No. 18-15416

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DENNIS JOSEPH RAIMONDO, AKA JUSTIN RAIMONDO AND ERIC ANTHONY GARRIS,

Plaintiff-Appellants,

v.

FEDERAL BUREAU OF INVESTIGATION

Defendant-Appellee,

On Appeal from the United States District Court
for the Northern District of California
No. 3:13-CV-02295-JSC
The Honorable Jacqueline Scott Corley

AMICUS BRIEF OF FIRST AMENDMENT COALITION IN SUPPORT OF APPELLANTS RAIMONDO AND GARRIS

ADAM GERSHENSON
(agershenson@cooley.com)
COOLEY LLP
500 Boylston Street
Boston, MA 02116-3736
(617) 937-2300 (telephone)
(617) 937-2400 (facsimile)

DAVID HOUSKA
(dhouska@cooley.com)
MAXWELL ALDERMAN
(malderman@cooley.com)
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111-5800
(415) 693-2000 (telephone)
(415) 693-2222 (facsimile)

Attorneys for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(a)(4)(A), *amicus curiae* certifies that it has no parent corporations or any publicly held corporations owning 10% or more of its stock.

Dated: August 3, 2018

COOLEY LLP

/s/ *Adam Gershenson*
Adam Gershenson

Attorneys for Amicus Curiae
FIRST AMENDMENT COALITION

TABLE OF CONTENTS

Page

I. INTEREST OF THE *AMICUS CURIAE* 1
II. SUMMARY OF ARGUMENT 2
III. ARGUMENT 3
A. If Affirmed, the District Court's Opinion Would Chill Essential Reporting on Politics and National Security. 4
1. The district court functionally stripped most journalists and newspapers of the Privacy Act's protections. 4
2. Blanket deference to the government's invocation of "national security" was especially inappropriate here. 8
a. The Watch List was already in the public record. 9
b. The Watch List was not classified. 10
3. Widespread surveillance of journalists chills press freedoms without advancing a legitimate government interest. 11
a. Courts consistently require strong justifications for government action that chills speech. 13
b. A mere exception to the Privacy Act cannot overwhelm First Amendment protections. 15
B. There Is No Legitimate Law Enforcement Interest Here. 17
1. The government did not classify the Watch List. 18
2. Publication of the Watch List posed no national security threat. 20
C. The Court Should Avoid Unconstitutional Statutory Interpretations. 24
D. The Court Should Announce a Clear Rule. 28
1. The rule needs to balance the needs of law enforcement and First Amendment protections. 28
2. Proper balancing here would have shown no threat from re-publication of an unclassified document. 30
IV. CONCLUSION 32

TABLE OF AUTHORITIES

Page

Cases

Bartnicki v. Vopper,
532 U.S. 514 (2001) 6

Bassiouni v. FBI,
436 F.3d 712 (7th Cir. 2006) 16

Becker v. I.R.S.,
34 F.3d 398 (7th Cir. 1994) 17

BedRoc Ltd., LLC v. United States,
541 U.S. 176 (2004) 25

Cal. First Amendment Coalition v. Calderon,
150 F.3d 976 (9th Cir. 1998) 1

Clark v. Library of Congress,
750 F.2d 89 (D.C. Cir. 1984) 13, 17, 18

Clarkson v. I.R.S.,
678 F.2d 1368 (11th Cir. 1982) 17

Crowell v. Benson,
285 U.S. 22 (1932) 24, 25

Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Const. Trades Council,
485 U.S. 568 (1988) 24, 26

Elrod v. Burns,
427 U.S. 347 (1976) 5, 12

First Amendment Coalition v. United States Dep't of Justice,
Case No. 15-15117 (9th Cir. Aug. 17, 2017) 1

Gomez v. United States,
490 U.S. 858 (1989) 24

TABLE OF AUTHORITIES
(continued)

Page

Henke v. U.S. Dep't of Commerce,
83 F.3d 1453 (D.C. Cir. 1996) 3

Hernandez v. Williams, Zinman, & Parham PC,
829 F.3d 1068 (9th Cir. 2016) 25

Hooper v. People,
155 U.S. 648 (1895) 24

MacPherson v. I.R.S.,
803 F.2d 479 (9th Cir. 1986) ..... *passim*

Mills v. State of Alabama,
384 U.S. 214 (1966) 11, 12, 14, 15

Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue,
460 U.S. 575 (1983) 14

N.L.R.B. v. Catholic Bishop of Chicago,
440 U.S. 490 (1979) 26

New York Times Co. v. United States,
403 U.S. 713 (1971) 6, 10, 23, 24

Presbyterian Church (U.S.A.) v. United States,
870 F.2d 518 (9th Cir. 1989) 13

Rust v. Sullivan,
500 U.S. 173 (1991) 27

Sander v. State Bar of Cal.,
58 Cal. 4th 300 (2013) 1

Spencer v. World Vision, Inc.,
633 F.3d 723 (9th Cir. 2011) 26

Thornhill v. Alabama,
310 U.S. 88 (1940) 12

TABLE OF AUTHORITIES
(continued)

