RICHARD R. WINTER, ESQ.
SARAH E. PACE, ESQ.
McBride Baker & Coles
500 West Madison Street
Chicago, IL 60661
(312) 715–5778

KARL OLSON, ESQ.; SBN 104760
Levy, Ram, Olson & Rossi
639 Front Street, 4th Floor
San Francisco, CA 94111
(415) 433–4949

JAMES WHEATON, ESQ.; SBN 115230
FIRST AMENDMENT PROJECT
1736 Franklin, 8th Floor
Oakland, CA 94612
(510) 208–7744

ROBERT CORN-REVERE, ESQ.
Hogan & Hartson, L.L.P.
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637–5600

Attorneys for Plaintiff
Daniel J. Bernstein

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF COMMERCE, et al.,

Defendants.

C 95–00582 MHP

PLAINTIFF'S MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT

Date: August 2, 2002
Time: 2:00 p.m.
Place: Courtroom 15, 18th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Regulations

Other materials

I. INTRODUCTION

Plaintiff Professor Daniel J. Bernstein ("Prof. Bernstein"), a graduate student when this case began, is now an established researcher helping protect the Internet against attack.[1] Cryptography, the science of protecting messages against eavesdropping and forgery, is a crucial part of Prof. Bernstein's work. Prof. Bernstein's cryptographic research aims at low-cost systems suitable for protecting communications among all Internet users.

The visible results of Prof. Bernstein's research are Internet-security instructions—often "software," i.e., instructions comprehensible to a computer. Prof. Bernstein's colleagues can read and improve the instructions. Users can follow the instructions to protect their Internet activities.

Ten years ago, the government censored Prof. Bernstein's "Snuffle."[2] The government appeared to believe that Snuffle might allow terrorists and other criminals to communicate in secret.[3] However, the tragic history of terrorist attacks over the past two decades[4] demonstrates that criminals were *already* capable of communicating in secret. Unbreakable cryptographic systems, suitable for communication among small groups of people, have been widely known for years.[5] The government's regulations were hurting scientists and legitimate users, while doing nothing to stop terrorists.

In January, 2000, finally recognizing the facts,[6] the government modified the Export Administration Regulations ("EAR"), 15 C.F.R. §§730 *et seq*., to allow publication of cryptographic software of any strength, subject to various limitations having no connection with cryptographic strength.

---

1 *See* Bernstein Decl., ¶¶3 *et seq*.

2 *See, e.g.,* Bernstein Decl., ¶¶88–100.

3 "The United States, through export restrictions, seeks to control the widespread foreign availability of cryptographic devices and software which might hinder its foreign intelligence collection efforts." Defendants' Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss, at 2 (1995).

4 *See* Plaintiff's Request for Judicial Notice.

5 *See* Schneier Decl., ¶¶3–13.

6 A government official recently put it this way: "We just have to realize we're living in a world where bad guys are going to get encryption, and there's nothing we can do from a policy perspective that's going to stop this." *See* Olson Decl., ¶9.

Unfortunately, those limitations, and other burdens imposed by the regulations, continue to interfere with Prof. Bernstein's work. Bernstein Decl., ¶¶108 *et seq*. EAR continues to hurt scientists and legitimate users, and it continues to do nothing to stop terrorists.

This Motion seeks, first, summary adjudication that EAR burdens speech; second, summary adjudication that EAR is content-based; third, summary judgment that EAR is an unconstitutional content-based regulation of speech. This Motion also seeks summary judgment that EAR is an unconstitutional prior restraint, that EAR is unconstitutionally overbroad, that EAR is unconstitutionally vague, that EAR is an unconstitutional regulation of association and assembly, and that EAR is an unconstitutional search and seizure.

II. PROCEDURAL HISTORY

In 1995, Prof. Bernstein filed a Complaint alleging that the licensing requirements in the International Traffic in Arms Regulations ("ITAR"), specifically ITAR's Category XIII(B) controls over cryptography, were unconstitutional, on their face and as applied to him.

This Court held that Prof. Bernstein's censored documents were speech under the First Amendment. *Bernstein v. Department of State et al.*, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996) ("Bernstein I") (denying defendants' motion to dismiss). The Court then held that, because the ITAR licensing scheme failed to provide various procedural safeguards, ITAR Category XIII(B) was an unconstitutional prior restraint. *Bernstein v. Department of State et al.*, 945 F. Supp. 1279, 1290 (N.D. Cal. 1996) ("Bernstein II").

