NO. 15-50759

DEFENSE DISTRIBUTED, et al.,
Plaintiffs-Appellants,

v.

UNITED STATES DEPARTMENT OF STATE, et al.,
Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS, AUSTIN DIVISION

No. 1:15-cv-00372-RP
The Hon. Robert L. Pitman
United States District Court Judge

AMICI CURIAE BRIEF OF THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS AND THE THOMAS JEFFERSON CENTER FOR THE PROTECTION OF FREE EXPRESSION IN SUPPORT OF APPELLANTS

J. Joshua Wheeler
THOMAS JEFFERSON CENTER FOR THE PROTECTION OF FREE EXPRESSION &
THE UNIVERSITY OF VIRGINIA SCHOOL OF LAW
FIRST AMENDMENT CLINIC
400 Worrell Drive
Charlottesville, VA 22911
Telephone: (434) 295–4784
jjw@tjcenter.org

Bruce D. Brown
Counsel of Record
Gregg P. Leslie
Hannah Bloch-Wehba
REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
bbrown@rcfp.org

CERTIFICATE OF INTERESTED PERSONS

Defense Distributed, et al. v. *U.S. Dep't of State, et al.*, No. 15-50759

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici* disclose that:

The Reporters Committee for Freedom of the Press is an unincorporated nonprofit association of reporters and editors with no parent corporation and no stock.

The Thomas Jefferson Center for the Protection of Free Expression is a nonprofit organization with no parent corporation and no stock.

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this Court may evaluate possible disqualification or recusal.

Plaintiffs:
Defense Distributed, Second Amendment Foundation, Inc.

Defendants:
U.S. Dep't of State, John F. Kerry, Directorate of Defense Trade Controls, Kenneth B. Handelman, C. Edward Peartree, Sarah J. Heidema, Glenn Smith

Plaintiffs' Counsel:
Alan Gura, Gura & Possessky, PLLC; Matthew A. Goldstein, Matthew A. Goldstein, PLLC; William B. Mateja, William T. "Tommy" Jacks, David Morris, Fish & Richardson P.C.; Josh Blackman

Defendants' Counsel:
Loretta Lynch, Michael S. Raab, Daniel Bentele Hahs Tenny, Eric J. Soskin, Stuart

J. Robinson, Richard L. Durban, Benjamin C. Mizer, Anthony J. Coppolino, Zachary C. Richter – U.S. Department of Justice

Amici Curiae: Reporters Committee for Freedom of the Press; Thomas Jefferson Center for the Protection of Free Expression

Counsel for *Amici*: Bruce D. Brown, Gregg P. Leslie, Hannah Bloch-Wehba – Reporters Committee for Freedom of the Press; J. Joshua Wheeler – Thomas Jefferson Center for the Protection of Free Expression

/s/ Bruce D. Brown
Bruce D. Brown
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
bbrown@rcfp.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

REGULATIONS

STATEMENT OF INTEREST OF *AMICI CURIAE*[1]

The Reporters Committee for Freedom of the Press and the Thomas Jefferson Center for the Protection of Free Expression submit this *amici curiae* brief in support of Petitioners-Appellants.

The Reporters Committee for Freedom of the Press is an unincorporated nonprofit association of reporters and editors that works to safeguard the First Amendment's guarantee of a free and unfettered press, and the public's right to be informed, through the news media, about the government. The Reporters Committee has provided guidance and research in First Amendment and freedom of information litigation since 1970.

The Thomas Jefferson Center for the Protection of Free Expression is a nonprofit, nonpartisan organization located in Charlottesville, Virginia. Founded in 1990, the Center has as its sole mission the protection of free speech and press. The Center has pursued that mission in various forms, including the filing of *amici curiae* briefs in this and other federal courts, and in state courts around the country.

[1] Pursuant to Rule 29(c)(5) of the Federal Rules of Appellate Procedure, *amici* state that no party's counsel authored this brief in whole or in part, and no party, party's counsel, or any other person, other than the *amici curiae*, their members, or their counsel, contributed money that was intended to fund preparing or submitting the brief. Pursuant to Rule 29(c)(4), all parties have consented to the filing of this brief.

This case is of particular importance to *amici* because the district court below erred in holding that the Arms Export Control Act ("AECA"), Pub. L. 94-329, tit. II, 90 Stat. 729 (1976), 22 U.S.C. § 2751 et seq., and its implementing regulations, the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. §§ 120–130, do not violate the First Amendment.

