, 380 F.3d 83, 93 (2d Cir. 7 2004). Sealed docket sheets frustrate the ability of the public to oversee the judicial process. 8 Pellegrino, 380 F.3d at 94. Secrecy erodes the legitimacy of the institution of the courts: g Maintaining "a two-tier system, open and closed," threatens public "[c]onfidence in the accuracy 10of [the court's] records ..., ... the authority of its rulings and the respect due its judgments." CBS, 11 Inc. v. U.S. Dist. Ct., 765 F.2d 823, 826 (9th Cir. 1985) (Kennedy, J.). 12

Further, because courts have historically made their dockets publicly available, the 13 common law right of access applies and requires disclosure of the docket sheet information 14 requested by Petitioner. See In re Application of N.Y. Times Co. for Access to Certain Sealed Court 15 *Records*, 585 F. Supp. 2d 83, 88-89 (D.D.C. 2008) ("[T]here is an historic common law right of 16 access to judicial records and documents that has been recognized in United States courts for well 17 over a century"); In re Sealing & Non-Disclosure, 562 F. Supp. 2d 876, 895 (S.D. Tex. 2008) ("It 18 is difficult to conceive any circumstance under which permanent sealing of the entire file, 19 including the order itself, could ever be justified."). 20

"[M]aking court files accessible" is particularly appropriate where, as here, the government
is a party to the matter: "in such circumstances, the public's right to know what the executive
branch is about coalesces with the concomitant right of the citizenry to appraise the judicial
branch." *Fed. Trade Comm'n v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404, 410 (1st Cir. 1987)
(*FTC*); *see also Doe*, 749 F.3d at 271 ("[T]he public has a strong interest in monitoring not only

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 17

1 functions of the courts but also the positions that its elected officials and government agencies take
2 in litigation" (citing *FTC*)).

While keeping certain information regarding electronic surveillance proceedings secret 3 during the pendency of an investigation can make sense, eventually those matters must be publicly 4 docketed, to provide notice and "an opportunity ... to voice objections to the denial of access." 5 Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989). This is the minimum level of 6 transparency necessary to ensure electronic surveillance decisions are both known and accountable 7 to the public and to other judges. There is no compelling countervailing reason that prevents 8 unsealing docket sheets for investigations that have concluded. See In re State-Record Co., Inc., g 917 F.2d 124, 129 (4th Cir. 1990) ("we can not understand how the docket entry sheet could be 10prejudicial"). 11

Moreover, even during the pendency of an investigation, when there may be compelling 12 reasons to maintain certain information under seal, there is no compelling reason why the public 13 should not know of the existence of an electronic surveillance request, along with certain basic 14 categories of information regarding the request, such as: (1) law enforcement agency filing the 15 application; (2) jurisdictional authority (e.g., PRA, SCA, Wiretap Act, AWA); (3) relief sought 16 (e.g., search warrant, seizure warrant, wire interception, pen register, trap and trace, tracking 17 device, prospective cell site data, historical cell site data, toll records, email contents, customer 18 account records); and (4) recipient of order/warrant (e.g., identity of phone company, ISP). See 19 Mackey Decl., Ex. H at 335. Such basic docket information need not include information such as 20telephone numbers or email addresses that could be used to identify particular suspects or 21 investigative targets. 22

As noted above, at least one other district court has agreed to change its docketing procedures to provide for the electronic filing and public reporting of caption information in certain surveillance cases. *See* Mackey Decl., Ex. M at 3.

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 18

Petitioner respectfully requests the Court to publicly docket electronic surveillance cases filed in this District and to unseal and require public disclosure of basic docketing information 2 regarding those cases, as detailed in Section VI, *infra*, and in the accompanying proposed order. 3

4 5

**B**.

1

#### Petitioner Has a Right to Access Electronic Surveillance Applications and Orders Filed in This District, Once Secrecy is No Longer Necessary

Petitioner also has constitutional and common law rights to access the underlying 6 electronic surveillance applications, orders, and related materials filed in this Court, when secrecy 7 is no longer necessary and privacy interests can be addressed via redaction. More specifically, as 8 9 detailed in Section VI, *infra*, Petitioner seeks access to applications and supporting documents, including affidavits, and orders granting or denying said applications in certain electronic 10surveillance cases filed under the Pen Register Act, the Stored Communications Act, the Wiretap 11 Act, and the All Writs Act. 12