The Commerce Department promptly issued new regulations, 61 Fed. Reg. 68572 (December 30, 1996), controlling "encryption items" under EAR. Prof. Bernstein filed a First Supplemental Complaint challenging the constitutionality of EAR.

The Court held that EAR's procedural safeguards were, "like the ITAR, woefully inadequate," and that EAR was an unconstitutional prior restraint. *Bernstein v. Department of State et al.*, 974 F. Supp. 1288, 1308 (N.D. Cal. 1997) ("Bernstein III"). The Court permanently enjoined Defendants from, *inter alia*, enforcing EAR against Prof. Bernstein "or anyone who uses, discusses or publishes or seeks to use, discuss or publish plaintiff's encryption program and related materials"; and from "threatening, detaining, prosecuting, discouraging or other-

wise interfering with plaintiff or any other person described ... above in the exercise of their federal constitutional rights as declared in this order." *Bernstein III*, 974 F. Supp. at 1311. The injunction was stayed pending appeal.

On appeal, the Ninth Circuit held that EAR was an unconstitutional prior restraint, because it "applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards." *Bernstein v. Department of Justice et al.*, 176 F.3d 1132, 1145 (9th Cir. 1999) ("Bernstein IV"), *reh'g en banc granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

Before the Ninth Circuit had an opportunity to hear the matter en banc, the Commerce Department announced plans to make significant changes to EAR. The changes were issued as 65 Fed. Reg. 2492 (January 14, 2000); the case was remanded to this Court.

Prof. Bernstein filed his Second Supplemental Complaint on January 7, 2002.

III. CURRENT REGULATORY FRAMEWORK AND IMPACT

A. Overview

The current Export Administration Regulations have the same overall framework as the regulations considered by this Court in *Bernstein III*. One major new exception is of direct relevance to this case.

EAR continues to regulate various types of information under the headings of (1) "software" and (2) "technology."[7] EAR continues to impose various prohibitions upon unlicensed transportation and disclosure of information,[8] although it continues to exempt "printed" publications.[9] Violators are subject to civil fines, criminal fines, and imprisonment.[10]

The major new exception is that information "is released from EI controls and may be exported or reexported without review" if all four of the following tests are simultaneously

---

7 *See* 15 C.F.R. §774, Supplement 1, ECCN 5D002; 5E002; 15 C.F.R. §772.1, definition of "technology". For the convenience of the Court, the relevant portions of the regulations, including the relevant definitions from 15 C.F.R. §772.1, are attached in numerical order as Olson Decl., Exhibits F(1) *et seq*.

8 *See, e.g.*, 15 C.F.R. §736.2(b)(1); §734.2(b)(4); §734.2(b)(5); §744.9(a).

9 15 C.F.R. §734.3(b)(2); §734.3(b)(3), Note.

10 15 C.F.R. §764.3.

met: (1) the information is "[e]ncryption source code controlled under ECCN 5D002"; (2) the information "would be considered publicly available under §734.3(b)(3) of the EAR"; (3) the information is not subject to certain commercial agreements; and (4) "you have submitted written notification to BIS of the Internet location (e.g., URL or Internet address) or a copy of the source code by the time of export."[11] A similar rule applies to "[o]bject code resulting from the compiling of" such "source code."[12]

To summarize the effects of the new exception: In situations where notifying the government is impractical or impossible, the new exception is inapplicable, and EAR continues to act as an outright prohibition. In situations where notifying the government is practical, but where the information is not "encryption source code" or "object code" or is not "publicly available," the new exception is also inapplicable, and EAR continues to act as a licensing scheme. In other situations, the new exception reduces EAR's effect from a licensing scheme to a notification requirement.

B. Definitions: "Software"

15 C.F.R. §772.1 defines "software" as "[a] collection of one or more 'programs' or 'microprograms' fixed in any tangible medium of expression," and defines "program" as "[a] sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer."

"Software" is controlled under 15 C.F.R. §774, Supplement 1, ECCN 5D002 if it is "[d]esigned or modified to use 'cryptography' employing digital techniques performing any cryptographic function other than authentication or digital signature," subject to certain minimum levels of cryptographic strength. *See* 5D002.c.1; 5A002.a.1. "Software" is also controlled under 5D002 if it is "[d]esigned or modified to perform cryptanalytic functions," or if it is "[d]esigned or modified to provide" certain high levels of computer security. *See* 5D002.c.1; 5A002.a.2; 5A002.a.6.