Page

United States v. U.S. Dist. Ct.,
407 U.S. 297 (1972) 12

Valenzuela Gallardo v. Lynch,
818 F.3d 808 (9th Cir. 2016) 26, 27

U.S. Constitution

Art. VI 15
First Amendment ..... *passim*

Statutes

5 U.S.C.
§ 552 ..... *passim*
§ 552a(e)(7) ..... *passim*

18 U.S.C.
§ 793(d)-(f) 19
§ 1924 19

California Public Records Act, Cal. Gov. Code, § 6250 et seq. 1

Other Authorities

120 Cong. Rec. 36,651 16

120 Cong. Rec. H10,892 (daily ed. Nov. 20, 1974) 16

40 Fed. Reg. 28, 965 (1975) 16, 17

Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 Journalism & Mass. Comm. Q. 193 (June 2016) 13, 14

Executive Order 13292 ..... 18, 19, 29

TABLE OF AUTHORITIES
(continued)

Page

Joan Jackson, *Beyond the Scope of Ordinary Training and Knowledge*, 32 Pace L. Rev. 676 (2012) 20

Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech. L.J. 117 (2016)..... 14

Legislative History of the Privacy Act of 1974, S. 3418 (Pub. L. No. 93-579), Source Book on Privacy, at 796 (Joint Comm. Print 1976) 10

Media Incentives and National Security Secrets, 122 Harvard L. Rev. 2228 (2009) 23

Presidential Task Force on Controlled Unclassified Info., Report and Recommendations (2009) 20

S. Rep. No. 1183, 93d Cong., 2d Sess., *reprinted in* 1974 U.S.C.C.A.N. 6916 ..... 17, 29, 30

Sam Westrop, *Exclusive: Obama Administration Knowingly Funded a Designated al-Qaeda Affiliate*, National Review, July 25, 2018 7

Shane Harris, et. al., *Kushner's Overseas Contacts Raise Concerns as Foreign Officials Seek Leverage*, The Washington Post, Feb. 27, 2018 7

Shane Harris and Gordon Lubuld, *Russia Has Turned Kaspersky Software Into Tool for Spying*, The Wall Street Journal, Oct.11, 2017..... 7

T.C. Sottek and Janus Kopfstein, *Everything You Need to Know About PRISM*, The Verge 14

Thomas Blanton, Testimony to U.S. House Committee on the Judiciary, Dec. 16, 2010 23

I. INTEREST OF THE *AMICUS CURIAE*

The First Amendment Coalition ("FAC") is a non-profit public interest organization dedicated to promoting and defending free speech and a free press, more open and accountable government, and public participation in civic affairs. FAC regularly litigates issues relating to the First Amendment, the Freedom of Information Act, 5 U.S.C. § 552 et. seq. ("FOIA"), and the California Public Records Act, Cal. Gov. Code, § 6250 et seq., ("CPRA") in state and federal courts in California and beyond. *See, e.g., First Amendment Coalition v. United States Dep't of Justice*, Case No. 15-15117 (9th Cir. Aug. 25, 2017) (right of access under FOIA to DOJ records); *Cal. First Amendment Coalition v. Calderon*, 150 F.3d 976 (9th Cir. 1998) (First Amendment right of access to executions); *Sander v. State Bar of Cal.*, 58 Cal. 4th 300 (2013) (public right of access to records of the California State Bar).

To FAC's knowledge, this is the first case to consider when a journalist or news organization may be lawfully subjected to government surveillance under the Privacy Act. It can establish important precedent governing the intersection of First Amendment rights, the Privacy Act's broad protections, and the government interest in investigating legitimate national security threats. Given the well-recognized chilling effect that surveillance—or even the threat

of surveillance—has on how journalists and news organizations exercise their First Amendment Rights, this case goes to the heart of the FAC's mission. Unfortunately, the district court opinion, if left to stand, would eviscerate the Privacy Act's protections for journalists and news outlets. The First Amendment Coalition respectfully submits this brief to help the Court weigh the consequences its decision will likely have for reporters throughout the country.

This brief was prepared pro bono by counsel for the First Amendment Coalition. No funds, either of the First Amendment Coalition or its members, were used to create this submission. All parties to this action have consented to the First Amendment Coalition filing this amicus brief.

II. SUMMARY OF ARGUMENT

Allowing federal agencies to invoke purported "national security" concerns to investigate journalists in the absence of an actual threat imperils the core protections of the First Amendment. Yet here the lower court did exactly that, blessing FBI surveillance of a media outlet based on the mere re-publication of a non-classified document that was already in the public domain. That decision, if left to stand, would not only impact the subject of that needless

surveillance, Antiwar.com, but would have sweeping negative effects on America's free press.

This Court should reverse the lower court's decision in order to (1) safeguard political reporting, which lies at the heart of the First Amendment; (2) prevent investigations into media members in the absence of legitimate law enforcement interests; (3) cure the lower court's misinterpretation of the Privacy Act that threatens to both subvert the Act's purpose and render the Act unconstitutional; and (4) provide guidance through a practical test that permits surveillance of journalists only where the published material reasonably poses a threat to national security. That balanced approach would ensure that future investigations of journalists protect both national security and the First Amendment.