13 Courts consistently hold that a right of access attaches to search warrant materials once secrecy is no longer justified. See In re Search Warrant for Secretarial Area Outside Office of 14 Gunn, 855 F.2d 569, 573 (8th Cir. 1988) (holding there is a qualified First Amendment right to 15 inspect search warrants once the warrant is executed); In re Application and Affidavit for a Search 16 Warrant, 923 F.2d 324, 331 (4th Cir. 1991) (affirming order unsealing search warrant at post-17 indictment, pretrial stage); Application of Newsday, Inc., 895 F.2d 74, 79 (2d Cir. 1990) (finding 18 common law right of access to search warrant once plea agreement reached and government admits 19 20need for secrecy is over); see also Custer Battlefield Museum, 658 F.3d at 1196 (reserving the question of whether the First Amendment right covers warrant materials post-investigation but 21 finding a common-law right). 22

23 There is a "clear trend" of finding a First Amendment right to access warrant materials initially filed under seal. United States v. Loughner, 769 F. Supp. 2d 1188, 1193 (D. Ariz. 2011). 24 In Loughner, the court held that the "experience" prong of the First Amendment test was met. Id. 25

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 19

The court also found that the logic prong was met. "[E]ven after the fact," the court reasoned,
 public scrutiny of the warrant process can "further the public's interest in understanding the justice
 system" and "how well it works," and "may also serve to deter unreasonable warrant practices,
 either by the police or the courts." *Id.* at 1193-94 (citations omitted).

The same First Amendment right supports Petitioner's request to access the non-warrant 5 surveillance materials sought here. The non-warrant electronic surveillance records Petitioner 6 seeks to unseal serve the same purpose as search warrants in the judicial system-they authorize 7 government information collection and compel third-party assistance to collect that information. 8 The experience of courts unsealing search warrant materials when secrecy is no longer justified g directly applies to unsealing other types of surveillance orders law enforcement seeks and obtains 10in this Court. Moreover, logic supports unsealing these records because, like disclosing search 11 warrant materials, disclosing non-warrant surveillance materials will further the public's 12 understanding of law enforcement, the Court, and the operation of the criminal justice system. 13

The common-law right of access also supports unsealing non-warrant materials when secrecy is no longer justified. Courts have recognized that post-investigation search warrant materials "'have historically been available to the public.'" *Custer Battlefield Museum*, 658 F.3d at 1193 (quoting *In re N.Y. Times Co.*, 585 F. Supp. 2d at 88). Warrant applications generally may not "be sealed indefinitely after the investigation comes to a close," and should be sealed "only in exceptional cases." *In re Sealing & Non-Disclosure*, 562 F. Supp. 2d 876, 892 (S.D. Tex. 2008) (citation omitted).

These authorities apply with equal force to non-search warrant surveillance materials because "[s]ociety has an understandable interest . . . in law enforcement systems and how well they work. The public has legitimate concerns about methods and techniques of police investigation . . . ." *In re Application and Affidavit for a Search Warrant*, 923 F.2d 324, 331 (4th Cir. 1991). The public interest in government demands for technical assistance in executing search

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 20

warrants on encrypted information supports unsealing of the requested materials. *See* Mackey
 Decl. ¶¶ 2-15; Hsieh Decl. ¶¶ 13-14. No "sufficiently compelling reasons" exist to justify indefinite
 sealing. *Foltz*, 331 F.3d at 1135 (citation omitted).

4 5

# 1. Petitioner Has a Right to Access the Requested Pen Register Act Materials

Under the First Amendment experience and logic test, Petitioner has a constitutional right 6 of access to post-investigation Pen/Trap materials, including orders authorizing the installation and 7 use of a pen register or a trap and trace device under 18 U.S.C. § 3123 and orders requiring a third 8 9 party to provide information, facilities, or technical assistance to law enforcement officials under 18 U.S.C. § 3124. Permitting inspection of Pen/Trap applications and orders once an investigation 10has concluded will further public understanding of the law and "will enable the public to evaluate 11 for itself whether the government's [requests] went too far-or did not go far enough." Loughner, 12 13 769 F. Supp. 2d at 1994 (internal citation and quotation marks omitted).