---

11 15 C.F.R. §740.13(e)(1); 65 Fed. Reg. 2492 (January 14, 2000); 67 Fed. Reg. 20630 (April 26, 2002) (changing name "BXA" to "BIS"). There is a similar exception for information subject to commercial agreements. 15 C.F.R. §740.17(b)(4)(i).

12 15 C.F.R. §740.13(e)(2); 65 Fed. Reg. 62600 (October 19, 2000).

"Software" is controlled for "EI" reasons under 5D002 if it is an "encryption item" formerly controlled under ITAR. 15 C.F.R. §772.1 defines "encryption items" to include "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR," and defines "encryption software" as "[c]omputer programs that provide capability of encryption functions or confidentiality of information or information systems. Such software includes source code, object code, applications software, or system software."

C. Definitions: "Technology," "Technical Data," and "Technical Assistance"

15 C.F.R. §772.1 defines "technology" as "[s]pecific information necessary for the 'development,' 'production,' or 'use' of a product. The information takes the form of 'technical data' or 'technical assistance.' " "Technical assistance" may "take forms such as instruction, skills training, working knowledge, consulting services" and may "involve transfer of 'technical data' "; and "technical data" may "take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories."

"Technology" is controlled under 15 C.F.R. §774, Supplement 1, ECCN 5E002 if it is "required" for the "development," "production," or "use" of "software" controlled by 5D002. *See* 5E002; 15 C.F.R. §774, Supplement 2, General Technology Note. 15 C.F.R. §772.1 defines "required" as "peculiarly responsible for achieving or extending the controlled performance levels, characteristics or functions."

D. Prohibition of Collaboration at Scientific Conferences

Scientific conferences in the United States and abroad provide Prof. Bernstein the opportunity to work collaboratively on various types of software with his foreign colleagues, face to face. *See* Bernstein Decl., ¶¶18–22, 122–128. Such collaborations are highly interactive, with new versions of software being continually created and exchanged. Bernstein Decl., ¶115.

EAR has three overlapping prohibitions upon collaborations involving "EI" software.

i. 15 C.F.R. §744.9(a): "Technical Assistance"

15 C.F.R. §744.9(a) prohibits U.S. persons from providing unlicensed "technical assistance … to foreign persons with the intent to aid a foreign person in the development or

manufacture outside the United States of encryption commodities and software that, if of United States origin, would be controlled for EI reasons under ECCN 5A002 or 5D002."

15 C.F.R. §744.9(a) has an exception "if the U.S. person providing the assistance" is "entitled to export" the software; 15 C.F.R. §740.13(e)(1) states that "EI" software, under certain circumstances, "may be exported" if "you have submitted written notification to BIS of the Internet location (e.g., URL or Internet address) or a copy of the source code *by the time of export*" (emphasis added). 15 C.F.R. §744.9(a) also has an exception for certain countries "provided the exporter has submitted to BIS a completed classification request *by the time of export*" (emphasis added).

However, even when Internet access is readily available, contemporaneous communication with the government during interactive face-to-face collaboration would significantly slow down the collaboration. *See* Bernstein Decl., ¶¶18–20, 115. Furthermore, Internet access at conferences is usually limited and sometimes nonexistent. *Id.*, ¶¶116, 117, 124.

15 C.F.R. §744.9(a) further states that "the mere teaching or discussion of information about cryptography . . . would not establish" the requisite intent. However, there is no exception for such discussions when the intent is established by other means.

ii. 15 C.F.R. §736.2(b)(1) and §736.2(b)(2): "Reexport"

15 C.F.R. §736.2(b)(1) and 15 C.F.R. §736.2(b)(2) prohibit unlicensed "reexport" of "any item of U.S.-origin," or of any foreign-made item incorporating more than a certain amount of "controlled U.S. content," if the item and destination are controlled.

"Reexport" includes any "release of technology or software subject to the EAR" to a foreign national outside the United States. 15 C.F.R. §734.2(b)(4). Any "release of technology or source code subject to the EAR to a foreign national of another country is a deemed reexport to the home country or countries of the foreign national." 15 C.F.R. §734.2(b)(5).

"Release" includes "[v]isual inspection by foreign nationals of U.S.-origin equipment and facilities," "[o]ral exchanges of information," and "application to situations abroad of personal knowledge or technical experience acquired in the United States." 15 C.F.R. §734.2(b)(3).

15 C.F.R. §736.2(b)(1) and 15 C.F.R. §736.2(b)(2), like 15 C.F.R. §744.9(a), apply to

activities outside the United States. They are much less broad than 15 C.F.R. §744.9(a) in that they do not apply to items having no controlled U.S. content. However, when a controlled item is created in the U.S. and brought to Canada,[13] its unlicensed "release" to a non-U.S., non-Canadian citizen is prohibited by 15 C.F.R. §736.2(b)(1).