III. ARGUMENT

The Privacy Act, which "safeguards the public from unwarranted collection, maintenance, use and dissemination of personal information contained in agency records," should not be misconstrued to justify agencies broadly recording First Amendment activities. *See Henke v. U.S. Dep't of Commerce*, 83 F.3d 1453, 1456 (D.C. Cir. 1996). Here, the Government ignored this statutory proscription and opened a file to monitor Antiwar.com,

claiming that publication of a purported terrorist watch list (the "Watch List")—an unclassified and previously published document—satisfied the law enforcement exception to the Privacy Act. The court held that investigation was proper because the purported threat assessment was conducted in accordance with the extraordinarily broad October 31, 2003 Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection ("2003 AG Guidelines"). The district court's decision to bless that operation, in a case where neither the court nor the Government truly explained or justified how such a publication posed the required threat to national security, opens the gateway to widespread, baseless surveillance of journalists—an affront to both the Privacy Act and the First Amendment.

A. If Affirmed, the District Court's Opinion Would Chill Essential Reporting on Politics and National Security.

1. The district court functionally stripped most journalists and newspapers of the Privacy Act's protections.

Under the First Amendment, "Congress shall make no law . . . abridging the freedom of speech, or of the press." U.S. Const. Amd. I. Consistent with these fundamental protections, the Privacy Act prohibits the federal government from "maintain[ing] [any] record describing how any individual exercises rights guaranteed by the First Amendment[.]" 5 U.S.C. § 552a(e)(7).

In passing the Privacy Act, however, Congress allowed for a narrow exception, allowing agencies to maintain records on First Amendment activity only where "pertinent to and within the scope of an authorized law enforcement activity." *Id.*

In *MacPherson v. I.R.S.*, this Circuit "decline[d] to fashion a hard and fast standard for determining whether a record of First Amendment activity" meets the so-called "law enforcement exception" because of "strong policy concerns on both sides of the issue." 803 F.2d 479, 483-84 (9th Cir. 1986). The Court recognized the need to balance law enforcement demands against the knowledge that "even 'incidental' surveillance and recording of innocent people exercising their First Amendment rights may have the 'chilling effect' on those rights that section (e)(7) was intended to prohibit." *Id.*; *see also Elrod v. Burns*, 427 U.S. 347, 362 (1976) (requiring strict scrutiny even for indirect restrictions that inadvertently chill First Amendment expression).

Here, however, rather than carefully balance law enforcement interests against the need for robust First Amendment protections, the lower court accepted with little scrutiny the FBI's opening a file on Antiwar.com based solely on an unsupported reference to a chimerical national security threat, while substantially discounting or ignoring the First Amendment rights at stake.

ER062:12-13. Rather than scrutinize the FBI's contention that the Watch List's re-publication could threaten national security, the court simply assumed the unclassified document was somehow dangerous, apparently because it was marked "FBI SUSPECT LIST" and "Law Enforcement Sensitive." *See* ER059:11-12. Such an approach turns the Privacy Act upside down, letting the government open surveillance files on news outlets that publish information the government deems sensitive—in other words, virtually any news outlet that publishes a document the government asserts, even with little or no evidentiary basis, could conceivably harm national security.

As the Supreme Court has recognized, government claims regarding national security must be carefully scrutinized where First Amendment rights are at stake. *New York Times Co. v. United States*, 403 U.S. 713 (1971) (affirming, despite credible claims of national security interests, a First Amendment right to publish the Pentagon Papers). Indeed, when outlets publish such materials they "should be commended for serving the purpose that the Founding Fathers saw so clearly. In revealing the workings of government . . . [they] nobly [do] precisely that which the Founders hoped and trusted they would do." *Id.* at 717 (Black, J., concurring); *see also Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) (First Amendment protects publication of information of

public concern, even if unlawfully obtained in the first instance, i.e., not by the publishing party).

Today's journalists continue this mission. In the last year alone:

- The Wall Street Journal revealed how Russian spies penetrated the NSA via popular Kaspersky Labs anti-virus software. Shane Harris and Gordon Lubuld, *Russia Has Turned Kaspersky Software Into Tool for Spying*, The Wall Street Journal, Oct. 11, 2017.

- The National Review reported that former President Obama knowingly funded designated al-Qaeda affiliates. The Review divulged sensitive information regarding entities on terror watch lists, emails between foreign powers, and the flow of money from the US to terrorist organizations. Sam Westrop, *Exclusive: Obama Administration Knowingly Funded a Designated al-Qaeda Affiliate*, National Review, July 25, 2018.

- The Washington Post warned that American intelligence agencies had intercepted communications where leaders of foreign countries discussed how to manipulate Jared Kushner. Shane Harris, et. al., *Kushner's Overseas Contacts Raise Concerns as Foreign Officials Seek Leverage*, The Washington Post, Feb. 27, 2018.

Each of these stories reported highly classified or sensitive government information. Under the district court's reasoning—that publishing classified or sensitive government documents on its own creates a plausible "national security threat" that justifies further investigation—merely publishing these stories would have rendered the National Review, The Wall Street Journal, and the Washington Post legitimate targets of government surveillance. Under the

district court's approach, such investigations would comport with the Privacy Act and First Amendment, because every one of these article met the 2003 Guidelines. ER551 (purporting to justify investigations for any publication implicating "information concerning possible targets of international terrorism, espionage, foreign computer intrusion, or other threats to the national security"). Indeed, each of the articles noted above would provide far stronger justification for opening an FBI file than the publication at issue here, because unlike the Antiwar.com posting, they all disclosed previously secret intelligence. But the First Amendment's protection of free speech and a free press cannot be squared with a rule that would allow such vital information sharing, by itself, to serve as a lawful basis for investigating the National Review, the Washington Post, and the Wall Street Journal.

