

1 JENNIFER STISA GRANICK (SBN 168423)
jennifer@law.stanford.edu
2 RIANA PFEFFERKORN (SBN 266817)
riana@law.stanford.edu
3 559 Nathan Abbott Way
4 Stanford, California 94305-8610
Telephone: (650) 736-8675
5 Facsimile: (650) 725-4086

6 *Pro Se* Petitioners
7

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA

10 **IN RE:**
11 **PETITION OF JENNIFER GRANICK AND**
12 **RIANA PFEFFERKORN TO UNSEAL**
13 **TECHNICAL-ASSISTANCE ORDERS AND**
14 **MATERIALS**

CV 16 80206 MISC.

MISC. CASE NO.
15 **PETITION TO UNSEAL TECHNICAL-**
16 **ASSISTANCE ORDERS AND**
17 **MATERIALS**

ORIGINAL FILED
SEP 28 2016
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

KAW

1 Petitioners Jennifer Granick and Riana Pfefferkorn, researchers at the Stanford Center for
2 Internet and Society proceeding *pro se*, file this Petition to unseal court records. We file this
3 Petition so that the public may better understand how government agents are using legal
4 authorities to compel companies to assist them in decrypting or otherwise accessing private data
5 subject to surveillance orders. Petitioners hereby seek the docketing of surveillance orders issued
6 by this Court; the unsealing of those dockets; and the unsealing of the underlying Court records
7 in surveillance cases relating to technical-assistance orders issued by this Court to
8 communications service providers, smartphone manufacturers, or other third parties, in matters
9 where there is no longer any need for secrecy, as further explained below and in the attached
10 Memorandum of Points and Authorities. In support of the Petition, Petitioners file herewith said
11 Memorandum, the Declaration of Petitioner Riana Pfefferkorn, and a Proposed Order granting
12 Petitioners’ request.

13 **RELIEF REQUESTED**

14 Petitioners seek the docketing of the surveillance matters handled in this District; the
15 unsealing of the docket sheets; and the unsealing of technical-assistance applications and orders
16 issued by this Court, whether relating to access to encrypted information or to other forms of
17 compelled third-party assistance in carrying out court-authorized surveillance.

18 Specifically, Petitioners respectfully request that:

19 (1) the Court assign case numbers to, and docket in its Case Management/Electronic Case
20 Filing system (“CM/ECF”), any and all applications, motions, opposition briefs, orders, and/or
21 warrants, filed at any time, under the following statutes:

- 22 ● the Wiretap Act, 18 U.S.C. §§ 2510-2522;
- 23 ● the Stored Communications Act (or “SCA”), 18 U.S.C. §§ 2701-2712;
- 24 ● the Pen Register Act (or “Pen/Trap Act”), 18 U.S.C. §§ 3121-3127; and/or
- 25 ● the All Writs Act (or “AWA”), 28 U.S.C. § 1651;

26 (2) the docket sheets for the foregoing surveillance matters in number (1) above be
27 unsealed and made publicly available, including on CM/ECF;

28 (3) the underlying documents in the dockets for surveillance matters falling under the

1 following specific statutory provisions (relating to technical assistance), filed from January 1,
2 2006 through six months before the date this Petition is granted, be unsealed and made publicly
3 available, including on CM/ECF:

- 4 ● Sections 18 U.S.C. §§ 2511(2)(a)(ii) and/or 2518(4) of the Wiretap Act;
- 5 ● Section 18 U.S.C. § 2703 of the SCA;
- 6 ● Sections 18 U.S.C. §§ 3123(b)(2) and/or 3124(a) or (b) of the Pen/Trap Act; and/or
- 7 ● Section 28 U.S.C. § 1651(a) of the AWA;

8 and

9 (4) the Court revise its practices going forward, such that the Clerk's office will assign
10 case numbers to, docket, and enter into CM/ECF all applications and orders for search warrants,
11 surveillance, and technical assistance; the Court will undertake a periodic review (*e.g.*, annually
12 or biannually) of sealed dockets, warrants, surveillance orders, and technical-assistance orders;
13 and after such review, the Court will unseal those records for which there is no longer any need
14 for continued sealing.

15 Petitioners seek the unsealing of underlying materials only from cases where there is no
16 longer any need for secrecy, *e.g.*, the criminal investigation has terminated, the surveillance order
17 (including any delayed-notice order) has expired, or charges have been filed. These records are
18 public documents and should be publicly docketed and unsealed unless good cause exists on a
19 case-by-case basis for continued secrecy based on the facts and circumstances of the individual
20 matter.

21 Petitioners are unable to access these records without the assistance of the Court because
22 they are not entered into the Court's system, assigned case numbers, or docketed, and in any
23 event any identifying information from which Petitioners could identify the relevant matters is
24 sealed and outside of public view.

25 Petitioners are not seeking to unseal the names or other identifying information of targets
26 of any investigation or their associates. Because Petitioners are interested in the development of
27 the law of technical assistance, names and other identifying information can be redacted from
28 unsealed materials.

1 As explained in the attached Memorandum of Points and Authorities, the purpose of this
2 Petition is to promote the public interest by illuminating the legal authorities under which law
3 enforcement may require the assistance of third parties in conducting court-authorized searches,
4 seizures, data collection, or surveillance. Publicly docketing and unsealing the requested
5 materials would inform the current public debate over encryption policy including pending
6 legislation, would further public understanding of surveillance law, would help reveal law
7 enforcement's legal authority to compel service providers to create and maintain surveillance-
8 capable communications and data services, and would serve the deep-seated American principle
9 of open access to the courts by disclosing documents for which there is no longer any reason for
10 continued secrecy.

11 Respectfully submitted,

12
13 Dated: September 28, 2016


14 JENNIFER STISA GRANICK (SBN 168423)
15 RIANA PFEFFERKORN (SBN 266817)

16 *Pro Se*

1 JENNIFER STISA GRANICK (SBN 168423)
jennifer@law.stanford.edu
2 RIANA PFEFFERKORN (SBN 266817)
riana@law.stanford.edu
3 559 Nathan Abbott Way
4 Stanford, California 94305-8610
Telephone: (650) 736-8675
5 Facsimile: (650) 725-4086

6 *Pro Se* Petitioners

ORIGINAL
FILED
SEP 28 2016
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

7
8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA

10
11 **IN RE:**
12 **PETITION OF JENNIFER GRANICK AND**
13 **RIANA PFEFFERKORN TO UNSEAL**
14 **TECHNICAL-ASSISTANCE ORDERS AND**
15 **MATERIALS**

CV 16 80206 MISC.

MISC. CASE NO.

16
17
18
19
20
21
22
23
24
25
26
27
28
**MEMORANDUM OF POINTS AND
AUTHORITIES IN SUPPORT OF
PETITION TO UNSEAL TECHNICAL-
ASSISTANCE ORDERS AND
MATERIALS**

KAW

TABLE OF CONTENTS

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
26
27
28

INTRODUCTION 1

PETITIONERS' REQUEST 2

JURISDICTION AND VENUE 3

INTRADISTRICT ASSIGNMENT 4

STANDING 4

BACKGROUND 4

 I. Interest of Petitioners 4

 II. Judicial Interpretation of Technical-Assistance Provisions Enables Novel and
 Controversial Surveillance 6

 A. Turning Consumer Goods into Eavesdropping Devices Under the
 Wiretap Act 6

 B. Obtaining Service-Wide Decryption Keys Under the Pen/Trap Act and
 the Stored Communications Act 7

 C. Forcing Security Modifications to Smartphones Under the All Writs Act 8

 III. Sealed Proceedings Deprive the Public of Information about Judicial
 Interpretations of Technical-Assistance Provisions 9

 IV. It Is in the Public Interest Judicial Documents Mandating Technical
 Assistance Eventually Be Unsealed 10

ARGUMENT 11

 I. The Public Has a Right of Access to Judicial Documents Concerning
 Technical-Assistance Applications and Orders 11

 A. Legal Standards for Public Right to Access Judicial Documents 11

 1. First Amendment Right of Access 11

 2. Common-Law Right of Access 13

 B. Petitioners' Right of Access to Each Category of Documents 13

 1. Docket Sheets 13

 2. Search and Seizure Warrants, Applications, and Supporting
 Materials 16

 3. Technical-Assistance Orders under the SCA 18

 4. Technical-Assistance Orders under the Pen/Trap Act 20

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
26
27
28

5. Technical-Assistance Orders under the AWA 21

6. Technical-Assistance Orders under the Wiretap Act 24

II. Redaction, Not Continued Sealing, Is the Proper Mechanism for Protecting
Any Sensitive Information..... 25

CONCLUSION 26

TABLE OF AUTHORITIES

Cases

1

2

3 *Associated Press v. U.S. District Court*, 705 F.2d 1143 (9th Cir. 1983)..... 11

4 *Baltimore Sun Co. v. Goetz*, 886 F.2d 60 (4th Cir. 1989) 15

5 *CBS, Inc. v. U.S. District Court*, 765 F.2d 823 (9th Cir. 1985)..... 14

6 *Company Doe v. Public Citizen*, 749 F.3d 246 (4th Cir. 2014)..... 14, 15

7 *Federal Trade Commission v. Standard Financial Management Corp.*,
8 830 F.2d 404 (1st Cir. 1987)..... 15

9 *Foltz v. State Farm Mutual Automobile Ins. Co.*, 331 F.3d 1122 (9th Cir. 2003)..... 13, 18, 23

10 *Glaxo Group Ltd. v. Leavitt*, 481 F. Supp. 2d 437 (D. Md. 2007) 23

11 *Globe Newspaper Co. v. Superior Court*, 456 U.S. 596 (1982) 12

12 *Hagestad v. Tragesser*, 49 F.3d 1430 (9th Cir. 1995) 13

13 *Hartford Courant Co. v. Pellegrino*, 380 F.3d 83 (2d Cir. 2004) 13, 14

14 *In re Application and Affidavit for a Search Warrant*, 923 F.2d 324
(4th Cir. 1991) 18

15 *In re Application of Jason Leopold to Unseal Certain Electronic Surveillance*
16 *Applications and Orders*, No. 13-mc-00712 (D.D.C. filed July 16, 2013) 16

17 *In re Application of the United States*, 128 F. Supp. 3d 478 (D.P.R. 2015)..... 22

18 *In the Matter of the Application of the United States for an Order Authorizing the*
19 *Roving Interception of Oral Communications*, 349 F.3d 1132
(9th Cir. 2003) 7

20 *In re Copley Press, Inc.*, 518 F.3d 1022 (9th Cir. 2008) 12, 18

21 *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484
(FISA Ct. 2007) 3

22 *In re New York Times Co.*, 585 F. Supp. 2d 83 (D.D.C. 2008) 17

23 *In re New York Times Co.*, 828 F.2d 110 (2d Cir. 1987)..... 24

24 *In re New York Times Co.*, 577 F.3d 401 (2d Cir. 2009)..... 24, 25

25 *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant*
26 *Issued by this Court*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) 8