The public also has a common law right of access to post-investigation Pen/Trap materials. 14 In re Sealing & Non-Disclosure, 562 F. Supp. 2d at 894, 896. This Court has discretion to unseal 15 these materials. Pen/Trap orders must be sealed "until otherwise ordered by the court." 18 U.S.C. 16 § 3123(d)(1). "How long a pen/trap order should be sealed, and whether sealing should continue 17 beyond the life of the pen register itself, is left to the sound discretion of the court." In re Sealing 18 & Non-Disclosure, 562 F. Supp. 2d at 879. The Court should exercise its discretion and unseal the 19 20requested Pen/Trap materials because indefinite sealing "deprive[s] the law-abiding public of significant data about the frequency of compelled Government access to individual e-mail and 21 phone records." Id. at 886. 22

No competing interest merits indefinite sealing of post-investigation Pen/Trap materials,
under either a First Amendment or common law analysis. The unsealing and public disclosure of
the Pen/Trap materials requested by Petitioner in Section VI, *infra*, would not jeopardize current

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 21

or future investigations, and any sensitive information in those materials could be redacted as
 further explained below.

2.

3

4

#### Petitioner Has a Right to Access the Requested Stored Communications Act Materials

Petitioner has constitutional and common law rights of access to the SCA materials
requested in Section VI, *infra*, including orders under 18 U.S.C. § 2703(d) requiring disclosure of
communications, records, or other information pertaining to a subscriber or a customer.

8 Under the "experience and logic" test, Petitioner has a First Amendment right of access to
9 the requested SCA materials. Although there is no historical tradition of access to SCA materials,
10 the Ninth Circuit has held that the "logic" prong alone can establish a right of access if "public
11 scrutiny" would "benefit" the proceedings. *See Copley Press*, 518 F.3d at 1026-27.

Logic supports Petitioner's right of access to these SCA materials. Section 2703(d) orders, 12 like any orders issued by a court, are judicial records. United States v. Appelbaum, 707 F.3d 283, 13 290-91 (4th Cir. 2013). They serve a similar role as search warrants do, which is to ensure judicial 14 oversight of information collection during an investigation. There is no logical reason to treat 15 Section 2703(d) orders differently from search warrants and related materials once an investigation 16 has concluded. Therefore, SCA orders and related documents should be treated like post-17 18 indictment search warrant materials, for which there is a First Amendment right of access. Loughner, 769 F. Supp. 2d at 1193-94 (applying "logic" prong after holding "experience" prong 19 met).<sup>1</sup> 20

21

As with search warrant materials, opening Section 2703 materials to public scrutiny post-

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 22

<sup>22</sup> 

 <sup>&</sup>lt;sup>1</sup> The Fourth Circuit's denial in *Appelbaum* of a First Amendment right of access to Section 2703(d) materials is distinguishable because Petitioner here seeks post-investigation SCA materials. 707 F.3d at 291-92 (holding that because secrecy was necessary to support ongoing criminal investigations in which such orders were sought). The *Appelbaum* court did not consider whether the First Amendment right of access attached to materials once an investigation had concluded.

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 32 of 41

*investigation* serves several important public interests. These interests include: "knowing that
proper procedures have been followed"; "understanding the justice system"; "deter[ring]
unreasonable [surveillance] practices, either by the police or the courts"; and "ensur[ing] that
judges are not merely serving as a rubber stamp for the police." *Loughner*, 769 F. Supp. 2d at 1194
(citations and internal quotation marks omitted).

All of these interests are at stake in Section 2703(d) orders as in search warrants—perhaps
even more so. Indeed, because Section 2703(d) orders require an evidentiary showing lower than
the probable-cause warrant standard, public scrutiny is arguably even more important to ensure
that courts are not giving too much power to law enforcement under this less-demanding bar. *See United States v. Espudo*, 954 F. Supp. 2d 1029, 1033 (S.D. Cal. 2013) (Section 2703(d)'s "'specific
and articulable facts' standard [for issuance of a court order for disclosure of user's records] is a
significantly lower legal hurdle than probable cause." (citation omitted)).