SUMMARY OF ARGUMENT

This case arises out of Plaintiffs' challenge to the constitutionality of the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. §§ 120–130, which purport to require Plaintiffs to obtain a license before publishing certain information allegedly related to national defense on the Internet. The Arms Export Control Act ("AECA"), Pub. L. 94-329, tit. II, 90 Stat. 729 (1976), 22 U.S.C. § 2751 et seq., regulates the trade of "defense articles and defense services." *Id.* § 2778(a)(1). The Act's implementing regulations, the ITAR, include the United States Munitions List ("USML"), 22 C.F.R. § 121.1, the list of all defense articles, services, and related "technical data" whose "export" requires a license. *See id.* § 121.1(b)(2) ("Most U.S. Munitions List categories contain an entry on technical data . . . ."). The ITAR requires that a person who wishes to export "technical data" first "obtain the approval of the Directorate of Defense Trade Controls," the component of the Department of State that administers the regulations. 22 C.F.R. § 123. Violation of the AECA is a criminal offense punishable by a fine up to $1 million, twenty years in prison, or both. 22 U.S.C. § 2778(c).

At issue in this case is the constitutionality of the licensing requirement for exporting "technical data." The decision below erroneously "conflates two distinct but related limitations that the First Amendment places on government regulation of speech," *Reed v. Town of Gilbert, Ariz.*, 135 S.Ct. 2218, 2230 (2015),

concluding that because the ITAR's ban on unlicensed export of "technical data" is a viewpoint-neutral speech restriction, it is content-neutral as well. As the Supreme Court explained in *Town of Gilbert*, however, restrictions may be impermissibly content-based despite being viewpoint-neutral. The decision below failed to account for this possibility and thus failed to impose the appropriate standard of scrutiny in analyzing the restrictions at issue here.

Second, the ITAR's restrictions on the "export" of "technical data" are both overbroad and vague. The AECA and ITAR are overbroad because they burden significant amounts of speech protected by the First Amendment, including reporting and online journalism. The ITAR's definitions of the terms "export" and "technical data" reach far beyond the ordinary meaning of those words, and unquestionably tread on lawful speech and publication acts. The AECA and ITAR also allow the government practically unfettered discretion as to the scope of proscribed activity, and exempt government decision-making from judicial review. Even on its own terms, the ITAR presents practically unlimited definitions of "technical data" and "export" that are incomprehensible to reasonable citizens. As a result, the ITAR threatens to punish not only legitimate trade violations but substantial amounts of protected speech as well.

INTRODUCTION

At issue in this case are a broad and sweeping set of regulations that purport to criminalize the dissemination of certain "technical data" without a license. Although the statute and regulations at issue in this case are meant to curb the unauthorized import and export of arms and other defense articles, they also restrict the dissemination of "related technical data" without a license. This restraint is an unlawful content-based speech restriction. *See infra* pp. 4–10.

Even more troubling, however, is the government's assertion of broad and sweeping authority to punish protected speech that happens to include "technical data." The overbroad and vague definitions of "export" and "technical data" appear to cover lawful publication of journalism on important matters of public interest, including reporting on the United States' drone programs, *see infra* p. 17, North Korean nuclear enrichment, *see infra* pp. 18–19, or even medical breakthroughs using iron powder, *see infra* p. 19. Although the Defendants have not sought to apply these regulations to journalists or reporters, the government appears to possess unfettered discretion under the regulations to do so. The absence of judicial review raises further concerns that an already overbroad regulatory regime may be applied to limit First Amendment-protected speech in an unlawful manner. *Amicus* writes to emphasize that the regulations at issue here deter protected speech on important matters of public concern.

ARGUMENT

I. The AECA and ITAR are content-based regulations of speech.

The Arms Export Control Act ("AECA") controls the "import and the export of defense articles and defense services." 22 U.S.C. § 2778(a)(1). Items designated as "defense articles and defense services" comprise the United States Munitions List (the "Munitions List"), a part of the International Traffic in Arms Regulations ("ITAR"), the implementing regulations for the AECA. The President has delegated his authority to designate "defense articles and services" to the State Department. Exec. Order No. 11,958, 42 Fed. Reg. 4311 (Jan. 18, 1977).

The Munitions List is a long list of "articles, services and related technical data," the export of which is proscribed without a license. 22 C.F.R. § 121.1. "Technical data" is information "required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles," specifically including "blueprints, drawings, photographs, plans, instructions or documentation." 22 C.F.R. § 120.10; *see also id.* at § 121.1(I)(i) (defining as "technical data" any data "directly related to the defense articles described in paragraphs (a) through (h) of this category," including data related to rifle scopes and "cylinders"); *id.* § 121.1(II)(k) (using a similar definition, which in Category II includes data concerning tooling and "diagnostic instrumentation").