2. Blanket deference to the government's invocation of "national security" was especially inappropriate here.

Future cases may pose challenging scenarios that require a difficult balancing of interests between national security and freedom of the press. For that reason, in Section III.D.), *infra*, we propose an approach to guide such inquiries. This was not, however, a close case. By failing to meaningfully weigh either side of the question—the tissue-thin "national security"

justification on the one hand, and the substantial First Amendment harm from baseless surveillance on the other—the district court set a dangerous precedent.

a. The Watch List was already in the public record.

Antiwar.com was not the first outlet to publish the Watch List. The Watch List was available elsewhere online; indeed, the information was already in widespread circulation. ER436-37 (noting that the Watch List is available on Italian and Finnish banking association websites); ER532 ("Many agencies outside of law enforcement have been utilizing this [Watch List] information to screen their employees."). Accordingly, the district court opinion not only allows for law enforcement to surveil journalists based on a single publication of purportedly "sensitive" (but not actually classified, see *infra* III.B.1.) government information, but would also permit the government to open a file on any other news organization that re-publishes or otherwise follows the original report—even if its further publication could not reasonably create a true security threat. Under that approach, every successive outlet that picks up the story would lose the Privacy Act's protections. Congress did not enact a nullity, but the district court's interpretation would make it so.

b. The Watch List was not classified.

The Watch List was not even a classified document.[1] If the government could invoke the law enforcement exception based on the redundant publication of non-classified material, the Privacy Act's First Amendment protections would be nullified upon publication of any information unilaterally deemed "sensitive," irrespective of any actual security threat resulting from the disclosure of such information. This would radically expand the number of news stories that could trigger lawful surveillance. Given the ill-defined limits of what constitutes "sensitive" information (see below *infra* III.B.), there is little to stop the government from abusing this designation to deter unfavorable or embarrassing press coverage. This is the exact scenario the Supreme Court warned against when it wrote that "'security' is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment." *New York Times Co.*, 403 U.S. at 719.

Moreover, Congress was highly attuned to the risk posed by expansive, and expanding, "security" justifications when it passed the Privacy Act. *See, e.g.*, Legislative History of the Privacy Act of 1974, S. 3418 (Pub. L. No. 93-

[1] Discussed further in Part III.B. below.

579), Source Book on Privacy, at 796 (Joint Comm. Print 1976) (statement of Senator Nelson) (noting that Nixon had "secretly authorized wiretaps on 17 Government officials and newspapermen . . . . The Government allegedly believed that publication of this information did or would jeopardize 'national security.' There is still no public evidence to justify that "belief"). This Court should heed the Supreme Court and Congress' warnings and refuse to allow surveillance based merely on the publication of purportedly "sensitive" information.

3. Widespread surveillance of journalists chills press freedoms without advancing a legitimate government interest.

When the district court green-lit surveillance of journalists based solely on the re-publication of "sensitive" information, it not only eviscerated the Privacy Act's First Amendment protections, but also sanctioned government conduct that will inevitably chill accountability journalism that lies at the historical and legal heart of the First Amendment. "[A] major purpose of that Amendment was to protect the free discussion of governmental affairs" and "[s]uppression of the right of the press to praise or criticize governmental agents and to clamor and contend for or against change . . . . muzzles one of the very agencies the Framers of our Constitution thoughtfully and deliberately

selected to improve our society and keep it free." *Mills v. State of Alabama*, 384 U.S. 214, 218-19 (1966). The Supreme Court has recognized that even indirect restrictions on the media's First Amendment activity must survive exacting scrutiny, due to their pervasive chilling effects. *Elrod v. Burns*, 427 U.S. 347, 362 (1976). The record here shows the investigation of Antiwar.com had exactly the chilling effect the Supreme Court and the Framers feared. Antiwar.com experienced negative impacts on its ability to secure writers and information from confidential sources (ER393, ER441-42, ER244-45), and lost financial support from several major donors, which resulted in the termination of four employees, five paid columnists, and two part-time assistants. (ER361.)

Both preemptive censorship and post-publication retaliation deter free speech. *Thornhill v. Alabama*, 310 U.S. 88, 101-02 (1940) ("The freedom of speech and of the press . . . embraces at the least the liberty to discuss publicly and truthfully all matters of public concern without . . . fear of subsequent punishment."). Surveillance by law enforcement or security agencies is a particularly chilling form of retaliation. The "dread of subjection to an unchecked surveillance power . . . deter[s] vigorous citizen dissent." *United States v. U.S. Dist. Ct.*, 407 U.S. 297, 320 (1972).

a. Courts consistently require strong justifications for government action that chills speech.

The Government may not place a person or organization under surveillance based solely on their First Amendment activities without showing a "paramount [] interest." *Clark v. Library of Congress*, 750 F.2d 89, 94-95 (D.C. Cir. 1984) (holding that surveillance ordered in response to federal employee's membership in socialist political organizations violated the First Amendment). The shadow of surveillance falls darkly over the legitimate exercise of First Amendment rights. *See, e.g.*, *Presbyterian Church (U.S.A.) v. United States*, 870 F.2d 518, 522 (9th Cir. 1989) ("[S]urveillance has chilled [churchgoers] from attending worship services, and . . . this effect on the congregants has in turn interfered with the churches' ability to carry out their ministries.").