27 *In re Order Requiring XXX, Inc.*, No. 14-mj-2258, 2014 U.S. Dist.
LEXIS 154743 (S.D.N.Y. Oct. 31, 2014)..... 8

28 *In re Sealed Case*, 199 F.3d 522 (D.C. Cir. 2000) 14

1	<i>In re Sealing & Non-Disclosure</i> , 562 F. Supp. 2d 876 (S.D. Tex. 2008).....	18, 21, 25
2	<i>In the Matter of the Search of an Apple iPhone Seized During the Execution of a</i>	
3	<i>Search Warrant on a Black Lexus IS300, California License Plate 5KGD203,</i>	
	No. 15-mj-0451, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016).....	9
4	<i>In re Search Warrant for Secretarial Area Outside Office of Gunn</i> , 855 F.2d 569	
5	(8th Cir. 1988)	17
6	<i>In re Special Proceedings</i> , 842 F. Supp. 2d 232 (D.D.C. 2012)	11
7	<i>In re State-Record Co., Inc.</i> , 917 F.2d 124 (4th Cir. 1990).....	16
8	<i>In re Under Seal (Lavabit)</i> , 749 F.3d 276 (4th Cir. 2014).....	7, 21
9	<i>In re Washington Post</i> , 807 F.2d 383 (4th Cir. 1986)	4
10	<i>In re WP Co. LLC</i> , No. 16-mc-351, 2016 U.S. Dist. LEXIS 109635 (D.D.C. Aug.	
	18, 2016)	17
11	<i>Kamakana v. City & County of Honolulu</i> , 447 F.3d 1172 (9th Cir. 2006).....	13
12	<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992)	4
13	<i>Media General Operations, Inc. v. Buchanan</i> , 417 F.3d 424 (4th Cir. 2005).....	14
14	<i>Nixon v. Warner Communications, Inc.</i> , 435 U.S. 589 (1978).....	3, 11
15	<i>Oregonian Publishing Co. v. U.S. District Court</i> , 920 F.2d 1462 (9th Cir. 1990).....	12
16	<i>Pepsico, Inc. v. Redmond</i> , 46 F.3d 29 (7th Cir. 1995).....	22, 23
17	<i>Press-Enterprise Co. v. Superior Court</i> , 464 U.S. 501 (1984).....	12
18	<i>Press-Enterprise Co. v. Superior Court</i> , 478 U.S. 1 (1986).....	<i>passim</i>
19	<i>Richmond Newspapers, Inc. v. Virginia</i> , 448 U.S. 555 (1980).....	11
20	<i>Seattle Times Co. v. U.S. District Court</i> , 845 F.2d 1513 (9th Cir. 1988).....	18
21	<i>Times Mirror Co. v. United States</i> , 873 F.2d 1210 (9th Cir. 1989).....	12, 13
22	<i>United States v. Appelbaum</i> , 707 F.3d 283 (4th Cir. 2013).....	15, 19, 20
23	<i>United States v. Business of Custer Battlefield Museum and Store</i> , 658 F.3d 1188	
24	(9th Cir. 2011)	<i>passim</i>
25	<i>United States v. Chow</i> , No. 14-cr-00196, 2015 U.S. Dist. LEXIS 114802 (N.D.	
	Cal. Aug. 28, 2015).....	24
26	<i>United States v. Denedo</i> , 556 U.S. 904 (2009).....	22
27	<i>United States v. Espudo</i> , 954 F. Supp. 2d 1029 (S.D. Cal. 2013)	20
28	<i>United States v. Index Newspapers LLC</i> , 766 F.3d 1072 (9th Cir. 2014)	11

1	<i>United States v. Loughner</i> , 769 F. Supp. 2d 1188 (D. Ariz. 2011)	<i>passim</i>
2	<i>United States v. Mendoza</i> , 698 F.3d 1303 (10th Cir. 2012)	14
3	<i>United States v. New York Telephone Co.</i> , 434 U.S. 159 (1977)	6, 8, 22
4	<i>United States v. Ochoa-Vasquez</i> , 428 F.3d 1015 (11th Cir. 2005).....	13, 14
5	<i>United States v. Ressam</i> , 221 F. Supp. 2d 1252 (W.D. Wash. 2002)	22
6	<i>United States v. Ring</i> , 47 F. Supp. 3d 38 (D.D.C. 2014)	4
7	<i>United States v. Tillman</i> , No. 07-cr-1209, 2009 U.S. Dist. LEXIS 35400 (S.D.N.Y. Apr. 6, 2009).....	23
8		
9	<i>United States v. Valenti</i> , 987 F.2d 708 (11th Cir. 1993)	14
10		
	<u>Statutes</u>	
11	18 U.S.C. §§ 2510-2522	2
12	18 U.S.C. § 2511(2)(a)(ii).....	3, 6, 24
13	18 U.S.C. § 2518(4).....	3, 6, 24
14	18 U.S.C. § 2518(8)(b)	24
15	18 U.S.C. §§ 2701-2712	2
16	18 U.S.C. § 2703.....	3, 7, 18
17	18 U.S.C. § 2705(b).....	1
18	18 U.S.C. §§ 3121-3127	2
19	18 U.S.C. § 3123(b)(2)	3, 7, 20
20	18 U.S.C. § 3123(d)(1)	21
21	18 U.S.C. § 3123(d)(2)	1
22	18 U.S.C. § 3124.....	7
23	18 U.S.C. § 3124(a)	3, 20
24	18 U.S.C. § 3124(b).....	3, 20
25	28 U.S.C. § 1391(b)(2)	4
26	28 U.S.C. § 1651.....	2
27	28 U.S.C. § 1651(a)	3, 8, 21
28	1 Stat. 73, § 14 (Sept. 24, 1789)	22

Other Authorities

1

2

3 American Civil Liberties Union, All Writs Act Orders for Assistance from Tech
4 Companies, <https://www.aclu.org/map/all-writs-act-orders-assistance-tech-companies> 10

5 Devlin Barrett, *Federal Prosecutors Drop Court Case to Force Apple to Unlock*
6 *iPhone*, Wall St. J. (Apr. 22, 2016), <http://www.wsj.com/articles/federal-prosecutors-drop-court-case-to-force-apple-to-unlock-iphone-1461377642> 9

7 Katie Benner and Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without*
8 *Apple*, N.Y. Times (Mar. 28, 2016),
9 <https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html> 9

10 Katie Benner, Eric Lichtblau, and Nick Wingfield, *Apple Goes to Court, and*
11 *F.B.I. Presses Congress to Settle iPhone Privacy Fight*, N.Y. Times
(Feb. 25, 2016), <https://www.nytimes.com/2016/02/26/technology/apple-unlock-iphone-fbi-san-bernardino-brief.html> 9

12 Brief of *Amici Curiae* iPhone Security and Applied Cryptography Experts in
13 Support of Apple Inc.’s Mot. to Vacate Order Compelling Apple Inc. to Assist
14 Agents in Search, and Opposition to Gov’t’s Mot. to Compel Assistance, *In*
15 *the Matter of the Search of an Apple iPhone Seized During the Execution of a*
16 *Search Warrant on a Black Lexus IS300, California License Plate 5KGD203,*
17 No. 16-cm-00010 (C.D. Cal. Mar. 4, 2016) 10

18 Urs Gasser, *et al.*, *Don’t Panic: Making Progress on the “Going Dark” Debate*
19 (2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf 7

20 Nicole Hong, *Judge Questions Legal Authority to Force Apple to Unlock iPhones*,
21 Wall St. J. (Oct. 26, 2015), <http://blogs.wsj.com/law/2015/10/26/judge-questions-legal-authority-to-force-apple-to-unlock-iphones/> 9

22 Eric Lichtblau and Katie Benner, *Apple Fights Order to Unlock San Bernardino*
23 *Gunman’s iPhone*, N.Y. Times (Feb. 17, 2016),
24 <https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html> 9

25 Ellen Nakashima, *Judge Rules in Favor of Apple in Key Case Involving a Locked*
26 *iPhone*, Wash. Post (Feb. 29, 2016),
27 https://www.washingtonpost.com/world/national-security/judge-rules-in-favor-of-apple-in-key-case-involving-a-locked-iphone/2016/02/29/fa76783e-db3d-11e5-925f-1d10062cc82d_story.html 8

28 Ellen Nakashima, *With Court Order, Federal Judge Seeks to Fuel Debate about*
Data Encryption, Wash. Post (Oct. 10, 2015),
https://www.washingtonpost.com/world/national-security/federal-judge-stokes-debate-about-data-encryption/2015/10/10/c75da20e-6f6f-11e5-9bfe-e59f5e244f92_story.html 8, 9

1 Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA’s Secret*
2 *Docket*, 6 Harv. L. & Pol’y Rev. 313 (2012)..... 25

3 Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*,
4 3 Fed. Cts. L. Rev. 177 (2009) 25, 26

5 **Rules**

6 Northern District of California Civil Local Rule 3-2(c)..... 4

7 Northern District of California Criminal Local Rule 56-1 commentary 11

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

INTRODUCTION

1
2 Americans' privacy and security are impacted when communications providers give the
3 government technical assistance in conducting surveillance. Yet the public is ignorant of
4 whether, when, and how providers are legally obligated to offer assistance. This important issue
5 is obscure because legal decisions interpreting and imposing technical-assistance obligations are
6 commonly sealed in perpetuity. To remedy this problem, this Petition asks the Court to docket its
7 surveillance matters, unseal the docket sheets, and unseal its technical-assistance applications,
8 opinions, and orders where there is no longer a need for ongoing secrecy, retroactively and going
9 forward.

10 Law enforcement routinely seeks the assistance of private companies in obtaining data in
11 the course of criminal investigations. In many cases, the private entity holds data relevant to an
12 investigation in a legible format and, upon receiving a judicial order, discloses it to police.
13 However, more recently, communications companies have started encrypting their users'
14 communications. Encryption can interfere with government ability to understand data that is
15 relevant to a criminal inquiry, even as it protects the public from hackers, identity thieves, and
16 suspicionless searches. Additionally, modern technology products may not presently collect data
17 about customers, but could nevertheless be reconfigured to do so upon government demand. Law
18 enforcement has sought and obtained, and is likely continuing to seek and to obtain, technical-
19 assistance orders forcing private companies to decrypt data, to disclose encryption keys, to turn
20 on microphones or cameras in consumer goods, to circumvent password lock-out mechanisms,
21 and more.

22 These novel forms of technical assistance take place pursuant to judicial orders.
23 Nevertheless, the public has very little insight into judicial interpretations of the law of technical
24 assistance. Commonly, the records of the government's applications, courts' resulting technical-
25 assistance orders to third parties, and the third parties' responses remain under seal indefinitely,
26 well beyond any need for secrecy. Providers who are subject to these technical-assistance
27 demands may be the subject of gag orders preventing them from independently disclosing any
28 information about the demand. *See* 18 U.S.C. §§ 2705(b), 3123(d)(2). Sealing interferes with

1 public understanding of technical-assistance demands, specifically whether legal orders take into
2 account the impact technical assistance can have on technology design, privacy, security, and
3 business interests.