It is undisputed that "technical data" can amount to protected speech. As a result, the court below was correct in finding that the ITAR "unquestionably regulates speech concerning a specific topic." ROA.691. Nonetheless, the court went on, "The ITAR does not regulate disclosure of technical data based on the *message* it is communicating." *Id.* As a result, the court concluded that the ITAR is not content based because the regulations are "intended to satisfy a number of foreign policy and national defense goals." *Id.*

The court's conclusion that a regulation is content neutral so long as it is not based on message has no foundation. "A speech regulation targeted at specific subject matter is content based even if it does not discriminate among viewpoints within that subject matter." *Reed v. Town of Gilbert, Ariz.*, 135 S. Ct. 2218, 2230 (2015). *Town of Gilbert* recognizes that laws that "single[] out specific subject matter for differential treatment," as ITAR does, are facially content based and subject to strict scrutiny. *Id.*

ITAR creates numerous distinctions on the basis of the content of protected speech. The regulations distinguish "technical" data from data that is presumably "nontechnical," and proscribe the unlicensed publication only of technical data "related" to designated defense articles. 22 C.F.R. § 121.1 ("Most U.S. Munitions List categories contain an entry on technical data . . . and defense services . . . related to the defense articles described in that U.S. Munitions List category."). As

in *Town of Gilbert*, the regulation at issue here singles out and distinguishes types of speech that are permissible from those that are not. 22 C.F.R. § 120.10 (distinguishing "technical data" from information "commonly taught" in institutions of learning, "information in the public domain," "basic marketing information," or "general system descriptions of defense articles") (*cf. Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2663 (2011) (statutory exemption permitting "educational communications" but not marketing was facially content-based)).

ITAR is also fundamentally unlike content neutral regulatory schemes that the Fifth Circuit has previously upheld. Last year, this Court upheld a provision of the New Orleans Code requiring a license for a person to charge for tours of City points of interest and historic sites, concluding that the licensing requirement "has no effect whatsoever on the content of what tour guides say." *Kagan v. City of New Orleans, La.*, 753 F.3d 560, 562 (5th Cir. 2014) *cert. denied*, 135 S. Ct. 1403 (2015). In contrast, the regulations at issue here are explicitly designed to affect the content of speech that includes technical data.

Likewise, in 2012, this Court upheld provisions of the Texas Open Meetings Act that criminalized discussion of public matters by a quorum of public officials outside of an open meeting, finding that the statute was content neutral because its "purpose is to control the secondary effects of closed meetings." *Asgeirsson v. Abbott*, 696 F.3d 454, 461 (5th Cir. 2012). This Court distinguished the Act,

which "is applicable only to private forums and is designed to *encourage* public discussion," from content based regulations that discourage protected speech in public forums. *Id.* (citing *Burson v. Freeman*, 504 U.S. 191 (1992)). In contrast, the ITAR unquestionably applies to restrict speech on specific topics in public forums, and operates to deter, not encourage, expression. *See* ROA.689 (acknowledging that the World Wide Web is a public forum). As a result, although the ITAR is intended to address the export of defense articles and services, its restrictions on "technical data" unquestionably have a substantial effect on expression and speech as well.

Likewise, this Court should reverse the District Court's conclusion that the ITAR is content neutral because it "does not regulate disclosure of technical data based on the *message* it is communicating." ROA.691. The District Court's approach flouts the constitutional rule that "[t]he First Amendment's hostility to content-based regulation extends not only to restrictions on particular viewpoints, but also to prohibition of public discussion of an entire topic." *Consolidated Edison Co. of N.Y. v. Public Serv. Comm'n of N.Y.*, 447 U. S. 530, 537 (1980). Similarly, the Ninth Circuit's conclusion that the ITAR is content neutral because it "defines the technical data based on its *function* and not its viewpoint" contravenes the express holding in *Town of Gilbert*. *United States v. Chi Mak*, 683 F.3d 1126, 1135 (9th Cir. 2012). Nor can the regulations be saved by their

purported overall purpose: a government's purpose is not relevant to the interpretation of a facially content-based regulation. *Town of Gilbert*, 135 S.Ct. at 2228 ("That is why we have repeatedly considered whether a law is content neutral on its face *before* turning to the law's justification or purpose.").

Finally, because the ITAR is a content-based regulation that requires licensing, it is a classic prior restraint and requires adequate safeguards under *Freedman v. Maryland*, 380 U.S. 51 (1965). Content-based licensing requirements such as the one at issue here must satisfy demanding requirements:

> (1) any restraint prior to judicial review can be imposed only for a specified brief period during which the status quo must be maintained;
>
> (2) expeditious judicial review of that decision must be available; and
>
> (3) the censor must bear the burden of going to court to suppress the speech and must bear the burden of proof once in court."