There is thus a First Amendment right of access to the Section 2703(d) orders and related
materials sought by Petitioner, and there is no compelling interest to keep them sealed.

Petitioner also has a common law right of access to the requested SCA materials. SCA orders are "judicially authored or created documents." *Appelbaum*, 707 F.3d at 290-91. Applications and related materials are also "judicial records" because they play a role in the adjudicatory process: "they were filed with the objective of obtaining judicial action or relief pertaining to § 2703(d) orders." *Id.* (citations to First, Second, Fourth, and D.C. Circuit authorities omitted).

The common law presumption of access outweighs any countervailing interests in maintaining under seal the SCA materials requested by Petitioner. The government's "significant countervailing interest" identified by the *Applebaum* court—not hampering ongoing investigations or tipping off targets, 707 F.3d at 292-94—does not apply to Petitioner's request, which provides a mechanism for the continued sealing of SCA materials for which there is a compelling

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 23

confidentiality interest such as protecting an ongoing law enforcement investigation.

1

2

3

4

5

3. Petitioner Has a Right to Access the Requested Wiretap Act Materials Petitioner has constitutional and common law rights of access to the Wiretap Act materials requested in Section VI, infra, including orders requiring a third party to provide technical assistance to law enforcement officials under 18 U.S.C. § 2511(2)(a)(ii).

Although there is a statutory scheme for unsealing the underlying wiretap applications and 6 orders themselves under 18 U.S.C. § 2518(8)(b),<sup>2</sup> Petitioner has an independent First Amendment 7 right of access to the requested third-party technical assistance materials. "[A] statute cannot 8 override a constitutional right" of access. NYT I, 828 F.2d at 115 (footnote omitted). Logic supports g a First Amendment right of access here. The requested unsealing would "play[] a significant 10positive role in the functioning of" how this Court administers third-party assistance orders sought 11 by law enforcement under the Wiretap Act. *Press-Enter. II*, 478 U.S. at 8 (citation omitted). 12

Petitioner's request includes a mechanism for the continued sealing of Wiretap Act 13 materials for which there is a compelling confidentiality interest such as protecting an ongoing law 14 enforcement investigation. Petitioner's request further includes a mechanism for the redaction of 15 certain information (e.g., personal identifiers) from unsealed documents. Accordingly, the Wiretap 16 Act's privacy interests can be satisfied while permitting public access to the requested records. See 17 generally Mackey Decl., Ex. O (describing the growing, ahistorical trend of indefinitely-sealed 18 records and its threat to the public and the institution of the judiciary); Mackey Decl., Ex. H (in-19 depth dive into "the most secret court docket in America": electronic surveillance matters under 20SCA, Wiretap, and Pen/Trap Acts). 21

- 22

The mechanisms for continued sealing and redaction provided in Petitioner's request

23 24

25

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 24

<sup>&</sup>lt;sup>2</sup> 18 U.S.C. § 2518(8)(b) states that "[a]pplications made and orders granted under this chapter shall be sealed by the judge . . . [and] disclosed only upon a showing of good cause before a judge of competent jurisdiction." The statute seeks to protect the integrity of ongoing investigations and the privacy interests of innocent third parties and of defendants.

distinguish this request from decisions in other Circuits holding that the Wiretap Act's secrecy and 1 confidentiality provisions outweigh the public's right of access. See In re N.Y. Times Co., 828 F.2d 2 110, 116 (2d Cir. 1987); In re N.Y. Times Co., 577 F.3d 401, 409-11 (2d Cir. 2009). It is Petitioner's 3 understanding that the Ninth Circuit has not yet addressed how the Wiretap Act's secrecy 4 provisions interact with the First Amendment right of access to third-party technical assistance 5 orders under the Wiretap Act. See United States v. Chow, No. 14-cr-00196, 2015 U.S. Dist. LEXIS 6 114802, at \*12 (N.D. Cal. Aug. 28, 2015) (noting the lack of binding Ninth Circuit precedent on 7 access to wiretap materials). 8

9 4. Petitioner Has a Right to Access the Requested All Writs Act Materials
10 Petitioner has constitutional and common law rights of access to the All Writs Act materials
11 requested in Section VI, *infra*, including orders requiring third parties to provide technical
12 assistance to law enforcement officials under 28 U.S.C. § 1651(a).