4 Indefinite sealing of judicial orders is contrary to the long-standing American tradition of
5 open access to the courts. The public has a right under the First Amendment and the common
6 law to have access to judicial orders and proceedings concerning law enforcement efforts to
7 compel private entities to provide technical assistance in conducting government surveillance
8 and other investigative techniques. Petitioners Jennifer Granick and Riana Pfefferkorn
9 (“Petitioners”) therefore petition this Court for the following relief.

10 **PETITIONERS’ REQUEST**

11 Petitioners seek the docketing of the surveillance matters handled in this District; the
12 unsealing of the docket sheets; and the unsealing of technical-assistance applications and orders
13 issued by this Court, whether relating to access to encrypted information or to other forms of
14 compelled third-party assistance in carrying out court-authorized surveillance.

15 Specifically, Petitioners respectfully request that:

16 (1) the Court assign case numbers to, and docket in its Case Management/Electronic Case
17 Filing system (“CM/ECF”), any and all applications, motions, opposition briefs, orders, and/or
18 warrants, filed at any time, under the following statutes:

- 19 ● the Wiretap Act, 18 U.S.C. §§ 2510-2522;
- 20 ● the Stored Communications Act (or “SCA”), 18 U.S.C. §§ 2701-2712;
- 21 ● the Pen Register Act (or “Pen/Trap Act”), 18 U.S.C. §§ 3121-3127; and/or
- 22 ● the All Writs Act (or “AWA”), 28 U.S.C. § 1651;

23 (2) the docket sheets for the foregoing surveillance matters in number (1) above be
24 unsealed and made publicly available, including on CM/ECF;

25 (3) the underlying documents in the dockets for surveillance matters falling under the
26 following specific statutory provisions (relating to technical assistance), filed from January 1,
27 2006 through six months before the date this Petition is granted, be unsealed and made publicly
28 available, including on CM/ECF:

- 1 • Sections 18 U.S.C. §§ 2511(2)(a)(ii) and/or 2518(4) of the Wiretap Act;
- 2 • Section 18 U.S.C. § 2703 of the SCA;
- 3 • Sections 18 U.S.C. §§ 3123(b)(2) and/or 3124(a) or (b) of the Pen/Trap Act; and/or
- 4 • Section 28 U.S.C. § 1651(a) of the AWA;
- 5 and

6 (4) the Court revise its practices going forward, such that the Clerk's office will assign
7 case numbers to, docket, and enter into CM/ECF all applications and orders for search warrants,
8 surveillance, and technical assistance; the Court will undertake a periodic review (*e.g.*, annually
9 or biannually) of sealed dockets, warrants, surveillance orders, and technical-assistance orders;
10 and after such review, the Court will unseal those records for which there is no longer any need
11 for continued sealing.

12 Unfortunately, Petitioners are unable to provide the Court with any information to
13 identify specific matters containing the technical-assistance materials sought, because, as said,
14 the Clerk does not docket them or assign them case numbers, and in any event any identifying
15 information is sealed.

16 Importantly, Petitioners seek the unsealing of underlying materials only from cases where
17 there is no longer any need for secrecy, *e.g.*, the criminal investigation has terminated, the
18 surveillance order (including any delayed-notice order) has expired, or charges have been filed.
19 Further, Petitioners are not seeking to unseal the names or other identifying information of
20 targets of any investigation or their associates. Because Petitioners are interested in the
21 development of the law of technical assistance, names and other identifying information can be
22 redacted from unsealed materials.

23 **JURISDICTION AND VENUE**

24 The Court has jurisdiction over this Petition because “[e]very court has supervisory
25 power over its own records and files.” *Nixon v. Warner Commc’ns, Inc.*, 435 U.S. 589, 598
26 (1978). *Accord In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 487 (FISA Ct.
27 2007) (footnote omitted) (courts have “jurisdiction in the first instance to adjudicate a claim of
28 right to [their] very own records and files. ... [T]his Court’s inherent power over its records

1 supplies the authority to consider a claim of legal right to release of those records”).

2 Venue within this District is proper under 28 U.S.C. § 1391(b)(2) because the actions or
3 omissions giving rise to the action occurred within this District, namely, the sealing of the
4 specified judicial records of this Court that Petitioners seek to unseal.

5 **INTRADISTRICT ASSIGNMENT**

6 This action seeks District-wide relief, namely unsealing of the sealed judicial records
7 specified herein, wherever they may be located within this District. Therefore, pursuant to Civil
8 Local Rule 3-2(c), assignment to any division is proper.

9 **STANDING**

10 Petitioners have standing to unseal judicial records. “[M]embers of the public have
11 standing to move to unseal criminal proceedings.” *United States v. Ring*, 47 F. Supp. 3d 38, 41
12 (D.D.C. 2014) (citing *Press-Enter. Co. v. Superior Court*, 478 U.S. 1 (1986) (*Press-Enterprise*
13 *II*)). The sealing of the requested materials constitutes “an injury [to Petitioners] that is likely to
14 be redressed by a favorable decision” to unseal those materials. *In re Wash. Post*, 807 F.2d 383,
15 388 n.4 (4th Cir. 1986) (internal quotation marks and alteration omitted); *see also Lujan v.*
16 *Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).

17 **BACKGROUND**

18 **I. Interest of Petitioners**

19 Petitioner Jennifer Granick is the Director of Civil Liberties, and Petitioner Riana
20 Pfefferkorn is the Cryptography Fellow, at the Center for Internet and Society (“CIS”) in
21 Stanford, California. CIS is a public interest technology law and policy program at Stanford Law
22 School and a part of the school’s Law, Science and Technology Program. As part of our work at
23 CIS, we study the interaction of technology and the law and examine how that dynamic can
24 either promote or harm public goods such as privacy, free speech, innovation, and scientific
25 inquiry. Through our work, including the CIS blog, speeches, and publications, Petitioners
26 provide law students and the general public with educational resources and analyses of policy
27
28

1 issues arising at the intersection of law, technology, and the public interest.¹

2 Petitioners research and analyze judicially-authorized government surveillance activities
3 as a key part of our work. We investigate and analyze the policies and practices of the U.S. and
4 foreign governments for forcing decryption and/or influencing cryptography- or security-related
5 design of online platforms and services, devices, and products through the courts and
6 legislatures.² Petitioner Pfefferkorn’s position at CIS is specifically dedicated to researching
7 government surveillance and encryption law and policy.³ This Petition seeks to unseal court
8 records for Petitioners to use in our academic research, as well as for public scrutiny. Petitioners
9 bring this action in our individual capacities.

10 Prior to filing this action, Petitioner Pfefferkorn spoke with the Deputy Clerk of this
11 Court to inquire regarding the Court’s system for tracking surveillance orders and search
12 warrants.⁴ The Deputy Clerk informed Petitioner Pfefferkorn that the Clerk’s office keeps paper
13 records of warrants and surveillance orders authorized by the Court, but does not keep track of
14 them.⁵ According to the Deputy Clerk, warrants and surveillance orders are not entered into the
15 Court’s system or assigned a case number, so they are not searchable and there is no way to look
16 them up.⁶ The Deputy Clerk further informed Petitioner Pfefferkorn that these warrants and
17 orders are usually sealed and cannot be unsealed without a court order.⁷ The Deputy Clerk said
18 that the Clerk’s office has received requests in the past from members of the public to review
19 surveillance orders, but could not honor them.⁸

21 _____
22 ¹ See generally About Us, Center for Internet and Society, [https://cyberlaw.stanford.edu/about-](https://cyberlaw.stanford.edu/about-us)
23 [us](https://cyberlaw.stanford.edu/about-us); Blog, Center for Internet and Society, <https://cyberlaw.stanford.edu/blog>; Publications,
24 [Center for Internet and Society, https://cyberlaw.stanford.edu/publications.](https://cyberlaw.stanford.edu/publications)

25 ² See Crypto Policy Project, Center for Internet and Society, [https://cyberlaw.stanford.edu/our-](https://cyberlaw.stanford.edu/our-work/projects/crypto-policy-project)
26 [work/projects/crypto-policy-project.](https://cyberlaw.stanford.edu/our-work/projects/crypto-policy-project)

27 ³ See People: Riana Pfefferkorn, Center for Internet and Society,
28 [https://cyberlaw.stanford.edu/about/people/riana-pfefferkorn.](https://cyberlaw.stanford.edu/about/people/riana-pfefferkorn)

⁴ See Declaration of Riana Pfefferkorn ¶ 2, attached hereto (“Pfefferkorn Declaration”).
Surveillance orders and search warrants are where the technical-assistance orders Petitioners
seek would be contained.

⁵ *Id.* ¶¶ 3, 4.

⁶ *Id.* ¶ 3.

⁷ *Id.* ¶ 5.

⁸ *Id.*

1 Before filing the Petition, Petitioners attempted multiple times to meet and confer
2 telephonically with the United States Attorney’s Office for the Northern District of California
3 (“USAO”).⁹ Unfortunately, we were unable to do so.¹⁰

4 **II. Judicial Interpretation of Technical-Assistance Provisions Enables Novel and** 5 **Controversial Surveillance**

6 On request of law enforcement and under certain circumstances, U.S. courts may compel
7 phone companies, social networks, email providers, smart phone manufacturers, and others to
8 provide some technical assistance to law enforcement in carrying out search and seizure warrants
9 or other court-authorized acquisition of communications data. Historically, technical assistance
10 involved enlisting telephone companies to collect and disclose their customers’ calling records to
11 law enforcement. *See, e.g., United States v. N.Y. Tel. Co.*, 434 U.S. 159, 162 (1977) (upholding
12 use of All Writs Act order to compel installation of pen register).

13 More recently, technical-assistance demands are taking on a new and unprecedented
14 dimension. Law enforcement is obtaining controversial judicial orders purporting to compel
15 novel kinds of technical assistance—requiring on-board automobile assistance services to turn on
16 microphones in consumer products, demanding that communications providers to turn over
17 private encryption keys, and obligating phone manufacturers to decrypt data on handsets.
18 Whether courts may properly issue such orders under these legal provisions, and whether doing
19 so is wise, is a matter of heated public dispute.

20 **A. Turning Consumer Goods into Eavesdropping Devices Under the Wiretap** 21 **Act**

22 Judicial interpretation of the technical-assistance provisions of the Wiretap Act, 18
23 U.S.C. §§ 2511(2)(a)(ii) & 2518(4), may be enabling surveillance of oral communications via
24 smart TVs and other home consumer products. For example, in a 2003 decision, the Ninth
25 Circuit reviewed a district court decision to issue several *ex parte* orders pursuant to the Wiretap
26

27 ⁹ *Id.* ¶¶ 6, 7.