Thomas v. Chicago Park Dist., 534 U.S. 316, 321 (2002) (citing *Freedman v. Maryland*, 380 U.S. at 58–60).

The ITAR cannot satisfy these requirements because it explicitly limits the availability of judicial review. Under the AECA and ITAR, the Directorate of Defense Trade Controls ("DDTC"), a component of the State Department, has discretion to treat nearly any piece of research as technical data, and these decisions "shall not be subject to judicial review." 22 U.S.C. § 2778(h).

This unreviewable use of discretion allows the DDTC to treat many types of research as technical data subject to export controls. For example, the DDTC has brought enforcement actions against companies on the basis that physics modeling software is technical data, since it could possibly be used for weapons development. *See, e.g.*, Proposed Charging Letter, Analytical Methods, Inc. (Dec. 19, 2008), *available at* https://goo.gl/H7YpTs. Further, the DDTC considers technical data to include information about ammunition for any firearm up to and including .50 caliber—thus, ITAR bans the unlicensed dissemination even of information on bullets for a standard home-defense handgun. *See* 22 C.F.R. § 121.1(III)(e). ITAR also bans the publication of "technical data" about face paints, helmets, goggles, and visors. *See id.* § 121.1(X)(e). In short, the USML includes not only seemingly everything that could to any degree be connected with the military, but also any "technical data" about those same things.

II. The AECA and ITAR are unconstitutionally overbroad and vague.

The AECA and ITAR are overbroad because they levy criminal and civil penalties upon the unlicensed "export" of "technical data" without adequately defining those terms to ensure that legitimate speech goes unpunished.

"The objectionable quality of vagueness and overbreadth does not depend upon the absence of fair notice to a criminally accused or upon unchanneled

delegation of legislative powers, but upon a danger of tolerating, in the area of First Amendment freedoms, the existence of a penal statute susceptible of sweeping and improper application." *NAACP v. Button*, 371 U.S. 415, 432–33 (1963). The AECA and ITAR present precisely this danger.

A. ITAR's sweeping definitions of "technical data" and "export" reach substantial amounts of protected expression and do not adequately describe the conduct proscribed by the regulations.

The AECA's criminalization of the unlicensed "export" of "technical data" is unconstitutionally overbroad because the key terms "export" and "technical data" reach significant amounts of protected speech.

To satisfy an overbreadth challenge, a plaintiff must show that the challenged statute is not subject to a narrowing construction and has a real and substantial deterrent effect on legitimate expression. *Erzonznik v. City of Jacksonville*, 422 U.S. 205, 216 (1975); *see also United States v. Stevens*, 559 U.S. 460, 474 (2010) (stating that the first step of an overbreadth challenge is to determine the scope of the law at issue). Criminal statutes, such as those at issue here, "that make unlawful a substantial amount of constitutionally protected conduct may be held facially invalid even if they also have a legitimate application." *City of Houston v. Hill*, 482 U.S. 451, 459 (1987).

A law is unconstitutionally vague if it does not "give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may

act accordingly." *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). The Supreme Court has held that "the general test of vagueness applies with particular force in review of laws dealing with speech." *Hynes v. Mayor & Council of Oradell*, 425 U.S. 610, 620 (1976). In *Hynes*, the Court reasoned that the importance of the "free dissemination of ideas" was such that a heightened standard for clarity was appropriate. *Id.*; *see also Connally v. General Construction Co.*, 269 U.S. 385, 391 (1926) (noting that a statute is vague when "men of common intelligence must necessarily guess at its meaning and differ as to its applications").

The State Department, which implements ITAR, has interpreted the term "export" broadly, to include publication on the Internet: "providing technical data on a publicly accessible network, such as the Internet, is an export because of its inherent accessibility to foreign powers." Defs.' Opp. to Pl.'s Mot. for Preliminary Inj. at 3 n.2, 1:15-cv-00372-RP (June 10, 2015), ECF No. 132. As an initial matter, it is evident that the term "export" touches on First Amendment freedoms. DDTC has defined "export" to include "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad." 22 C.F.R. § 120.17(a)(4). As applied to goods such as defense articles, it is unambiguous that the word "export" "does not require proof that the goods actually arrived in the foreign country." *See United States v. Huynh*, 246

F.3d 734, 741 (5th Cir. 2001) ("Exportation occurs when the goods are shipped to another country with the intent that they will join the commerce of that country, not when they arrive in that country."). While the District Court concluded that "persons of ordinary intelligence are clearly put on notice by the language of the regulations" that online publication "would fall within the definition of export," ROA.702, that definition strays considerably from the ordinary meaning of the word.