Petitioner has a First Amendment right of access to the requested AWA materials. The 13 "experience" prong is easily met for the requested AWA materials, including court orders and 14 related documents. This is because "there is a venerable tradition of public access to court orders." 15 United States v. Ressam, 221 F. Supp. 2d 1252, 1262 (W.D. Wash. 2002) (qualified First 16 Amendment right of access attached to protective orders, which court ordered made publicly 17 available with classified information redacted); see also Pepsico, Inc. v. Redmond, 46 F.3d 29, 31 18 (7th Cir. 1995) (Easterbrook, J., in chambers) ("Opinions are not the litigants' property. They 19 belong to the public, which underwrites the judicial system that produces them." (citations 20omitted)). It should be uncontroversial that the "venerable tradition" of access encompasses the 21 requested court orders issued under the AWA, first enacted in 1789,<sup>3</sup> even though the AWA's use 22 in connection with other authorities that authorize law enforcement electronic surveillance is 23

24

25

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 25

<sup>&</sup>lt;sup>3</sup> The All Writs Act was originally enacted as part of the Judiciary Act of 1789, 1 Stat. 73, § 14 (Sept. 24, 1789).

relatively new. *See N.Y. Tel.*, 434 U.S. at 174-75 (holding in 1977 that AWA was properly used to
compel installation of pen register).

The logic prong also supports First Amendment access to the requested AWA materials. 3 Courts cannot issue stand-alone AWA orders. United States v. Denedo, 556 U.S. 904, 911 (2009) 4 ("As the text of the All Writs Act recognizes, a court's power to issue any form of relief ... is 5 contingent on that court's subject-matter jurisdiction over the case"). Issuance of an order under 6 the AWA requires "the existence of a previously-issued court order or warrant"; otherwise, "no 7 jurisdiction exists." In re Application of the United States, 128 F. Supp. 3d 478, 483 (D.P.R. 2015). 8 Because the AWA materials Petitioner seeks must have issued in furtherance of an underlying g warrant or non-warrant surveillance order, and because there is a right of access to those underlying 10documents as explained above, it follows logically that there is a right of public access to the 11 related AWA orders as well. See Loughner, 769 F. Supp. 2d at 1194 (listing interests). Logic also 12 compels access because it would allow the public to better understand how law enforcement uses 13 the AWA to accomplish some of its most controversial surveillance of individuals' digital devices, 14 as detailed in Section III.B.4 above. 15

Petitioner also has a common law right of access to the requested AWA materials. The 16 common law presumption of access attaches to these AWA materials because they qualify as 17 "judicial records." See Pepsico, 46 F.3d at 31 (courts' opinions "belong to the public" (citations 18 omitted)); Glaxo Grp. Ltd. v. Leavitt, 481 F. Supp. 2d 437, 438 (D. Md. 2007) (refusing to seal 19 publicly-issued opinion because "fundamentally, ... this court is a public institution doing the 20public's business. The public interest in an accountable judiciary generally demands that the 21 reasons for a judgment be exposed to public scrutiny." (citations and internal quotation marks 22 omitted)). 23

The government's applications for AWA orders and supporting (or opposing) materials are also "judicial records." *See Custer Battlefield Museum*, 658 F.3d at 1193 (deciding to "treat[]

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 26

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 36 of 41

search warrant affidavits as judicial records"). Because AWA orders must be premised on an
underlying warrant or order, it follows that AWA applications and supporting materials are, like
the original warrant affidavits, also "judicial records." *Cf. United States v. Tillman*, No. 07-cr1209, 2009 U.S. Dist. LEXIS 35400, at \*4 (S.D.N.Y. Apr. 6, 2009) (court order, government's
application for disclosure of defendant's tax returns, and supporting papers were "judicial
documents").

Therefore, a "strong presumption in favor of access" attaches to the requested AWA materials. *Foltz*, 331 F.3d at 1135 (citation omitted). Petitioner's request provides mechanisms for continued sealing and redaction, so disclosure will not "jeopardize an important law enforcement or security interest in this particular instance." *Tillman*, 2009 U.S. Dist. LEXIS 35400, at \*11-12 ("general proposition" that government's applications for court orders may sometimes contain sensitive details of ongoing investigations does not "justify a blanket rule of permanent nondisclosure").