28 ¹⁰ *Id.*

1 Act, 18 U.S.C. § 2518(4), requiring an unnamed company to assist in intercepting conversations
2 occurring in a vehicle equipped with an on-board system that listened to occupants' voice
3 commands and gave directions and other assistance according to request. The district court
4 granted a government technical-assistance application to force the unnamed company to
5 surreptitiously turn on the microphone included in an automobile's communication system.
6 Though the Federal Bureau of Investigation ("FBI") had a court-issued warrant to conduct a
7 wiretap, the Ninth Circuit ultimately reversed the district court for a fact-specific reason. The
8 Court held that the technical assistance demanded was not authorized by the Wiretap Act on the
9 grounds that it would disable the service entirely. *In re U.S. for an Order Authorizing Roving*
10 *Interception of Oral Commc'ns*, 349 F.3d 1132, 1144-46 (9th Cir. 2003).

11 Today, the public does not know whether courts are using the Wiretap Act's technical-
12 assistance provisions to turn other home appliances into eavesdropping equipment, for example,
13 by requiring Samsung or Amazon to turn on the microphones in smart televisions or the Echo
14 home assistance device. See Urs Gasser *et al.*, *Don't Panic: Making Progress on the "Going*
15 *Dark" Debate* 13-14 (2016), [https://cyber.law.harvard.edu/pubrelease/dont-](https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf)
16 [panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf](https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf).

17 **B. Obtaining Service-Wide Decryption Keys Under the Pen/Trap Act and the**
18 **Stored Communications Act**

19 Courts may be using the technical-assistance provisions in the Pen Register/Trap and
20 Trace Act, 18 U.S.C. §§ 3123(b)(2), 3124 (hereinafter the "Pen/Trap Act"), or the provisions of
21 the Stored Communications Act ("SCA"), 18 U.S.C. § 2703, to force services to disclose their
22 private encryption keys to government investigators. For example, in 2013, a judge in the
23 Eastern District of Virginia issued several orders and a seizure warrant compelling a third-party
24 encrypted email service provider, Lavabit, to turn over its encryption keys, pursuant to novel
25 interpretations of the Pen Register Statute and the Stored Communications Act. See *In re Under*
26 *Seal (Lavabit)*, 749 F.3d 276, 282-84 (4th Cir. 2014). Giving the FBI Lavabit's encryption keys
27 would have enabled investigators to access the private data of all Lavabit users, not just the
28 target of the investigation. Lavabit shut down rather than provide investigators with a digital

1 copy of its encryption key. However, the public does not know whether this or other courts have
2 ordered other providers to give their encryption keys to investigators under seal.

3 **C. Forcing Security Modifications to Smartphones Under the All Writs Act**

4 Courts have been secretly obligating Apple, Google, and possibly other companies to
5 decrypt private data on iPhones or Android phones pursuant to the All Writs Act, 28 U.S.C. §
6 1651(a), or AWA. Prior to passage of the Pen/Trap Act in 1986, the Supreme Court had
7 interpreted the AWA to give law enforcement agents the authority to demand technical
8 assistance in implementing a court-issued order for phone call data (*e.g.*, numbers dialed). *See,*
9 *e.g.*, *N.Y. Tel. Co.*, 434 U.S. at 171-75 (AWA authorized district court’s order compelling phone
10 company to assist in implementing pen register order). After the passage of the Pen/Trap Act,
11 which explicitly authorizes some technical assistance in installing a pen register or trap and trace
12 device to obtain call data, it appears that the government ceased using the AWA for technical
13 assistance.

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

21 A year later, another magistrate in the Eastern District of New York unsealed a similar
22 AWA application (which he ultimately denied), this time directed at iPhone manufacturer Apple.
23 *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued By this*
24 *Court*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (denying AWA application).¹¹ During that case, the

25 _____
26 ¹¹ For news coverage of the case, see, *e.g.*, Ellen Nakashima, *Judge Rules in Favor of Apple in*
27 *Key Case Involving a Locked iPhone*, Wash. Post (Feb. 29, 2016),
28 https://www.washingtonpost.com/world/national-security/judge-rules-in-favor-of-apple-in-key-case-involving-a-locked-iphone/2016/02/29/fa76783e-db3d-11e5-925f-1d10062cc82d_story.html; Ellen Nakashima, *With Court Order, Federal Judge Seeks to Fuel*

(Footnote Continued on Next Page.)

1 public learned that courts have granted at least 70 other government applications for AWA
2 orders compelling manufacturers to bypass smartphone passcodes in sealed proceedings.¹²

3 Most recently, in mid-February of this year, a magistrate in the Central District of
4 California issued an AWA order compelling Apple to write new software code to let law
5 enforcement attempt to “brute force” guess the password protecting an encrypted iPhone used by
6 one of the San Bernardino terrorists. *In the Matter of the Search of an Apple iPhone Seized*
7 *During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate*
8 *5KGD203*, No. 15-mj-0451, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016) (*In re*
9 *iPhone*).¹³ Although the FBI subsequently dropped the matter after accessing the phone data by
10 other means, that case has sparked discussion of whether compelling such access is within the
11 courts’ authority to mandate.¹⁴

12 III. Sealed Proceedings Deprive the Public of Information about Judicial 13 Interpretations of Technical-Assistance Provisions

14 In the few cases where the issue has become public, Americans have hotly debated
15 whether judicial power can properly be used to mandate private entities to assist with
16 government investigations by unlocking phones, writing new software, revealing private

17 (Footnote Continued from Previous Page.)

18 *Debate about Data Encryption*, Wash. Post (Oct. 10, 2015),
19 [https://www.washingtonpost.com/world/national-security/federal-judge-stokes-debate-about-](https://www.washingtonpost.com/world/national-security/federal-judge-stokes-debate-about-data-encryption/2015/10/10/c75da20e-6f6f-11e5-9bfe-e59f5e244f92_story.html)
20 [data-encryption/2015/10/10/c75da20e-6f6f-11e5-9bfe-e59f5e244f92_story.html](https://www.washingtonpost.com/world/national-security/federal-judge-stokes-debate-about-data-encryption/2015/10/10/c75da20e-6f6f-11e5-9bfe-e59f5e244f92_story.html). After the
21 application was denied, the FBI obtained the defendant’s cooperation to unlock the phone.
22 Devlin Barrett, *Federal Prosecutors Drop Court Case to Force Apple to Unlock iPhone*, Wall St.
23 J. (Apr. 22, 2016), [http://www.wsj.com/articles/federal-prosecutors-drop-court-case-to-force-](http://www.wsj.com/articles/federal-prosecutors-drop-court-case-to-force-apple-to-unlock-iphone-1461377642)
24 [apple-to-unlock-iphone-1461377642](http://www.wsj.com/articles/federal-prosecutors-drop-court-case-to-force-apple-to-unlock-iphone-1461377642).

25 ¹² Nicole Hong, *Judge Questions Legal Authority to Force Apple to Unlock iPhones*, Wall St. J.
26 (Oct. 26, 2015), [http://blogs.wsj.com/law/2015/10/26/judge-questions-legal-authority-to-force-](http://blogs.wsj.com/law/2015/10/26/judge-questions-legal-authority-to-force-apple-to-unlock-iphones/)
27 [apple-to-unlock-iphones/](http://blogs.wsj.com/law/2015/10/26/judge-questions-legal-authority-to-force-apple-to-unlock-iphones/).

28 ¹³ For news coverage, see, e.g., Eric Lichtblau and Katie Benner, *Apple Fights Order to Unlock*
San Bernardino Gunman’s iPhone, N.Y. Times (Feb. 17, 2016),
<https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html>.
¹⁴ See, e.g., Katie Benner and Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*,
N.Y. Times (Mar. 28, 2016), [https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-](https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html)
justice-department-case.html; Katie Benner, Eric Lichtblau, and Nick Wingfield, *Apple Goes to*
Court, and F.B.I. Presses Congress to Settle iPhone Privacy Fight, N.Y. Times (Feb. 25, 2016),
[https://www.nytimes.com/2016/02/26/technology/apple-unlock-iphone-fbi-san-bernardino-](https://www.nytimes.com/2016/02/26/technology/apple-unlock-iphone-fbi-san-bernardino-brief.html)
brief.html (reporting that both the FBI and Apple wanted Congress, not the courts, to decide
iPhone encryption issue).

1 encryption keys, or remotely turning on microphones or cameras in consumer goods.

2 Most surveillance orders are sealed, however. Therefore, the public does not have a
3 strong understanding of what technical assistance courts may order private entities to provide to
4 law enforcement. There are at least 70 cases, many under seal, in which courts have mandated
5 that Apple and Google unlock mobile phones—and potentially many more.¹⁵ The Lavabit district
6 court may not be the only court to have ordered companies to turn over private encryption keys
7 to law enforcement based on novel interpretations of law. Courts today may be granting orders
8 forcing private companies to turn on microphones or cameras in cars, laptops, mobile phones,
9 smart TVs, or other audio- and video-enabled Internet-connected devices in order to conduct
10 wiretapping or visual surveillance.

11 This pervasive sealing cripples public discussion of whether these judicial orders are
12 lawful and appropriate.

13 **IV. It Is in the Public Interest That Judicial Documents Mandating Technical** 14 **Assistance Eventually Be Unsealed**

15 Public disclosure serves an important role in exploring the risks and rewards of technical
16 assistance. Technical-assistance demands can create privacy and security risks that United States
17 Attorneys and courts sitting *ex parte* might not fully understand. In the *Lavabit* case, for
18 example, the FBI's demand for the company's encryption keys would expose the private data of
19 all Lavabit users. In the San Bernardino dispute between Apple and the FBI, security experts
20 opposed the government's AWA application on the grounds that it would endanger public
21 safety.¹⁶ The assistance measure could escape Apple's control through theft, embezzlement, or
22 order of another court, including a foreign government, and be misused by criminals and
23

24 ¹⁵ See *supra* n.12; see also All Writs Act Orders for Assistance from Tech Companies, American
25 Civil Liberties Union, <https://www.aclu.org/map/all-writs-act-orders-assistance-tech-companies>
26 (map of United States showing where applications have been filed for AWA orders to Apple and
27 Google).

28 ¹⁶ See Br. of *Amici Curiae* iPhone Security and Applied Cryptography Experts in Support of
Apple Inc.'s Mot. to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and
Opposition to Gov't's Mot. to Compel Assistance, *In re iPhone*, No. 16-cm-00010 (C.D. Cal.
Mar. 4, 2016).

1 oppressive governments to extract sensitive personal and business data from seized, lost, or
2 stolen iPhones. Before purchasing consumer goods with microphones or video cameras in our
3 homes, the public should know whether law enforcement can use the Wiretap Act or the AWA to
4 repurpose those devices for wiretapping or visual surveillance in the most intimate rooms of our
5 homes.