As a result, there is no question that the State Department has not offered a narrowing construction of "export" that would save the statute. *See Village of Hoffman Estates et al. v. The Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 494 n.5 (1989) ("In evaluating a facial challenge to a state law, a federal court must, of course, consider any limiting construction that a state court or enforcement agency has proffered."). Indeed, under proposed regulations, ITAR's definition of "export" would be expanded to expressly include "[m]aking technical data available via a publicly available network (*e.g.*, the Internet)." International Traffic in Arms, 80 Fed. Reg. 31,525, 31,535 (proposed June 3, 2015) (to be codified at 22 C.F.R. § 120.17(a)(7)). According to the Department, this proposed definition "makes more explicit the existing control in (a)(4)." *Id.* at 31,529. In other words, the State Department already reads "export" expansively, and its proposed rules are intended merely to codify this.

The definition of "technical data" is similarly overbroad. The DDTC controls the export of technical data largely through its maintenance of the USML, which describes what technology is subject to the AECA. Though many of the entries in the USML refer to actual military hardware, the Munitions List consistently includes technical data "related to" those articles. *See, e.g.*, 22 C.F.R. § 121.1(I)(i), (II)(k). In addition to specifically enumerating various types of technical data, the USML also broadly notes that technical data related to broad categories of "defense articles" considered "significant military equipment"—including explosives, propellants, and aircraft—are defense items themselves. *See id.* § 121.1(b). Further, the USML also includes a catch-all provision allowing the DDTC to include any article or technical data not otherwise listed which has "substantial military applicability." *Id.* § 121.1(XXI). Still further, the USML is not even an exhaustive list of export-controlled items but rather a "series of categories describing the *kinds* of items that qualify as 'defense articles' requiring export licenses." *United States v. Zhen Zhou Wu*, 711 F.3d 1, 12 (1st Cir. 2013) *cert. denied sub nom. Yufeng Wei v. United States*, 134 S. Ct. 365 (2013) (emphasis added).

Indeed, the very terms designed to limit the scope of the ITAR's restraint on publication of "technical data"—"required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or

modification of defense articles"—actually create an expansive definition that "sweeps within its prohibitions what may not be punished under the First and Fourteenth Amendments." *City of Rockford*, 408 U.S. at 113, 115 (upholding an antinoise ordinance because it "contains no broad invitation to subjective or discriminatory enforcement"); *see also Cox v. Louisiana*, 379 U.S. 536, 5512 (1965) (striking down a Louisiana criminalizing "breach of the peace". In its proposed rule, the Department of State notes, "'Required' is used in the definition of 'technical data' and has, to this point, been an undefined term in the ITAR." 80 Fed. Reg. at 31,527. The proposed new definition of "required" in the NPRM remains quite vague, and "explicitly includes information for meeting not only controlled performance levels, but also characteristics and functions." *Id.* As DDTC explains in relation to the example of controlled "bomber" aircraft," "The characteristic of the aircraft that is controlled is that it is a bomber, and therefore, any 'technical data' peculiar to making an aircraft a bomber is 'required.'" *Id.* This explanation hardly clarifies or limits the scope of the definition.

Moreover, while the District Court was correct that "at least two circuits have rejected due process challenges to the AECA and ITAR, and upheld criminal convictions for its violation," both of those circuits considered the vagueness of the statute as applied to export of defense articles, not technical data comprising speech. *See Zhen Zhou Wu*, 711 F.3d at 12 (denying vagueness challenge to ITAR

as applied to defendants convicted of unlicensed export of phase shifters); *United States v. Hsu*, 364 F.3d 192, 198 (4th Cir. 2004) (denying vagueness challenge as applied to defendants convicted of conspiracy to violate ITAR by exporting encryption devices); *but see also Chi Mak*, 683 F.3d at 1135–36 (reviewing vagueness claim related to "technical data" provision for plain error). In contrast, the "technical data" provision clearly implicates First Amendment rights, and courts cannot assume that the government will exercise its prosecutorial discretion with a careful eye toward not violating the First Amendment. *NAACP v. Button*, 371 U.S. at 438 ("Precision of regulation must be the touchstone in an area so closely touching our most precious freedoms.").

On top of these definitions, ITAR offers exceptions for general scientific principles "commonly taught in schools, colleges, and universities or information in the public domain." 22 C.F.R. § 120.10(b). The "public domain exception" covers research from accredited universities that is ordinarily published and shared in the field. *Id.*; *id.* at § 120.11 (defining "public domain"). In proposed amendments to ITAR, the Department of State has recognized that the exception is "unnecessarily limiting in scope and insufficiently flexible with respect to the continually evolving array of media, whether physical or electronic, through which information may be disseminated." 80 Fed. Reg. 31527.