Empirical research confirms that the mere threat of government surveillance chills debate and dissent. In 2016, Professor Elizabeth Stoycheff studied how users expressed political views on Facebook following published revelations that the NSA's PRISM program collected information on Americans' online activity. When Americans with dissenting opinions perceived they were being monitored, they readily conformed their behavior—expressing opinions only when they were in the majority and otherwise self-

censoring and remaining silent. Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 Journalism & Mass. Comm. Q. 193, 296 (June 2016). Similarly, after the NSA's PRISM program was widely reported, Wikipedia saw a marked decrease in page views related to various terrorism-related subjects. Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech. L.J. 117 (2016). Importantly, the PRISM program was a largely automated process which indiscriminately collected data without targeting anyone in particular. T.C. Sottek and Janus Kopfstein, *Everything You Need to Know About PRISM*, *The Verge*, July 17, 2013. The chilling effect of surveillance is far greater when—as here—the government specifically targets individuals and organizations.

According to the lower court, the government may target journalists for surveillance based solely on publishing activity that both advances the core values of the First Amendment and depends on that Amendment for its survival. *See, e.g.*, *Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue*, 460 U.S. 575, 585 (1983) (recognizing that it is a "basic assumption of our political system that the press will often serve as an important restraint on government"); *Mills*, 384 U.S. at 219 ("The press serves and was designed

to serve as a powerful antidote to any abuses of power by governmental officials and as a constitutionally chosen means for keeping officials elected by the people responsible to all the people whom they were selected to serve."). The empirical research and Supreme Court authorities point in the same direction: toward a free press, and away from the chilling impact of widespread or pre-textual surveillance. Permitting the lower court's ruling to stand, despite the lack of justification for the government's surveillance, would stifle free speech and a free press, contravening both the plain language of the Privacy Act and the First Amendment protections that Act expressly embraces.

b. A mere exception to the Privacy Act cannot overwhelm First Amendment protections.

Even if Congress *had* intended the Privacy Act's statutory exception to limit First Amendment protections, the Supremacy Clause and the First Amendment would have barred such an attempt. U.S. Const. Art. VI ("This Constitution . . . shall be the supreme law of the land."); U.S. Const. Amd. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press.").

But of course, that was not Congress' intent. When he introduced the language that would eventually become the law enforcement exception, then-Congressman Richard H. Ichord Jr. stated:

> I want to emphasize – so that there is no misunderstanding – these changes are designed to protect only legitimate national or internal security intelligence and investigations, and *no records or files shall be kept on persons which are not within constitutional limitations. Let the legislative history be explicit. None of these changes are intended to abridge the exercise of first amendment rights.* The rights of Americans to dissent in a lawful manner and for lawful purposes must be preserved.

Bassiouni v. FBI, 436 F.3d 712, 718 (7th Cir. 2006) (citing 120 Cong. Rec. 36,651, reprinted in Senate Comm. On Gov't Operations and House Comm. On Gov't Operations, 93rd Cong., 2d Sess., Legislative History of the Privacy Act of 1974, S. 3418 (Pub. L. No. 93-579): Source Book on Privacy, at 902-903 (Joint Comm. Print 1976) (emphasis added)). Congress aimed only "to make certain that political and religious activities are not used as a cover for illegal or subversive activities." 120 Cong. Rec. H10,892 (daily ed. Nov. 20, 1974). To use that narrow statutory exception—designed to avoid disingenuous claims to political and religious conduct—as a basis for authorizing blanket, potentially pre-textual surveillance of journalists would turn the law on its head.

The Privacy Act's legislative history is rife with warnings against precisely the sort of error committed by the lower court here. As advocates for the Privacy Act and the law enforcement exception stated, "there was no intention to interfere with First Amendment rights." OMB Guidelines, 40 Fed.

Reg. 28,965 (1975) (quoting *Congressional Record*, Nov. 20, 1974, H10,892 and Nov. 21, 1974, H10952). The Senate, likewise, concurred: "This section's restraint is aimed particularly at preventing collection of protected information not immediately needed, about law-abiding Americans, on the off-chance that Government or the particular agency might possibly have to deal with them in the future." S. Rep. No. 1183, 93d Cong., 2d Sess., *reprinted in* 1974 U.S.C.C.A.N. 6916, 6971. This clear evidence shows that the law enforcement exception was meant to be narrow, and that the overall purpose was to *restrict* government surveillance. *See, e.g.*, *MacPherson*, 803 F.2d at 482 ("[T]he Privacy Act . . . is intended to restrict the information about individuals' First Amendment activities that the government may collect and maintain."); *Becker v. I.R.S.*, 34 F.3d 398, 410 (7th Cir. 1994); *Clarkson v. I.R.S.*, 678 F.2d 1368, 1374 (11th Cir. 1982) ("By enacting this exception, however, Congress did not intend to dilute the guarantees of the First Amendment[.]"). The District Court's approach would betray both Congress and the Constitution.

B. There is no legitimate law enforcement interest here.

Far from showing a "paramount" interest required to justify surveillance of journalists, the government's interest here is either non-existent or, at best, *de minimis*. *See Clark*, 750 F.2d at 94-95 ("paramount" interest required under

First Amendment). The district court found the FBI had a legitimate law enforcement interest in investigating Antiwar.com based solely on the purported "threat to national security" posed by the publication of the Watch List. ER059:11-17, n.11. The government's own conduct proves, however, there never was any such threat because (1) the Watch List was not classified and (2) the government never explicitly found that the List's dissemination would harm national security.