6 What technical assistance does U.S. law require people to provide to law enforcement?
7 Are courts issuing technical-assistance orders appropriately and wisely? The public does not and
8 cannot know the answers to these questions unless courts unseal the applications, opinions, and
9 orders. For this reason, this District “has a policy of providing to the public full access to
10 documents filed with the Court.” N.D. Cal. Crim. L.R. 56-1 commentary. Where sealing is
11 appropriate, the correct way to handle the matter is to ensure that “a redacted copy is filed and
12 available for public review with the minimum redactions necessary to protect sealable
13 information.” *Id.*

14 ARGUMENT

15 **I. The Public Has a Right of Access to Judicial Documents Concerning Technical-** 16 **Assistance Applications and Orders**

17 **A. Legal Standards for Public Right to Access Judicial Documents**

18 Petitioners and the public have the right to access the judicial proceedings and records
19 that are the subject of this Petition. The United States “has a long history of distrust for secret
20 proceedings,” which “are the exception rather than the rule in our courts.” *United States v. Index*
21 *Newspapers LLC*, 766 F.3d 1072, 1084 (9th Cir. 2014) (citations omitted). The documents we
22 request that the Court unseal are subject to qualified rights of access to judicial proceedings
23 under the First Amendment and under the common law. *Press-Enter. II*, 478 U.S. at 8-9 (First
24 Amendment); *Nixon*, 435 U.S. at 597 (footnotes omitted) (common law).

25 *1. First Amendment Right of Access*

26 The First Amendment provides a right of access to criminal proceedings. *Richmond*
27 *Newspapers, Inc. v. Virginia*, 448 U.S. 555, 580-81 (1980); *Associated Press v. U.S. Dist. Court*,
28 705 F.2d 1143, 1145 (9th Cir. 1983) (pre-trial documents); *In re Special Proceedings*, 842 F.

1 Supp. 2d 232, 239 (D.D.C. 2012) (collecting cases). Pursuant to the First Amendment, the public
2 right of access to court proceedings is presumed. *See Oregonian Publ'g Co. v. U.S. Dist. Court*,
3 920 F.2d 1462, 1465 (9th Cir. 1990) (citing *Press-Enter. Co. v. Superior Court*, 464 U.S. 501,
4 510 (1984) (*Press-Enterprise I*)). This right of access “ensure[s] that th[e] constitutionally
5 protected ‘discussion of governmental affairs’ is an informed one.” *Globe Newspaper Co. v.*
6 *Superior Court*, 456 U.S. 596, 604-05 (1982) (quotation omitted). The right is based on the
7 history of open criminal trials in the American and English legal systems and on policy grounds
8 including the potential for public scrutiny to “enhance[] the quality and safeguard[] the integrity
9 of the factfinding process,” the “appearance of fairness,” and the opportunity for “the public to
10 participate in and serve as a check upon the judicial process.” *Id.* at 605-06 (footnotes omitted).

11 There is a two-part test for determining whether a First Amendment right of access
12 applies to a particular judicial proceeding. The court must ask 1) “whether the place and process
13 have historically been open to the press and general public,” and 2) “whether public access plays
14 a significant positive role in the functioning of the particular process in question.” *Press-Enter.*
15 *II*, 478 U.S. at 8-9 (citation omitted). This test is commonly referred to as the “experience and
16 logic” test. *See, e.g., id.* at 9. The same test applies to the disclosure of “documents generated as
17 part of a judicial proceeding.” *Times Mirror Co. v. United States*, 873 F.2d 1210, 1213 n.4 (9th
18 Cir. 1989) (citations omitted). However, in the Ninth Circuit, “logic alone, even without
19 experience, may be enough to establish the right” of access. *In re Copley Press, Inc.*, 518 F.3d
20 1022, 1026 (9th Cir. 2008) (citations omitted).

21 Once a petitioner has established a First Amendment right of access, the bar for
22 overcoming the right is demanding. A First Amendment right of access can be denied only by
23 proof of a “compelling governmental interest” and proof that the denial is “narrowly tailored to
24 serve that interest,” *Globe Newspaper*, 457 U.S. at 606-07, “based on [specific] findings that
25 closure is essential to preserve higher values.” *Press-Enter. I*, 464 U.S. at 510; *Oregonian Publ'g*
26 *Co.*, 920 F.2d at 1465. There must be a “substantial probability” of harm to the overriding
27 interest; even a “reasonable likelihood” is insufficient. *Press-Enter. II*, 478 U.S. at 14.

1 2. *Common-Law Right of Access*

2 The public records to which the common-law right of access applies comprise an even
3 broader set than those covered by the First Amendment right of access. Only “a narrow range of
4 documents” is exempt from the common-law right of public access, *Kamakana v. City & Cnty. of*
5 *Honolulu*, 447 F.3d 1172, 1178 (9th Cir. 2006)—those which have “traditionally been kept
6 secret for important policy reasons.” *Times Mirror Co.*, 873 F.2d at 1219.

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

19 In sum, judicial records are generally subject to the public’s right of access.

20 **B. Petitioners’ Right of Access to Each Category of Documents**

21 1. *Docket Sheets*

22 Public docket sheets play a key role in the public’s relationship with the courts. The
23 docket sheet notifies the public of activity in a matter. *United States v. Ochoa-Vasquez*, 428 F.3d
24 1015, 1029 n.15 (11th Cir. 2005) (citation omitted). Docket sheets provide an index to judicial
25 proceedings and documents, and endow the public and press with the capacity to exercise their
26 rights of access guaranteed by the First Amendment. *Hartford Courant Co. v. Pellegrino*, 380
27 F.3d 83, 93 (2d Cir. 2004). Secrecy, by contrast, erodes the legitimacy of the institution of the
28 courts. Maintaining “a two-tier system, open and closed,” threatens public “[c]onfidence in the

1 accuracy of [the court’s] records ..., ... the authority of its rulings and the respect due its
2 judgments.” *CBS, Inc. v. U.S. Dist. Ct.*, 765 F.2d 823, 826 (9th Cir. 1985) (Kennedy, J.). In sum,
3 sealed docket sheets frustrate the ability of the public and the appellate courts to oversee the
4 judicial process. *Pellegrino*, 380 F.3d at 94.

5 In recognition of docket sheets’ vital role, the United States has a “centuries-long history
6 of public access to dockets.” *United States v. Mendoza*, 698 F.3d 1303, 1304 (10th Cir. 2012).
7 “Logic supports this judgment of history.” *Pellegrino*, 380 F.3d at 95. Accordingly, access to
8 dockets meets the First Amendment “experience and logic” test. *Id.* at 96.

9 For a district court to maintain a dual-docketing system, one open, one sealed, is “facially
10 unconstitutional.” *Ochoa-Vasquez*, 428 F.3d at 1029 (citing *United States v. Valenti*, 987 F.2d
11 708, 715 (11th Cir. 1993)). It “violates the public and press’s First Amendment right of access to
12 criminal proceedings.” *Co. Doe v. Public Citizen*, 749 F.3d 246, 268 (4th Cir. 2014) (citing
13 *Valenti*, 987 F.2d at 715). A secret docketing system “can effectively preclude the public and the
14 press from seeking to exercise their constitutional right of access” to court records. *Valenti*, 987
15 F.2d at 715. In short, a “district court ... cannot employ ... secret docketing procedures.” *Ochoa-*
16 *Vasquez*, 428 F.3d at 1030. *See generally In re Sealed Case*, 199 F.3d 522, 525 (D.C. Cir. 2000)
17 (collecting federal appeals court cases requiring public docketing in judicial proceedings other
18 than grand jury matters); *Media Gen. Operations, Inc. v. Buchanan*, 417 F.3d 424, 437 (4th Cir.
19 2005) (clerk of court must maintain a public docket of search warrant proceedings, once warrant
20 has been returned).

21 Yet this District’s docketing procedures are worse. The Clerk of this Court does not
22 docket the Court’s surveillance and related technical-assistance matters at all, much less make
23 those dockets publicly available. *See Pfefferkorn Decl.* ¶ 3. Without docket sheets, members of
24 the public do not have many options for exercising First Amendment rights. We can move, as
25 Petitioners have done, for the Court to review its own records, docket them, and unseal them, or
26 we can remain in the dark. What we cannot do is review the Court’s dockets to help identify
27 relevant cases or to petition to unseal in those particular matters only.

28 Failing to publicly docket surveillance-related matters means the public does not know

1 whether, when, how often, to whom, or on what legal basis the government collects private
2 information. Nor do we know how often investigators demand third-party technical assistance,
3 whether the third parties get an opportunity to be heard, what kind of technical assistance is
4 compelled or denied, and for what reasons.

5 “[M]aking court files accessible” is particularly appropriate where, as here, the
6 government is a party to the matter: “in such circumstances, the public’s right to know what the
7 executive branch is about coalesces with the concomitant right of the citizenry to appraise the
8 judicial branch.” *Fed. Trade Comm’n v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404, 410 (1st Cir.
9 1987) (*FTC*); *Doe*, 749 F.3d at 271 (“the public has a strong interest in monitoring not only
10 functions of the courts but also the positions that its elected officials and government agencies
11 take in litigation” (citing *FTC*)). In the Lavabit and Apple matters, the law enforcement arm of
12 the Executive has asserted a novel and expansive right to enlist third parties’ technical assistance
13 in police investigations. Petitioners and the public have a strong interest in learning whether the
14 government has advanced that argument before this Court. But the public cannot know that, and
15 thus cannot play an informed role in the contentious debate over the topic of compelled third-
16 party technical assistance, if there are no docket sheets the public can access that reflect such
17 requests.

18 Even if this Court declines to unseal some or all of the underlying materials, those
19 records nevertheless should be docketed and the docket sheets made public. The Fourth Circuit
20 has declined to require public docketing of a pre-indictment § 2703(d) order, and noted that no
21 court had yet required other investigative tools such as pen registers, and wiretaps to be publicly
22 docketed. *United States v. Appelbaum*, 707 F.3d 283, 295 (4th Cir. 2013). Petitioners, however,
23 are asking for *post*-investigative materials. While keeping surveillance proceedings secret during
24 the pendency of an investigation can make sense, eventually those matters must be publicly
25 docketed, in order to provide notice and “an opportunity ... to voice objections to the denial of
26 access.” *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 65 (4th Cir. 1989). This is the minimum
27
28

1 necessary to ensure electronic surveillance decisions are both known and accountable to the
2 public and to other judges.¹⁷

3 There is no compelling countervailing reason not to create and unseal docket sheets for
4 investigations that have concluded. *See In re State-Record Co., Inc.*, 917 F.2d 124, 129 (4th Cir.
5 1990) (“we can not understand how the docket entry sheet could be prejudicial”). Petitioners thus
6 respectfully ask the Court to docket all matters implicated in its Request and unseal their docket
7 sheets.

8 2. *Search and Seizure Warrants, Applications, and Supporting Materials*

9 Petitioners seek access to applications and supporting materials seeking to compel third-
10 party technical assistance with the execution of search and/or seizure warrants to access a device
11 or information that is encrypted, passcode-, passphrase-, or password-protected, or otherwise
12 “locked.”