B. The broad restraints on "export" of "technical data" appear to apply to significant amounts of protected speech.

Under the ITAR, posting "technical data" to a domestic website, or publishing the same information in a domestic publication, becomes an "export" under the AECA whenever a foreign citizen reads that information. This definition raises serious First Amendment concerns, as it suggests that publication of facts lawfully obtained may be a violation of the ITAR. *See Bartnicki v. Vopper*, 532 U.S. 514, 528 (2001) ("[S]tate action to punish the publication of truthful information seldom can satisfy constitutional standards."), *citing Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 102 (1979).

For example, when an online news outlet publishes "technical data" which it has "lawfully obtained," but which is not in the public domain, the capacious definition of "export" suggests that publication is a violation of export controls. In 2013 technology reporters at CNET published an article relating to the Predator drones used by the U.S. Military. Declan McCullagh, *DHS Built Domestic Surveillance Tech into Predator Drones*, CNET (Mar. 2, 2013), http://www.cnet.com/news/dhs-built-domestic-surveillance-tech-into-predator-drones/. Although the Department of Homeland Security had offered a redacted document listing performance requirements for unmanned surveillance drones in response to a Freedom of Information Act request, the article included a link to an "unredacted copy" of that same document that CNET had obtained lawfully. *Id.* If the unredacted copy included "technical data," CNET's publication would appear

to constitute an ITAR violation. At the same time, the technical specifications of the drone were central to the article, which considered whether the DHS was using or developing technology that would enable domestic surveillance. *Id.* Likewise, search engines, research databases, library catalogs, and other online resources that include links to "technical data" may "export" that information by making it available to users abroad.

Similarly, in 2013, the Arms Control Wonk blog published a post by R. Scott Kemp, Norman C. Rasmussen Assistant Professor of Nuclear Science and Engineering at the Massachusetts Institute of Technology, republishing photographs of Kim Jong-un's trip to a factory that may be used to manufacture centrifuges. R. Scott Kemp, *Is This Where North Korea Makes Its Centrifuges?* Arms Control Wonk (June 24, 2013), *available at* www.armscontrolwonk.com/archive/206637/is-this-where-north-korea-makes-its-centrifuges/. The post included photographs and discussion of flow-forming machines that are "the only way to manufacture the thin-walled P-2 centrifuge rotor on which the North Korean enrichment program is thought to be built." *Id.* The post describes the flow-forming machine as "part of an assembly-line fabrication process for making thin-walled components" for centrifuges. *Id.*

The plain text of the ITAR indicates that the information included in Professor Kemp's blog post, although general and speculative, may be "technical

data." It is clear that the photographs in the post include information "required" for the design, operation, or manufacture of a centrifuge, which is "specifically designed or modified for use in the design, development, or fabrication of nuclear weapons or nuclear explosive devices." 22 C.F.R. § 120.10 (defining "technical data" as information "required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles," specifically including "blueprints, drawings, photographs, plans, instructions or documentation"); *id.* § 121.1(XVI) ("Nuclear Weapons, Design and Testing Related Items"). In this case, photographs of machines required for the manufacture of centrifuges, although obtained from a publicly available source, may not be within ITAR's "public domain exception" because they were republished online from North Korean state media, not available "through sales at newsstands and bookstores," through subscriptions, or through "second class mailing privileges." *Id.* § 120.11.

The State Department's construction of "technical data" discourages the press from discussing matters of great public importance, even if unrelated to defense. For example, iron may be used to detect certain forms of cancer, whether by utilizing it or by measuring it in the body. *See, e.g.*, Mukesh G. Harisinghani et al., *Noninvasive Detection of Clinically Occult Lymph-Node Metastases in Prostate Cancer*, 348 NEW ENG. J. MED. 2491 (2003); Richard G. Stevens et al.,

Body Iron Stores and the Risk of Cancer, 319 NEW ENG. J. MED. 1047 (1988). At the same time, the USML includes "[i]ron powder . . . with a particle size of 3 micrometers or less produced by reduction of iron oxide with hydrogen." 22 C.F.R. § 121.1(V)(c)(4)(i)(B). A journalist covering innovations in healthcare who wants to report on unpublished research concerning iron powder's utility in cancer treatment may be unable to do so under the ITAR. And courts may not assume that, should the reporter be prosecuted for this violation, her constitutional rights would be properly vindicated in the course of her defense. *See Dombrowski v. Pfister*, 380 U.S. 479, 486 (1965) ("When the statutes also have an overbroad sweep . . . the hazard of loss or substantial impairment of [First Amendment] rights may be critical. . . . The assumption that defense of a criminal prosecution will generally assure ample vindication of constitutional rights is unfounded in such cases.").