1. The Government Did Not Classify the Watch List.

At the time Antiwar.com published the Watch List, classified information in the United States was defined and governed by Executive Order 13292. E.O. 13292, Preamble, March 25, 2003. The Order (similar to those from prior and subsequent administrations) established three levels of classification. The lowest, "Confidential," was "applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security[.]" *Id.* at § 1.2. The highest, "Top Secret," applied to "information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security[.]" *Id.* Notably, the classifying officer had to be able to "identify or describe" the

particular harm which could come from the uncontrolled dissemination of information before it could receive any level of classification. *Id.*

Once information has been formally classified, it receives numerous protections. Classified information may be accessed only by persons with a requisite security clearance and must be secured using designated systems and safeguards. E.O. 13292 §§ 4.1-4.2. The intentional, reckless, or negligent failure to secure classified information by a federal employee or contractor is a criminal offense punishable by up to five years in prison. 18 U.S.C. § 1924; 18 U.S.C. § 793(d)-(f). Criminal penalties attach *only* to information which has been formally classified. 18 U.S.C. § 1924; 18 U.S.C. § 793 (d)-(e) (covering only transmission of information to persons "not entitled to receive it").

The Watch List was not even deemed to contain the *lowest* level of classified information. It was, instead, merely marked "Law Enforcement Sensitive." ER059:11-12. "Law Enforcement Sensitive" is one of numerous labels used by the government to mark "Sensitive but Unclassified" ("SBU") information.

By definition, the nebulous body of SBU information falls *outside* the realm of classified information. At the time the FBI surveilled Antiwar.com, SBU information had no formal definition either in statute or executive order.

Joan Jackson, *Beyond the Scope of Ordinary Training and Knowledge*, 32 Pace L. Rev. 676 (2012). Instead, SBU referred collectively to "the various designations used within the Federal Government for documents and information that are sufficiently sensitive to warrant some level of protection, but that do not meet the standards for National Security Classification." Presidential Task Force on Controlled Unclassified Info., Report and Recommendations 1, vii n.1 (2009). The plethora of different SBU designations reflects the lack of any uniform standards or regulations governing the label; there are over 130 different labels or markings for SBU information. *Id.* at 5. Given that there are no practical restrictions on what the government may deem "sensitive," relying on such a nebulous standard to justify recording First Amendment activities would render the Privacy Act's First Amendment protections a paper shield.

2. Publication of the Watch List posed no national security threat.

The district court found the law enforcement exception applied here because the FBI "was investigating whether the publication of the [Watch List] on Antiwar.com posed a national security threat." But the FBI never explained, and the district court never adequately questioned, why it was appropriate or even reasonable to conclude that the publication of the Watch List implicated

national security concerns. Both simply assumed that re-publication of the (unclassified) Watch List justified an investigation into alleged danger to national security. But unlike classified materials, for the List there was *no* prior determination that dissemination could pose any harm to national security. And it could not, as the List already appeared broadly elsewhere. Thus, the Government's ad hoc, purported justification for further investigation is not just unsupported, but directly contradicted by the evidence.

There may well be scenarios where disclosure of SBU information could theoretically or potentially harm the national interest or law enforcement operations. Thus, a categorical rule that no such information could justify an investigation would be inappropriate and impractical. That said, the breadth and malleability of this ambiguous designation means that neither an investigator nor a court can simply assume—as the district court did—that such non-classified materials pose a *per se* threat to national security.

Indeed, the evidence before the district court strongly suggests that the Watch List was deemed sensitive for reasons that had nothing to do with national security. As the government acknowledged, the Watch List was widely used by agencies and private companies outside of law enforcement to screen potential employees for security risks. ER532. Furthermore, the FBI's

San Francisco Field Office concluded that "the information contained therein is public source information and not a clear threat to National Security." ER416. The district court erred when it ignored this evidence and simply accepted the government's unsupported assertion that the FBI had a legitimate law enforcement interest in investigating the publication of the Watch List.

Allowing such surveillance based on mere publication of unclassified information places America's free press in existential danger. *First*, given the sheer volume of potentially "sensitive" information, many more stories and journalists could be subjected to surveillance. *Second*, imbuing the label with that power would encourage the government to use SBU designations as a weapon to protect itself from criticism. *Third*, given that there are no statutes or clear standards governing what constitutes SBU information, the executive branch (and each individual department within the executive branch) can designate SBU information as it sees fit. There are few obstacles to the government deciding to mark merely embarrassing or scandalous information "sensitive." Allowing surveillance of any whistleblower or journalist based on the publication of "sensitive" information thus invites the government to use the law enforcement exception to retaliate against whistleblowers and journalists who expose misconduct.