13 This Court has not decided whether, once the investigation is over, the First Amendment
14 right attaches to search warrant materials. *See Custer Battlefield Museum*, 658 F.3d at 1196
15 (reserving the question of whether the First Amendment right covers warrant materials post-
16 investigation but finding a common-law right). The Court should find, as other courts have done,
17 that there is a First Amendment right of access to search warrant materials once an investigation
18 has concluded. *United States v. Loughner*, 769 F. Supp. 2d 1188, 1195 (D. Ariz. 2011). In
19 *Loughner*, a high-profile case involving the mass shooter who killed a federal judge and gravely
20 wounded a congresswoman, the district court reviewed precedent regarding the First Amendment
21 and access to search warrant materials. *Id.* at 1190-1193. The court concluded that while there
22 were cases both for and against access, the more recent cases and the “clear trend” over the past
23 30 years support finding a constitutional right of access. *Id.* at 1193. Thus, the court found that
24 the “experience” prong of the First Amendment test was met. *Id.* The court also found that the

25
26 ¹⁷ Indeed, at least one other federal district court, which does docket these materials, is currently
27 considering how to proceed with unsealing the docket sheets for surveillance matters that no
28 longer have any need for secrecy, as well as the underlying applications, orders, and related
records. *See In re Application of Jason Leopold to Unseal Certain Elec. Surveillance*
Applications and Orders, No. 13-mc-00712 (D.D.C. filed July 16, 2013).

1 logic prong was met. “[E]ven after the fact,” the court reasoned, public scrutiny of the warrant
2 process can “further the public’s interest in understanding the justice system” and “how well it
3 works,” and “may also serve to deter unreasonable warrant practices, either by the police or the
4 courts.” *Id.* at 1193-94 (citations omitted). Therefore, the court found a qualified First
5 Amendment right of access to search warrant materials once the investigation has concluded and
6 a final indictment has issued. *Id.* at 1193 (emphasizing “the critical importance of the public’s
7 right to be fully informed in high profile case[s] like this one, as well as the need for robust
8 protection of a fre[e] press”).

9 Based on *Loughner*’s reasoning and the cases on which the ruling relies, Petitioners have
10 a First Amendment right to obtain search warrant materials. The materials to which the public
11 has a First Amendment right include “search warrants, warrant applications, supporting
12 affidavits, court orders, and returns for [the] warrants.” *In re N.Y. Times Co.*, 585 F. Supp. 2d 83,
13 86 (D.D.C. 2008). The experience of courts over the past 30 years demonstrates a clear trend
14 toward openness. Further, logic dictates that the public have access to judicial materials that can
15 inform an impactful and robust public debate over the proper scope of technical assistance.

16 Granting Petitioners access is appropriate here because we are seeking post-investigatory
17 materials. The First Amendment right of access to search warrant-related materials can be
18 overcome if the materials are part of an ongoing investigation that disclosure would compromise.
19 *See In re Search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d 569, 574 (8th
20 Cir. 1988) (ongoing investigation overcame First Amendment right of access to search warrant
21 materials). However, there is no such concern here.

22 Furthermore, any specific reputational, due process, or privacy interests that might be
23 harmed by disclosure of warrant materials can be adequately protected through redaction. It is
24 technical-assistance orders to third parties, not the individuals under investigation, their
25 associates, or their personal activities, that Petitioners seek to uncover. *See In re WP Co. LLC*,
26 No. 16-mc-351, 2016 U.S. Dist. LEXIS 109635, at *44-46 (D.D.C. Aug. 18, 2016) (denying
27 request to unseal and redact search warrant materials because case of businessman involved in
28 campaign-finance and sex scandals had already attracted a high “degree of media scrutiny” and

1 “limited redactions would invite conjecture and speculation” about private individuals).

2 In addition to a First Amendment right, Petitioners also have a common-law right to
3 access post-investigation warrant materials, because these “have historically been available to
4 the public.” *Custer Battlefield Museum*, 658 F.3d at 1193 (quoting *In re N.Y. Times Co.*, 585 F.
5 Supp. 2d at 88). Warrant applications generally may not “be sealed indefinitely after the
6 investigation comes to a close,” and should be sealed “only in exceptional cases.” *In re Sealing*
7 *& Non-Disclosure*, 562 F. Supp. 2d 876, 892 (S.D. Tex. 2008) (citation omitted). There is good
8 cause to unseal search warrant materials because “[s]ociety has an understandable interest ... in
9 law enforcement systems and how well they work. The public has legitimate concerns about
10 methods and techniques of police investigation....” *In re Application and Affidavit for a Search*
11 *Warrant*, 923 F.2d 324, 331 (4th Cir. 1991). The public interest in government demands for
12 technical assistance in executing search warrants on encrypted information requires unsealing of
13 the requested materials. No “sufficiently compelling reasons” exist to justify continued sealing.
14 *Foltz*, 331 F.3d at 1135 (citation omitted).

15 3. *Technical-Assistance Orders under the SCA*

16 Petitioners request access to sealed applications (whether styled as applications, motions,
17 or otherwise), materials filed in support or opposition thereto, and orders (whether granting or
18 denying the applications) under 18 U.S.C. § 2703 requiring or denying a third party’s technical
19 assistance in disclosing customer communications or records to law enforcement.

20 The SCA establishes rules governing service providers’ voluntary and compelled
21 disclosure of users’ online information to law enforcement and private parties. Passed in 1986,
22 the statute ensures Fourth Amendment-like protections for some electronic communications
23 while establishing other privacy safeguards for related information. 18 U.S.C. § 2703.

24 Under the “experience and logic” test, Petitioners have a First Amendment right of access
25 to these SCA documents. The SCA was passed only 30 years ago, meaning there is no historical
26 tradition of access to SCA documents. *See Copley Press*, 518 F.3d at 1027 (“no historical
27 experience of public access” to type of hearing that had been invented 25 years previously
28 (citations omitted)). However, in this circuit, the “logic” prong alone can suffice to establish a

1 right of access if “public scrutiny” would “benefit” the proceedings. *Id.* at 1026 (citing *Seattle*
2 *Times Co. v. U.S. Dist. Court*, 845 F.2d 1513, 1516, 1517 (9th Cir. 1988)).

3 Under the “logic” prong, Petitioners are entitled to access these materials. Section 2703
4 orders, like any orders issued by a court, are judicial records. *Appelbaum*, 707 F.3d at 290-91.
5 They serve a similar role as search warrants do, which is to ensure judicial oversight of
6 information collection during an investigation. There is no logical reason to treat them differently
7 from search warrants and related materials once the investigation has concluded. Therefore, SCA
8 orders and related documents should be treated like post-indictment search warrant materials, for
9 which there is a First Amendment right of access. *Loughner*, 769 F. Supp. 2d at 1193-94
10 (applying “logic” prong after holding “experience” prong met).

11 The Fourth Circuit’s denial in *Appelbaum* of a First Amendment right of access to
12 Section 2703(d) materials is distinguishable. There, the court analogized *pre-indictment* Section
13 2703(d) orders, materials, and proceedings to *pre-indictment* search warrants and proceedings (as
14 well as grand jury proceedings), which are not open to public scrutiny. 707 F.3d at 291-92 & n.9.
15 The logic prong failed because “secrecy is necessary for the proper functioning of the criminal
16 investigations at this § 2703(d) phase, [so] openness will frustrate the government’s operations.”
17 *Id.* at 292 (footnote omitted). The court also pointed to the statute’s delayed-notice and non-
18 disclosure provisions as factors favoring sealing. *Id.* at 292 n.11.

19 However, the *Appelbaum* court did not consider whether there is a First Amendment right
20 of access to Section 2703 materials at the post-investigation phase. As with search warrant
21 materials, opening Section 2703 materials to public scrutiny *post-investigation* serves a number
22 of important public interests without any negative impact on government operations. These
23 interests include “knowing that proper procedures have been followed”; “understanding the
24 justice system”; “deter[ring] unreasonable [surveillance] practices, either by the police or the
25 courts”; and “ensur[ing] that judges are not merely serving as a rubber stamp for the police.”
26 *Loughner*, 769 F. Supp. 2d at 1194 (citations and internal quotation marks omitted). All of these
27 interests are at stake equally in Section 2703 orders as in search warrants—perhaps even more
28 so. Since Section 2703 sometimes requires a lower evidentiary showing than the probable-cause

1 warrant standard, public scrutiny is arguably even more necessary to ensure that courts are not
2 giving too much power to police under this less-demanding bar. *See United States v. Espudo*, 954
3 F. Supp. 2d 1029, 1033 (S.D. Cal. 2013) (Section 2703(d)'s “specific and articulable facts’
4 standard [for issuance of a court order for disclosure of user’s records] is a significantly lower
5 legal hurdle than probable cause.” (citation omitted)).

6 In sum, there is a First Amendment right of access to Section 2703 orders and related
7 materials, and because they do not implicate any ongoing investigations, there is no compelling
8 government interest not to unseal them.

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

14 The common-law presumption of access outweighs any countervailing interests in this
15 case. While the *Appelbaum* court held that the government’s “significant countervailing interest”
16 in not hampering ongoing investigations or tipping off targets outweighed the public’s
17 presumption of access, 707 F.3d at 292-94, that countervailing interest does not apply to
18 Petitioners’ request, which excludes materials from ongoing investigations.

19 4. *Technical-Assistance Orders under the Pen/Trap Act*

20 Next, Petitioners seek the unsealing of sealed applications (whether styled as
21 applications, motions, or otherwise), materials filed in support or opposition thereto, and orders
22 (whether granting or denying the applications) under 18 U.S.C. §§ 3123(b)(2) or 3124(a) or (b),
23 requiring or denying a third party to assist law enforcement in accessing communications data.

24 The Pen/Trap Act establishes rules governing telephone companies’ and Internet service
25 providers’ compelled collection and disclosure of users’ dialing, routing, signaling, and
26 addressing information to law enforcement. Under the First Amendment experience and logic
27 test, there is a constitutional right of access to post-investigation Pen/Trap materials.

28 Pen register orders serve the same purpose as search warrants in the judicial system—

1 they authorize government information collection and can require third-party technical
2 assistance. As the court said in *Loughner*, there are sound reasons for public disclosure of such
3 documents. Society has a valid and understandable interest in the law enforcement system and
4 how well it works. Permitting inspection of pen register documents once an investigation has
5 concluded, no less than search warrants, will further public understanding of the law and “will
6 enable the public to evaluate for itself whether the government’s [demands for technical
7 assistance] went too far—or did not go far enough.” *Loughner*, 769 F. Supp. 2d at 1994 (internal
8 citation and quotation marks omitted). In short, the public’s interests in these documents track
9 those at stake in post-investigation SCA materials. *See supra* at 18-20.