Indeed, the proposed changes to ITAR make clear that "the *further* dissemination of 'technical data' or software that was made available to the public without authorization is a violation of the ITAR if, and only if, it is done with knowledge that the 'technical data' or software was made publicly available without an authorization." 80 Fed. Reg. at 31,528 (emphasis added). This interpretation of ITAR touches on significant amounts of protected expression. *Hill*, 482 U.S. at 459. A regulation that criminalizes news coverage of facts that

are lawfully obtained but that comprise "technical data" runs counter to the First Amendment. *Cf. Daily Mail Pub. Co.*, 443 U.S. at 103 ("[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.").

That the plain language of ITAR's prohibition on unlicensed export of "technical data" would suppress speech like that in Professor Kemp's blog post illustrates the overbreadth problem that inheres in the ITAR. The sweeping definitions of the terms "export" and "technical data" are further amplified when the two are read together, creating a real and substantial deterrent effect on speech. The substantiality of a deterrent effect is judged by the number of unconstitutional applications in relation to the statute's "plainly legitimate sweep." *Washington State Grange v. Washington State Republican Party*, 552 U.S. 442, 449 n.6 (2008); *see also United States v. Williams*, 553 U.S. 285, 292 (2008). This deterrence affects not only researchers and members of the defense community, but also the public more broadly, especially the press.

III. The AECA and ITAR provide the DDTC with unlimited, unreviewable discretion to enforce the law.

The district court also erred in determining that the ITAR and AECA are not impermissibly vague. Indeed, under this regulatory scheme, no reasonable citizen

could predict whether a particular piece of information regarding the design, operation, repair, or testing of "defense articles" is "required" for that task, and thus whether it is covered by the AECA and ITAR.

A statute may be vague if it gives too much discretion to the party that enforces it. In *Cramp v. Board of Public Instruction*, the Supreme Court invalidated a Florida statute that required state employees to swear an oath that they had never supported the Communist Party. 368 U.S. 278, 279 (1961). The Court explained that the oath was vague partly because it lacked any "terms susceptible of objective measurement." *Id.* at 286. This deficiency provoked the Court to note that the oath allowed prosecution for "guiltless knowing behavior" at the decision of those "always ready to affix a Communist label upon those whose ideas they violently oppose." *Id.* at 287. Because the statute could be used to prosecute guiltless behavior at the prosecutor's whim, it was unconstitutionally vague. *Id.*; *see also National Endowment of the Arts v. Findley*, 524 U.S. 569, 588 (1998) (finding that the First Amendment protects people from "arbitrary and discriminatory enforcement of vague standards"); *Baggett v. Bullitt*, 377 U.S. 360 (1964) (invalidating another oath statute on similar grounds). The vagueness standard applies with particular force to statutes that affect First Amendment rights. *See Village of Hoffman Estates*, 455 U.S. at 498 (1982).

The AECA and ITAR are vague under both formulations of the standard. As discussed above, the statutory terms "technical data" and "export" do not adequately inform a citizen regarding what conduct they cover. Because the DDTC has effectively unlimited discretion in applying these terms to specific conduct, the AECA and ITAR are unconstitutionally vague.

A. The definitions of "technical data" and "export" in the ITAR do not provide explicit enforcement standards to the DDTC.

The AECA and ITAR confer unbridled discretion on the DDTC to enforce them. Specifically, the DDTC has complete control over the USML. "The designation by the President (or by an official to whom the President's functions under subsection (a) have been duly delegated), in regulations issued under this section, of items as defense articles or defense services for purposes of this section *shall not be subject to judicial review*." 22 U.S.C. § 2778(h) (emphasis added).

Nonetheless, the DDTC's unilateral and unreviewable discretion with regard to the contents of the USML, and thus with regard to the content of the term "technical data," means the AECA lacks explicit standards to govern the proscribed conduct.

The AECA and ITAR are also vague with respect to the term "export" because they give the DDTC unlimited discretion to decide what activities are covered. Although the definition of "export" facially covers any disclosure or transfer of export-controlled information to a foreign person, in the instant case the

DDTC has interpreted this to include mere publication to the Internet. If such publication is a fair interpretation of the AECA and ITAR, then almost any Internet posting is subject to government censorship. Further, because the definition turns on whether the information is received by a "foreign person," even a purely domestic, traditional publication might qualify as an "export" if it is read by a foreign citizen on United States soil. Given this construction of the term, the DDTC has virtually unlimited discretion to selectively pursue prosecutions under the AECA and ITAR for unlawful "export" of "technical data."