This is no hypothetical threat. Overclassification is already a rampant problem, with high level national security officials estimating that between 50 and 90 percent of classified information could be released without compromising national security. Thomas Blanton, Testimony to U.S. House Committee on the Judiciary, Dec. 16, 2010. Nor is this overclassification a harmless result of departmental inertia. "[O]fficials often classify 'to deny the public an understanding of the policymaking process' or to conceal abuses of internal civil liberties, without real national security justification." *Media Incentives and National Security Secrets*, 122 Harvard L. Rev. 2228, 2234 (2009) (citation omitted). Allowing retaliatory surveillance based on the publication of non-classified information would embolden government abuses, expand the pool of shrouded materials, and further chill conduct protected by the First Amendment. If security is "a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment," certainly those contours should not be expanded to bless suppression of unclassified, "sensitive" information like the Watch List. *New York Times Co.*, 403 U.S. at 719.

Finally, allowing surveillance based on the publication of unclassified information contravenes this Court's approach in *MacPherson*, which provided

that the Privacy Act's law enforcement exception should be read narrowly. 803 F.2d at 482 (a "narrow reading of 'law enforcement activities' better serves the goal of privacy and avoids infringing on the overall First Amendment concerns of section (e)(7)"). Far from embracing that "narrow reading," the district court went to the opposite extreme. The district court held the FBI may invoke "national security" to surveil anyone who publishes or even re-publishes not only information the government has chosen to protect through classification but also any document the government deems "sensitive."

C. The Court Should Avoid Unconstitutional Statutory Interpretations.

Under "settled policy," courts "avoid an interpretation of a federal statute that engenders constitutional issues if a reasonable alternative interpretation poses no constitutional question." *Gomez v. United States*, 490 U.S. 858, 864 (1989). As the Supreme Court has cautioned, courts should "not lightly assume that Congress intended to infringe constitutionally protected liberties or usurp power constitutionally forbidden it." *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Const. Trades Council*, 485 U.S. 568, 575 (1988). Rather, "[t]he elementary rule is that every reasonable construction must be resorted to in order to save a statute from unconstitutionality." *Hooper v. People*, 155 U.S. 648, 657 (1895); *see Crowell v. Benson*, 285 U.S. 22, 62 (1932) ("When the

validity of an act of Congress is drawn in question, and even if a serious doubt of constitutionality is raised, it is a cardinal principle that this Court will first ascertain whether a construction of that statute is *fairly possible* by which the question may be avoided.") (emphasis added).

Here, by misconstruing the law enforcement exception to the Privacy Act to allow surveillance of almost any journalist in the name of national security, the district court needlessly broadened the statute to endanger First Amendment protections. Narrower approaches that would not have raised such constitutional problems or rendered the Act unconstitutional were fairly possible, and certainly available. The court needlessly, and impermissibly, expanded the circle of what types of publication could excuse an investigation into members of the press.

There is no cause to interpret the Privacy Act to infringe upon First Amendment rights. In interpreting a statute, this Court must "begin, as always, with the statutory text" because courts "must 'presume that [the] legislature says in a statute what it means and means in a statute what it says there.'" *Hernandez v. Williams, Zinman, & Parham PC*, 829 F.3d 1068, 1072 (9th Cir. 2016) (quoting *BedRoc Ltd., LLC v. United States*, 541 U.S. 176, 183 (2004)). Here, the Act demands that agencies *refrain* from recording (and infringing

upon) First Amendment activities except in two narrow circumstances: when "expressly authorized by statute" or when "pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7). Given the express prohibition against collecting information that might describe an individual's First Amendment activities, this Court has correctly required a "'narrow reading' of the statute," which "better serves the goal of privacy and avoids infringing on the overall First Amendment concerns of section (e)(7)." *MacPherson*, 803 F.2d at 482 (original emphasis omitted). The narrow exception should not swallow the rule where Congress required agencies to refrain from curtailing First Amendment rights.

Under such circumstances, where the district court's construction would raise "serious constitutional problems," precedent "requires courts to construe the statute to avoid such problems unless such a construction is plainly contrary to Congress' intent." *Edward J. DeBartolo Corp.*, 485 U.S. at 569; *see also N.L.R.B. v. Catholic Bishop of Chicago*, 440 U.S. 490, 499-501 (1979); *Spencer v. World Vision, Inc.*, 633 F.3d 723, 728-29 (9th Cir. 2011) (rejecting "as we must" a "constitutionally questionable" and "cramped reading" of a statute that "raises serious questions under both the Free Exercise Clause and the Establishment Clause" of the Constitution); *Valenzuela Gallardo v. Lynch*, 818

F.3d 808, 818 (9th Cir. 2016) (rejecting a statutory construction that raises "grave doubts" as to the constitutionality of the statute) (quoting *Rust v. Sullivan*, 500 U.S. 173, 190-91 (1991)).

Far from denying that its interpretation raised constitutional questions, the district court confirmed that "the records at issue describe Plaintiffs' exercise of their First Amendment activities—namely, political speech." ER058. It chose, however, to ignore this Court's instruction that agency records that have "a chilling effect on" the "exercise of First Amendment freedoms" be permitted only on a "case-by-case" basis under a narrow set of circumstances. *MacPherson*, 803 F.2d at 484. Instead, the district court's decision sweeps broadly, and could be reasonably interpreted to authorize the FBI to record and document the activities of any journalist who publishes *any* material that might give rise to even the most dubious invocation of a purported "a national security threat." ER062. As noted *supra*, by equating a "law enforcement activity" with "a national security threat," the district court effectively opened the door to surveillance and collection of records on any journalist who has ever seriously reported on security, foreign affairs, or military readiness. And by effectively neutralizing Section 552a(e)(7)'s First Amendment protections—and inviting surveillance of all journalistic inquiry

into issues of national security—the district court created needless tension between the Privacy Act's law enforcement exception and the First Amendment guarantees of a free press.