10 The public also has a common-law right of access to post-investigation pen/trap
11 materials. *In re Sealing & Non-Disclosure*, 562 F. Supp. 2d at 894, 896. This Court has
12 discretion to unseal these materials. Pen/trap orders must be sealed “until otherwise ordered by
13 the court.” 18 U.S.C. § 3123(d)(1). “How long a pen/trap order should be sealed, and whether
14 sealing should continue beyond the life of the pen register itself, is left to the sound discretion of
15 the court.” *In re Sealing & Non-Disclosure*, 562 F. Supp. 2d at 879. The Court should exercise
16 its discretion and unseal the requested pen/trap materials because indefinite non-disclosure
17 “deprive[s] the law-abiding public of significant data about the frequency of compelled
18 Government access to individual e-mail and phone records.” *Id.* at 886. The public interest in
19 unsealing technical-assistance pen/trap materials is particularly acute here given the current
20 debate over whether it is appropriate to compel service providers to disclose their private
21 encryption keys, and thereby put all their customers’ data at risk, as the district court had ordered
22 in *Lavabit*. *See Lavabit*, 749 F.3d at 280-82.

23 No competing consideration merits continued sealing of post-investigation pen/trap
24 materials, under either a First Amendment or common-law analysis. As with post-investigation
25 SCA materials, disclosure does not jeopardize current or future investigations, and any sensitive
26 information contained therein can be redacted.

27 5. *Technical-Assistance Orders under the AWA*

28 Petitioners seek to unseal the U.S. government’s applications under the All Writs Act

1 (“AWA”), 28 U.S.C. § 1651(a), that seek to compel a third party to assist the government in
2 accessing an individual’s device or information. Petitioners also seek to unseal all materials filed
3 in support of or opposition to these applications (such as briefs, affidavits, and proposed orders),
4 and all orders by the Court relating to the applications.

5 The public has a First Amendment right of access to AWA orders and supporting
6 materials under the experience and logic test. Under the experience prong, “there is a venerable
7 tradition of public access to court orders.” *United States v. Ressam*, 221 F. Supp. 2d 1252, 1262
8 (W.D. Wash. 2002) (qualified First Amendment right of access attached to protective orders,
9 which court ordered made publicly available with classified information redacted). *See also*
10 *Pepsico, Inc. v. Redmond*, 46 F.3d 29, 31 (7th Cir. 1995) (Easterbrook, J., in chambers)
11 (“Opinions are not the litigants’ property. They belong to the public, which underwrites the
12 judicial system that produces them.” (citations omitted)). This rule is so well-established that it
13 may come as no surprise that no federal court has apparently had occasion to apply the
14 “experience and logic” analysis to AWA orders (which may issue in a variety of circumstances)
15 in particular. It should be uncontroversial that the “venerable tradition” of access encompasses
16 court orders issued under the ancient¹⁸ AWA, even though its use to compel technical assistance
17 is relatively new. *See N.Y. Tel.*, 434 U.S. at 174-75 (holding in 1977 that AWA was properly
18 used to compel installation of pen register). The “experience” prong thus is easily met.

19 The logic prong also supports First Amendment access. Courts cannot issue stand-alone
20 AWA orders. *United States v. Denedo*, 556 U.S. 904, 911 (2009) (“[a]s the text of the All Writs
21 Act recognizes, a court’s power to issue any form of relief ... is contingent on that court’s
22 subject-matter jurisdiction over the case”). Issuance of an order under the AWA requires “the
23 existence of a previously-issued court order or warrant”; otherwise, “no jurisdiction exists.” *In re*
24 *Application of the United States*, 128 F. Supp. 3d 478, 483 (D.P.R. 2015). Because the AWA
25 orders Petitioners seek must have issued in furtherance of an underlying warrant or surveillance
26

27 ¹⁸ The All Writs Act was originally enacted as part of the Judiciary Act of 1789, 1 Stat. 73, § 14
28 (Sept. 24, 1789).

1 order, and since there is a right of access to those underlying documents, it follows logically that
2 there is a right of public access to the related AWA orders as well. *See supra* at 16-18; *Loughner*,
3 769 F. Supp. 2d at 1194 (listing interests).

4 The common law also entitles the public to access the requested AWA materials. The
5 common-law presumption of access attaches to AWA materials because they qualify as “judicial
6 records.” The court’s orders and opinions are indisputably judicial records subject to the public’s
7 right of access. *See Pepsico*, 46 F.3d at 31 (courts’ opinions “belong to the public” (citations
8 omitted)); *Glaxo Grp. Ltd. v. Leavitt*, 481 F. Supp. 2d 437, 438 (D. Md. 2007) (refusing to seal
9 publicly-issued opinion because “fundamentally, ... this court is a public institution doing the
10 public’s business. The public interest in an accountable judiciary generally demands that the
11 reasons for a judgment be exposed to public scrutiny.” (citations and internal quotation marks
12 omitted)).

13 The government’s applications for AWA orders and supporting (or opposing) materials
14 are also “judicial records.” *See Custer Battlefield Museum*, 658 F.3d at 1193 (deciding to “treat[]
15 search warrant affidavits as judicial records”). Because, as said, AWA orders must be premised
16 on an underlying warrant or order, it follows that AWA applications and supporting materials
17 are, like the original warrant affidavits, also “judicial records.” *Cf. United States v. Tillman*, No.
18 07-cr-1209, 2009 U.S. Dist. LEXIS 35400, at *4 (S.D.N.Y. Apr. 6, 2009) (court order,
19 government’s application for disclosure of defendant’s tax returns, and supporting papers were
20 “judicial documents”).

21 Therefore, a “strong presumption in favor of access” attaches to the requested materials.
22 *Foltz*, 331 F.3d at 1135 (citation omitted). No countervailing interests overcome the public right
23 of access to AWA materials. Petitioners’ request excludes ongoing investigations, so disclosure
24 will not “jeopardize an important law enforcement or security interest in this particular instance.”
25 *Tillman*, 2009 U.S. Dist. LEXIS 35400, at *11-12 (“general proposition” that government’s
26 applications for court orders may sometimes contain sensitive details of ongoing investigations
27 does not “justify a blanket rule of permanent non-disclosure”). Accordingly, the AWA materials
28 should be unsealed.

1 6. *Technical-Assistance Orders under the Wiretap Act*

2 Petitioners also seek to unseal any technical-assistance materials filed pursuant to the
3 Wiretap Act, 18 U.S.C. §§ 2511(2)(a)(ii), 2518(4).¹⁹

4 There is a statutory scheme for sealing and unsealing wiretap applications and orders
5 under 18 U.S.C. § 2518(8)(b), which provides that “[a]pplications made and orders granted
6 under this chapter”—*i.e.*, applications for and orders granting permission to engage in
7 wiretapping—“shall be sealed by the judge [and] disclosed only upon a showing of good cause
8 before a judge of competent jurisdiction.” 18 U.S.C. § 2518(8)(b). In sealing these materials, the
9 statute seeks to protect the integrity of ongoing investigations, as well as the privacy interests of
10 innocent third parties and of defendants. *In re N.Y. Times Co.*, 828 F.2d 110, 116 (2d Cir. 1987)
11 (*NYT I*).

12 Nevertheless, Petitioners have an independent First Amendment right of access to wiretap
13 materials, including technical-assistance orders, notwithstanding the statutory scheme for
14 unsealing. “[A] statute cannot override a constitutional right” of access. *NYT I*, 828 F.2d at 115
15 (footnote omitted). Logic supports a First Amendment right of access here. Unsealing would
16 “play[] a significant positive role in the functioning of” wiretap technical-assistance orders.
17 *Press-Enter. II*, 478 U.S. at 8 (citation omitted). It would enable the public to understand whether
18 the Wiretap Act allows the government to force private parties to help it access encrypted
19 communications at a time of contentious public debate over the propriety of such compulsion. It
20 would also help the public understand whether the law allows investigators to turn on the
21 cameras or microphones in consumer goods like televisions, smartphones, and computerized
22 home assistants to conduct surveillance.

23 While there is no “Ninth Circuit precedent addressing ... how [the Wiretap Act’s] sealing
24 provisions interact with the public’s First Amendment right of access,” *United States v. Chow*,
25 No. 14-cr-00196, 2015 U.S. Dist. LEXIS 114802, at *12 (N.D. Cal. Aug. 28, 2015), the Second
26 Circuit has rejected a First Amendment right to access Wiretap Act materials. *In re N.Y. Times*

27 ¹⁹ For clarity, Petitioners seek disclosure of any sealed orders relating to technical assistance
28 under the Wiretap Act, whether or not they grant the government’s application.

1 Co., 577 F.3d 401, 409-11 (2d Cir. 2009) (*NYT II*). That court concluded that the Act’s
2 “confidentiality and privacy” interests were more compelling than transparency. *Id.* at 410.

3 However, the Second Circuit did not consider whether there was a First Amendment right
4 to access technical-assistance applications and orders, but only wiretap applications. *NYT II*, 577
5 F.3d at 404. Logic is in favor of unsealing these materials. The Wiretap Act seals materials to
6 protect the confidentiality of ongoing criminal investigations and the rights of individual citizens
7 to maintain their privacy. *Id.* at 409. Disclosure of post-investigation technical-assistance
8 applications and orders need not implicate the confidentiality and privacy interests codified in
9 the Act. The investigations are finished, and Petitioners do not seek the disclosure of any
10 information about the wiretaps’ targets, their interlocutors, or their communications—the
11 information that sealing is designed to protect. These matters can continue to be protected via
12 redaction rather than indefinite sealing, which undermines the legitimacy of judicial process.²⁰ In
13 sum, post-investigation wiretap technical-assistance orders should be unsealed.

14 **II. Redaction, Not Continued Sealing, Is the Proper Mechanism for Protecting Any**
15 **Sensitive Information**

16 Petitioners recognize that there may be sensitive information in the requested materials
17 that legitimately ought to stay secret. However, that is not a sufficiently compelling reason to
18 rebut Petitioners’ and the public’s interest in disclosure of these materials. Redaction, rather than
19 indefinite continued sealing, is the appropriate answer.

20 As said, Petitioners’ request is limited to post-investigation surveillance orders and
21 materials. Once an underlying investigation has concluded, the need for sealing goes away, and
22 “[l]egitimate confidentiality interests” can be adequately protected through the less-restrictive
23 means of redaction. *In re Sealing & Non-Disclosure*, 562 F. Supp. 2d at 886, 894-95 (footnote
24

25 _____
26 ²⁰ See generally Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3
27 Fed. Cts. L. Rev. 177 (2009) (describing the growing, ahistorical trend of indefinitely-sealed
28 records and its threat to the public and the institution of the judiciary); Stephen Wm. Smith,
Gagged, Sealed & Delivered: Reforming ECPA’s Secret Docket, 6 Harv. L. & Pol’y Rev. 313
(2012) (in-depth dive into “the most secret court docket in America”: electronic-surveillance
matters under SCA, Wiretap, and Pen/Trap Acts).

1 and citation omitted). Redactions to render a sealed document appropriate for unsealing are
2 preferable to maintaining the entire document under seal, and there are no countervailing
3 interests to justify continued sealing. *See Custer Battlefield Museum*, 658 F.3d at 1195 n.5
4 (competing concerns can typically be accommodated “by redacting sensitive information rather
5 than refusing to unseal the materials entirely.” (citations omitted)).