As long as the DDTC may treat any publication that could be read by a foreign citizen as an "export" under the statute, that agency has broad license to quash publications of all sorts. For example, whether a journalist or other Internet user may post an article to a website discussing the moral, ethical, and legal implications of certain cluster bombs that purport to be 99 percent effective is unclear. *See, e.g.*, Bryan Schatz, *How US Cluster Bombs Banned by Most Countries Ended Up in Yemen*, Mother Jones (Jun. 9, 2015), http://bit.ly/1QIYwS8 (describing the Textron CBU-105 Sensor Fuzed Weapon). Under the AECA, the permissibility of publication would turn on whether the article is available to a foreign national.

Nor does the Government's suggestion that a publisher's liability can be limited by taking steps to locate users based on Internet Protocol addresses resolve

this issue. Defs.' Opp. to Pl.'s Mot. for Preliminary Inj. at 3 n.2, 1:15-cv-00372-RP (June 10, 2015), ECF No. 132. Even if a journalist manages to ensure that her publication is not available overseas, access by a foreign national on domestic soil may still qualify as a violation of the statute. Although the DDTC has generally not prosecuted such cases, nothing in the AECA or ITAR prevents it from doing so. *Cf. United States v. Roth*, 628 F.3d 827, 830–32 (6th Cir. 2011) (affirming professor's conviction of ITAR violations, partly on grounds that he allowed graduate research assistants who were foreign nationals access to technical data); *see also United States ex rel. McGrath v. Microsemi Corp.*, No. CV-13-00854-PHX-DJH, 2015 WL 6121568, at *10–11, *40–43 (D. Ariz. Sept. 30, 2015) (treating access to ITAR-controlled technical data by foreign employees as a possible violation of ITAR, though the court ultimately held there was no violation on the facts of the case). Consequently, journalists writing about technical aspects of defense issues—or, given the instant case, even gun control—risk receiving a cease and desist letter or criminal charges at the DDTC's sole discretion.

B. The absence of judicial review exacerbates the ITAR's overbroad sweep by obscuring the distinction between "permissible" journalism and prohibited speech.

Taken together, these broad definitions unquestionably reach protected speech, but the AECA also provides that executive branch decisions to add or remove an item from the USML "shall not be subject to judicial review." 22

U.S.C. § 2778(h). The Ninth Circuit has held that this portion of the statute provides the DDTC with the ability to decide whether documents are "technical data" subject to export controls. *United States v. Chi Mak*, 683 F.3d 1126, 1132 (9th Cir. 2012) (holding that the AECA "expressly prohibits judicial review" of such decisions).

Partly as a result of the absence of judicial review, it is difficult to establish bright lines between prohibited disclosures of "technical data," on the one hand, and permissible journalistic coverage of scientific and technological issues, on the other. *See Button*, 371 U.S. at 438 (highlighting the importance of clarity in laws affecting the First Amendment). The absence of judicial review only exacerbates the First Amendment problems, because the question of whether an online publication constitutes protected speech or "technical data" is not one that may be left to the executive branch to decide. Infringements of First Amendment rights are quintessentially judicial questions. *See Williams v. Rhodes*, 393 U.S. 23, 40 (1968) (Douglas, J., concurring) ("First Amendment rights . . . have a well-established claim to inclusion in justiciable, as distinguished from 'political,' questions . . . ."). The statute's provision regarding the unreviewable authority to designate "defense articles" therefore should not extend to the definition of "technical data," which includes a significant amount of protected speech.

This confluence of the DDTC's unilateral and unreviewable discretion to establish sweeping export prohibitions, on one hand, and overly narrow exceptions to the AECA, on the other, means that the DDTC has an effective veto over online publication of any information it considers to be in some way defense related. This complete control and wide discretion present a real, substantial deterrent to those seeking to discuss or report on matters of technology.

CONCLUSION

For the foregoing reasons, *amici curiae* respectfully urge this Court to reverse.

/s/ Bruce D. Brown
Bruce D. Brown
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-face and volume limitations set forth in Fed. R. of App. P. 32(a)(7)(B) as follows: The type face is fourteen-point Times New Roman font, and the word count is 6,152, excluding the portions of the brief exempted by Rule 32(a)(7)(B)(iii).

/s/ Bruce D. Brown

Bruce D. Brown
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005

CERTIFICATE OF SERVICE

I hereby certify that on December 17, 2015, an electronic copy of the foregoing brief was filed with the Clerk of Court for the United States Court of Appeals for the Fifth Circuit using the Court's CM/ECF system and was served electronically by the Notice of Docket Activity upon all parties in the case. I certify that all participants in the case are CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Bruce D. Brown

Bruce D. Brown
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005