D. The Court Should Announce a Clear Rule.

To FAC's knowledge, this is the first case to address whether a journalist may be lawfully subjected to surveillance under the Privacy Act based on his or her reporting. It will not be the last. Given the significant implications for freedom of the press, this Court should take the opportunity to announce a clear rule regarding when such surveillance is appropriate. Specifically, this Court should hold that the Privacy Act's law enforcement exception allows surveillance of a journalist or news outlet based on the publication of classified or sensitive government information only when the government determines in good faith that the publication of the information on its own poses a threat to national security.

1. The rule Nneeds to balance the needs of law enforcement and First Amendment protections.

Requiring good faith determination that the information, in isolation, represents a national security threat would strike a balance between the interests of the government and press because it properly focuses on the publication of a particular document, rather than the document's publisher. If a document has

been properly classified, for example, then the government will be able to evaluate, based on an analysis of the document itself, whether its publication poses a threat to national security. In some instances, such as the publication of older documents, the government may conclude that whatever risk existed at the time of classification has since dissipated and no harm has been done by the document's publication. But when there is a genuine danger the government will be able to determine that, based on the face of the document itself. As the Executive Orders defining classified information dictate, the classifying authority must at the time of classification be able to "identify or describe" the particular harm that might result from publication. *E.g.*, E.O. 13292 § 1.2. When the government concludes in good faith that the information's publication poses a threat, then the statute's exception pertaining to law enforcement needs would apply and allow the government to investigate further. When, however, the government concludes that the publication does *not* threaten national security, then there is no legitimate law enforcement interest in continued investigation and surveillance of the publisher or publication. Indeed, the need to *prevent* surveillance for its own sake in the absence of any serious national or domestic security concerns drove Congress to enact the Privacy Act in the first instance. S. Rep. No. 1183, 93d Cong., 2d

Sess., *reprinted in* 1974 U.S.C.C.A.N. 6916, 6971 (stating that the Privacy Act was "aimed particularly at preventing collection of protected information not immediately needed").

2. Proper balancing here would have shown no threat from re-publication of an unclassified document.

This case demonstrates how and why this practical, document-focused test could be readily implemented. The FBI could not have concluded in good faith that Antiwar.com's publication of the Watch List in April 2004 posed a legitimate threat to national security for two distinct reasons. First, the information was already publically available online and widely used by non-governmental entities. ER532, ER436-37. A single additional publication could not have posed a legitimate national security concern. Second, the Watch List was not a classified document, meaning that there was no prior determination or facial reason to believe its publication would harm national security. As the San Francisco Field Office would later confirm, "the information contained [In the Watch List] is public source information and not a clear threat to National Security." ER416. The FBI could and should have concluded, without investigating Antiwar.com itself, that there was no potential threat to national security and thus no legitimate reason to open a file on the publisher.

This analysis also shows where the district court erred. The lower court reasoned that the government was justified in opening a file on Antiwar.com in order to properly investigate whether the re-publication of the Watch List threatened national security. ER061:10-11; ER062:12-13. But the answer to this question was already clear on the face of the document—not to mention the fact that it had already been widely distributed. The district court's reasoning relies wholly on the false premise that the re-publication of the Watch List *could have* threatened national security—which, again, it could not have. The FBI did not need to investigate or open a file on Antiwar.com or its backers to make this determination.

This rule would not stop the government from investigating leaks that actually pose a threat to national security. The government may still lawfully investigate unauthorized disclosures, and, under *MacPherson*, journalists may still be incidentally surveilled as part of those efforts. But there is a substantial difference between the incidental surveillance of a journalist in the context of a legitimate investigation into a leaker of classified information, and the investigation of a journalist herself based solely on publication of an unclassified document that, on its face, presents no such threat. Moreover, the rule advanced here would not stop the government from investigating

journalists who published materials that in fact threatened national security. This approach would simply define the targets more sharply, while protecting the free press and precluding investigations into journalists who neither harmed nor threatened national security, but simply pursued their craft, as protected by the First Amendment.

IV. CONCLUSION

For the foregoing reasons the District Court's opinion should be reversed.

Dated: August 3, 2018

COOLEY LLP

/s/ *Adam Gershenson*
Adam Gershenson

Attorneys for Amicus Curiae
FIRST AMENDMENT COALITION

CERTIFICATE OF COMPLIANCE

I certify that pursuant to Federal Rules of Appellate Procedure 29, 32(a)(5), and 32(a)(7), the foregoing *amicus curiae* brief is proportionally spaced, has a typeface of 14 point Times New Roman, and contains 6,442 words, excluding those sections identified in Fed. R. App. P. 32(f).

Dated: August 3, 2018

COOLEY LLP

/s/ *Adam Gershenson*
Adam Gershenson

Attorneys for Amicus Curiae
FIRST AMENDMENT COALITION

CERTIFICATE OF SERVICE

I certify that on August 3, 2018, the foregoing *amicus curiae* brief was served on all parties or their counsel of record through the CM/ECF system.

Dated: August 3, 2018

COOLEY LLP

/s/ *Adam Gershenson*
Adam Gershenson

Attorneys for Amicus Curiae
FIRST AMENDMENT COALITION