6 Accordingly, Petitioners respectfully request that (1) the Court not keep entire documents
7 under seal that can feasibly be unsealed in redacted form, and (2) redactions be kept to a
8 minimum. Petitioners do not object in general to redactions required by statute or rule, or to the
9 redaction of sensitive law-enforcement information or of personal information (such as names or
10 contact information of defendants, victims, unindicted third parties, surveillance targets, their
11 interlocutors, or confidential informants).²¹ Petitioners reserve the right to request
12 reconsideration of specific redactions.

13 CONCLUSION

14 Sealing court orders related to surveillance indefinitely is a serious problem. As
15 Magistrate Judge Stephen Smith has argued, the public is blinded to the true state of surveillance
16 law because sealed orders escape scrutiny. As a result, “when it comes to marking the bounds of
17 legitimate government intrusion into our electronic lives,” as well as the proper scope of
18 government power to compel third parties to assist with these intrusions, “each magistrate judge
19 has effectively become a law unto himself.”²²

20 Public disclosure improves judicial deliberation and oversight, curbs government abuse
21 of power, bolsters the legitimacy of judicial decisions, and informs the public in current policy
22 debates. And yet, today technical-assistance matters are almost always sealed and remain so
23 forever. The government’s requests and arguments and the courts’ analysis and orders are secret.
24 Absent government or court action to end that secrecy, a Petition of the type filed here is the

25
26 ²¹ However, Petitioners request that the names of the third parties subjected to technical-
27 assistance demands not be redacted. The public has an interest in knowing what technical
28 assistance has been sought and/or required from, say, the maker of a smartphone or messaging
app that has millions of customers. *See supra* at 9-10.

²² Smith, *Kudzu in the Courthouse*, 3 Fed. Cts. L. Rev. at 212.

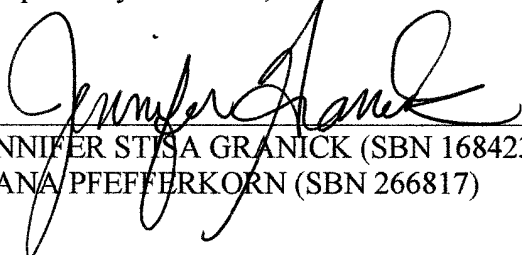
1 public's only recourse. There is no other way to identify judicial process that would reveal how
2 the technical-assistance provisions we identify are being interpreted by courts and used by
3 investigators today.

4 For these reasons, and because Petitioners have First Amendment and common-law rights
5 of access to the documents at issue, the requested records should be unsealed. Where there are
6 lingering confidentiality concerns, redaction, not continued sealing, will generally be the
7 appropriate response.

8 Therefore, Petitioners respectfully seek the docketing of the surveillance matters handled
9 in this District; the unsealing of the docket sheets; and the unsealing of technical-assistance
10 applications and orders issued by this Court, whether relating to access to encrypted information
11 or to other forms of compelled third-party assistance in carrying out court-authorized
12 surveillance, where there is no longer any compelling need for secrecy, as requested in the
13 accompanying Petition.

14 Respectfully submitted,

15
16 Dated: September 28, 2016


JENNIFER STISA GRANICK (SBN 168423)
RIANA PFEFFERKORN (SBN 266817)

1 JENNIFER STISA GRANICK (SBN 168423)
jennifer@law.stanford.edu
2 RIANA PFEFFERKORN (SBN 266817)
riana@law.stanford.edu
3 559 Nathan Abbott Way
4 Stanford, California 94305-8610
Telephone: (650) 736-8675
5 Facsimile: (650) 725-4086

6 *Pro Se* Petitioners
7

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA

10 **IN RE:**
11 **PETITION OF JENNIFER GRANICK AND**
12 **RIANA PFEFFERKORN TO UNSEAL**
13 **TECHNICAL-ASSISTANCE ORDERS AND**
14 **MATERIALS**

CV 16 80206 MISC.

**DECLARATION OF RIANA
PFEFFERKORN IN SUPPORT OF
PETITION TO UNSEAL TECHNICAL
ASSISTANCE ORDERS AND
MATERIALS**

KAW

**ORIGINAL
FILED**
SEP 28 2016
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 I, Riana Pfefferkorn, declare as follows:

2 1. I am an attorney licensed to practice law before this Court. I am the Cryptography
3 Fellow at the Center for Internet and Society at Stanford Law School (“CIS”), and am one of the
4 *pro se* Petitioners in the above-captioned matter. The following facts are true to the best of my
5 knowledge and belief and, if called and sworn as a witness, I could and would testify
6 competently to them.

7 2. On September 16, 2016, I spoke by telephone with Mr. Mark Jenkins, Deputy
8 Clerk of this Court. I asked Mr. Jenkins some questions regarding how this Court keeps track of
9 search warrants and surveillance authorization orders, such as wiretap or trap-and-trace orders.

10 3. Mr. Jenkins informed me that the Clerk’s office keeps paper records of warrants
11 and surveillance orders authorized by the Court, but that warrants and surveillance orders are not
12 entered into the Court’s system, they are not assigned a case number or any means to look them
13 up, and they are not searchable. He further stated that, while some search warrants are not sealed,
14 these warrants and orders are usually sealed and cannot be unsealed without a court order.

15 4. Mr. Jenkins further stated that the Clerk’s office does not keep track of these
16 materials, but that the United States Attorney’s Office for the Northern District of California
17 (“USAO”) would keep copies and categorize them.

18 5. Mr. Jenkins reiterated that these materials are not searchable and that in order to
19 locate a specific surveillance order, someone in the Clerk’s office would have to review all the
20 paper records of such materials one by one, potentially using a date range to narrow it down. He
21 stated that in the past, the Clerk’s office has received a few requests akin to my inquiry from
22 members of the public to review surveillance orders, but that it was impossible for the Clerk’s
23 office to honor these requests, and in any event sealed orders cannot be publicly disclosed
24 without court order.

25 6. On May 20, 26, and 31, June 1, 2, 6, 8, 13, 14, 17, 28, July 1, and September 16,
26 2016, my colleague Jennifer Granick, who is also a Petitioner in the above-captioned action and
27 the Director of Civil Liberties at CIS, corresponded by email with attorneys at the USAO to
28 attempt to meet and confer with the USAO regarding our efforts to have this Court’s technical-

1 assistance materials unsealed. As Ms. Granick explained in her emails, the purpose of the
2 proposed meet-and-confer was to learn more about the USAO's methods for tracking and
3 cataloging the materials Petitioners seek to unseal and to discuss how to minimize the burden to
4 the USAO of reviewing the materials. In addition to these emails, Ms. Granick also left
5 voicemail on June 1, 2016 with the then-Deputy Chief of the Criminal Division of the USAO
6 regarding the proposed meet-and-confer. These efforts were unsuccessful.

7 7. On September 20, 2016, Ms. Granick emailed Ms. Barbara Valliere, presently the
8 Chief of the Criminal Division of the USAO. The email informed Ms. Valliere that we planned
9 to file this Petition this week and requested a telephonic meet-and-confer. We received no
10 response.

11 I declare under penalty of perjury of the laws of the United States that the foregoing is
12 true and correct. Executed at San Francisco, California on September 28, 2016.

13
14 
15 Riana Pfefferkorn

1 JENNIFER STISA GRANICK (SBN 168423)
jennifer@law.stanford.edu
2 RIANA PFEFFERKORN (SBN 266817)
riana@law.stanford.edu
3 559 Nathan Abbott Way
4 Stanford, California 94305-8610
Telephone: (650) 736-8675
5 Facsimile: (650) 725-4086

6 *Pro Se* Petitioners
7

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA

10 IN RE:
11 PETITION OF JENNIFER GRANICK AND
12 RIANA PFEFFERKORN TO UNSEAL
13 TECHNICAL-ASSISTANCE ORDERS AND
14 MATERIALS

CV 16-80206 MISC. MIL. CAS. NO.

[PROPOSED]
ORDER GRANTING PETITION TO
UNSEAL TECHNICAL-ASSISTANCE
ORDERS AND MATERIALS

KAW

RECEIVED
SEP 28 2016
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 The Court has reviewed the Petition filed by Petitioners Jennifer Granick and Riana
2 Pfefferkorn to docket and unseal Court records relating to technical-assistance orders issued by
3 this Court. Having reviewed the Petition and the Memorandum of Points and Authorities and
4 supporting declaration attached thereto, and good cause appearing, the Petition is hereby
5 GRANTED.

6 (1) The Clerk of Court is respectfully ORDERED to assign case numbers to, and docket
7 in the Court's Case Management/Electronic Case Filing system ("CM/ECF"), any and all
8 applications, motions, opposition briefs, orders, and/or warrants, filed at any time, under the
9 following statutes:

- 10 ● the Wiretap Act, 18 U.S.C. §§ 2510-2522;
- 11 ● the Stored Communications Act (or "SCA"), 18 U.S.C. §§ 2701-2712;
- 12 ● the Pen Register Act (or "Pen/Trap Act"), 18 U.S.C. §§ 3121-3127; and/or
- 13 ● the All Writs Act (or "AWA"), 28 U.S.C. § 1651.

14 (2) It is further ORDERED that:

15 (a) the docket sheets for the foregoing surveillance matters be unsealed and made
16 publicly available, including on CM/ECF; and

17 (b) the underlying documents in the dockets for surveillance matters falling under the
18 following specific statutory provisions, filed from January 1, 2006 through six months before the
19 date of this Order, be unsealed and made publicly available, including on CM/ECF:

- 20 ● Sections 18 U.S.C. §§ 2511(2)(a)(ii) and/or 2518(4) of the Wiretap Act;
- 21 ● Section 18 U.S.C. § 2703 of the SCA;
- 22 ● Sections 18 U.S.C. §§ 3123(b)(2) and/or 3124(a) or (b) of the Pen/Trap Act; and/or
- 23 ● Section 28 U.S.C. § 1651(a) of the AWA.

24 (3) It is further ORDERED that, from the date of this Order onward,

25 (a) the Clerk of Court shall assign case numbers to, docket, and enter into CM/ECF
26 all applications and orders for search warrants, surveillance, and technical assistance;

27 (b) every 180 days, the Court shall undertake a review of sealed dockets, warrants,
28 surveillance orders, and technical-assistance orders; and

1 (c) after such review, the Court shall unseal those records for which there is no longer
2 any need for continued sealing.

3 Petitioners are directed to deliver a copy of this Order to the Office of the United States
4 Attorney for this District at the following address:

5 Federal Courthouse, 11th Floor

6 450 Golden Gate Avenue

7 San Francisco, CA 94102

8
9 SO ORDERED.

10
11 Dated: _____, 2016

12 _____
13 THE HONORABLE _____
14 UNITED STATES _____ JUDGE