14

C.

15

#### Redaction Is an Appropriate Mechanism to Address Privacy Interests and Other Concerns with Petitioner's Request to Unseal Judicial Records

Petitioner's request includes a mechanism for the redaction of sensitive information (*e.g.*, personal identifiers) from unsealed documents. Redaction is an appropriate way to address privacy interests and other concerns with Petitioner's request to unseal judicial records in electronic surveillance cases.

Petitioner acknowledges that the requested materials may contain sensitive information for which there is a legitimate need to maintain secrecy. However, the need to maintain secrecy for certain information in the requested records is not a sufficiently compelling reason to maintain the broad sealing of all records sought by Petitioner—obscuring the very existence of the records themselves—much less rebut Petitioner's First Amendment and common law rights of access to those judicial records. Redaction, rather than wholesale indefinite sealing, is the better way to

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 27

#### Case 2:17-mc-00145-RSL Document 1 Filed 11/15/17 Page 37 of 41

1 manage these competing interests. *See Custer Battlefield Museum*, 658 F.3d at 1195 n.5
2 (competing concerns can typically be accommodated "by redacting sensitive information rather
3 than refusing to unseal the materials entirely." (citations omitted)).

4

As noted above, Petitioner's request includes a mechanism for the continued sealing of documents for which secrecy is needed to protect an ongoing law enforcement investigation. Once the underlying investigation has concluded, however, the need for sealing goes away, and "[1]egitimate confidentiality interests" can be adequately protected through the less-restrictive means of redaction. *In re Sealing & Non-Disclosure*, 562 F. Supp. 2d at 886, 894-95 (footnote and citation omitted).

Petitioner does not object in general to redactions required by statute or rule, or to the redaction of sensitive law-enforcement information or personal information such as names or contact information of defendants, victims, unindicted third parties, surveillance targets, their interlocutors, or confidential informants. Petitioner does, however, request that the names of companies that have received technical assistance orders and other orders seeking access to their users' or customers' electronic information and records not be redacted from documents unsealed in response to this Petition.

17

#### VI. SPECIFIC RELIEF REQUESTED

Petitioner seeks public docketing and unsealing of certain electronic surveillance
applications and orders filed in the United States District Court for the Western District of
Washington, as set forth below. Petitioner respectfully requests that the Court issue an order
providing the following prospective and retrospective relief.

22

23

24

25

#### For future cases filed in the Western District of Washington:

 All cases seeking any of the following shall be designated as a Magistrate Judge (MJ) case or as a Miscellaneous (MC) case in the Court's CM/ECF system, and the docket sheets in these cases shall be unsealed within 180 days after case opening,

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 28

except to the extent the Court grants a request for continued sealing:

an order authorizing the installation and use of a pen register or a trap and 2 a. trace device under 18 U.S.C. § 3123; 3 an order requiring a third party to provide information, facilities, or b. 4 technical assistance to law enforcement officials under 18 U.S.C. § 3124; 5 an order under 18 U.S.C. § 2703(d) requiring disclosure of communications, с. 6 records, or other information pertaining to a subscriber or customer, as 7 described in 18 U.S.C. § 2703(b) or (c); 8 d. a warrant requiring a provider of electronic communication service or 9 remote computing service to disclose the contents of a wire or electronic 10 communication as described in 18 U.S.C. § 2703(a) or (b), or a record or 11 other information pertaining to a subscriber or customer as described in 18 12 U.S.C. § 2703(c); 13 an order requiring a third party to provide technical assistance to law e. 14 enforcement officials under 18 U.S.C. § 2511(2)(a)(ii); or 15 f. an order requiring a third party to provide technical assistance to law 16 enforcement officials under 28 U.S.C § 1651(a). 17 2. All applications and supporting documents, including affidavits, seeking any of 18 1(a)-(f) and all orders granting or denying said applications shall be unsealed within 19 180 days after case opening, except to the extent the Court grants a request for 20continued sealing. 213. Requests for continued sealing shall identify with particularity the information in 22 each docket sheet and document to remain sealed and the compelling interest (e.g., 23 to protect an ongoing law enforcement investigation) that justifies the continued 24 sealing of that information. Except as otherwise provided by the Court, a continued 25

1

sealing order shall expire after 180 days, at which time the sealed information shall be unsealed and made publicly available. The Court may authorize the redaction of certain information (*e.g.*., personal identifiers) from unsealed docket sheets and documents.

4. To the extent not otherwise publicly disclosed, the following information shall be publicly disclosed in a notice filed at the time of the initial application: (1) law enforcement agency filing the application; (2) jurisdictional authority (*e.g.*, Wiretap Act, SCA, Pen/Trap Statute, Fed. R. Crim. P. 41); (3) relief sought (*e.g.*, search warrant, seizure warrant, wire interception, pen register, trap and trace, tracking device, prospective cell site data, historical cell site data, toll records, email contents, customer account records); (4) type of crime under investigation; (5) identity of recipient of order/warrant (*e.g.*, identity of phone company, Internet Service Provider).

For past cases filed in the Western District of Washington between January 1, 2011 and the present:

- 5. All docket sheets for cases seeking any of the following shall be unsealed within 180 days after the date of this Order, except to the extent the Court grants a request for continued sealing:
  - a. an order authorizing the installation and use of a pen register or a trap and trace device under 18 U.S.C. § 3123;
  - b. an order requiring a third party to provide information, facilities, or technical assistance to law enforcement officials under 18 U.S.C. § 3124;
  - c. an order under 18 U.S.C. § 2703(d) requiring disclosure of communications, records, or other information pertaining to a subscriber or customer, as described in 18 U.S.C. § 2703(b) or (c);

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 30

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

d.	a warrant requiring a provider of electronic communication service or	
	remote computing service to disclose the contents of a wire or electronic	
	communication as described in 18 U.S.C. § 2703(a) or (b), or a record or	
	other information pertaining to a subscriber or customer as described in 1	
	U.S.C. § 2703(c);	

- e. an order requiring a third party to provide technical assistance to law enforcement officials under 18 U.S.C. § 2511(2)(a)(ii); or
- f. an order requiring a third party to provide technical assistance to law enforcement officials under 28 U.S.C § 1651(a).

6. All applications and supporting documents, including affidavits, seeking any of 5(a)-(f) and all orders granting or denying said applications shall be unsealed within 180 days after the date of this order, except to the extent the Court grants a request for continued sealing.

7. Requests for continued sealing shall be filed within 120 days of the date of this order. Such requests shall identify with particularity the information in each docket sheet and document to remain sealed and the compelling interest (*e.g.*, to protect an ongoing law enforcement investigation) that justifies the continued sealing of that information. Except as otherwise provided by the Court, a continued sealing order shall expire after 180 days, at which time the sealed information shall be unsealed and made publicly available. The Court may authorize the redaction of certain information (*e.g.*, personal identifiers) from unsealed docket sheets and documents.

25 ///

///

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 31

#### VII. CONCLUSION

For the reasons explained herein, Petitioner respectfully requests that the Court grant the requested relief set forth above and in Petitioner's concurrently filed Proposed Order.

5		
6	Dated: November 15, 2017	Respectfully submitted,
7		By: <u>s/ Geoffrey M. Godfrey</u> Geoffrey M. Godfrey (SBN 46876)
8		godfrey.geoff@dorsey.com
9		By: <u>s/ Nathan T. Alexander</u>
10		Nathan T. Alexander (SBN 37040) alexander.nathan@dorsey.com
11		By: s/ David H. Tseng
12		David H. Tseng (SBN 48334) tseng.david@dorsey.com
13		DORSEY & WHITNEY LLP Columbia
14		Center 701 Fifth Avenue, Suite 6100
15		Seattle, WA 98104-7043 Telephone: (206) 903-8800 Facsimile:
16		(206) 903-8820
17		
18		Aaron Mackey (pro hac vice to be filed)
19		amackey@eff.org ELECTRONIC FRONTIER
20		FOUNDATION
21		815 Eddy Street San Francisco, CA 94109
22		Telephone: (415) 436-9333
23		Attorneys for Petitioner INDEX NEWSPAPERS LLC D/B/A THE
24		STRANGER
25		

PETITION TO UNSEAL ELECTRONIC SURVEILLANCE DOCKETS, APPLICATIONS, AND ORDERS - 32

1

2

3

4