15 C.F.R. §740.13(e)(1) states that "EI" software is, under certain circumstances, "released from EI controls" if "you have submitted written notification to BIS of the Internet location (e.g., URL or Internet address) or a copy of the source code *by the time of export*" (emphasis added). However, when Internet access is sufficiently limited, taking advantage of this exception is a significant burden. Bernstein Decl., ¶¶115–118.

A recent example illustrates both 15 C.F.R. §736.2(b)(1) and 15 C.F.R. §744.9(a); *see* Bernstein Decl., ¶¶122–128. Prof. Bernstein traveled to a conference in Canada. He used the travel time for conference preparations, including writing some new "EI" software on his laptop computer. He was unable to connect his laptop computer to the Internet before or during the conference. He wanted to show the software to, and potentially engage in related collaborations with, a colleague at the conference, who he believes is Irish. However, disclosure to an Irishman would have violated 15 C.F.R. §736.2(b)(1), and collaboration with an Irishman would have violated 15 C.F.R. §744.9(a). Prof. Bernstein refrained from these activities. Prof. Bernstein expects to encounter similar problems at future conferences.

iii. 15 C.F.R. §764.2(e): "Transfer"

15 C.F.R. §764.2(e) prohibits any "transfer . . . in whole or in part" of "any item . . . subject to the EAR, with knowledge that a violation" of EAR "has occurred, is about to occur, or is intended to occur in connection with the item." 15 C.F.R. §772.1 defines "knowledge" to include "not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence."

This prohibition makes Prof. Bernstein vicariously liable for the predictable actions of his colleagues. For example, if Prof. Bernstein discloses "EI" software or "technical data" to a

[13] EAR does not require licenses to "export" "EI" items to Canada. 15 C.F.R. §742.15(a).

foreign colleague, aware that his colleague probably intends to take the information back home before it has been released from "EI" controls, then Prof. Bernstein has violated 15 C.F.R. §764.2(e). Prof. Bernstein is aware that many of his foreign colleagues ignore EAR. Bernstein Decl., ¶119.

Unlike 15 C.F.R. §744.9(a) and the "reexport" prohibitions, 15 C.F.R. §764.2(e) covers conferences inside the United States. Prof. Bernstein is refraining from activities at such conferences accordingly. Bernstein Decl., ¶119.

E. Notification Requirement for Private Email

Using 15 C.F.R. §740.13(e)(1) to release information from "EI" controls requires disclosing the information to the government, either indirectly as an "Internet location" or directly as "a copy."

15 C.F.R. §740.13(e)(1) also requires that the information be "publicly available under §734.3(b)(3)." This means information that is "already published or will be published"; that arises during, or results from, "fundamental research"; that is "educational"; or that is included in certain patent applications.[14] When information does not result from "fundamental research" and is not "educational," making it "publicly available" requires disclosing it to the public.

These forced disclosures are an invasion of Prof. Bernstein's privacy. *See* Bernstein Decl., ¶¶132–134. To avoid this situation, Prof. Bernstein is generally refraining from private discussions related to "EI" information, except when he knows that the recipient is a United States citizen. *Id.*, ¶131.

F. Notification Requirement for Web Publications

In the absence of EAR, Prof. Bernstein would add many more cryptography-related documents to his web pages. Bernstein Decl., ¶136. Prof. Bernstein has refrained from doing so, to avoid incurring the cost of determining which additions would require government notification under EAR. *Id.*

[14] *See* 15 C.F.R. §772.1, definition of "publicly available technology and software"; 15 C.F.R. §734.3(b)(3). "Fundamental" is defined in §734.8; "educational" is defined in §734.9.

Several factors contribute to this cost. First, a review of documents under EAR would not be limited to software focusing on cryptography. For example, Prof. Bernstein's "qmail" software is an Internet post-office program to which Prof. Bernstein would like to add cryptographic components. *Id.*, ¶¶57–64, 136.

Second, EAR's definition of "software" is not limited to instructions actually comprehensible to a computer; it includes instructions "convertible" into such a form.[15] A review of documents under EAR would have to be correspondingly broad.

Third, a review of documents under EAR would not be limited to documents that Prof. Bernstein wrote. Prof. Bernstein often wants to publish copies of documents that he finds elsewhere on the Internet; Prof. Bernstein is much less familiar with the contents of those documents than with his own documents. Bernstein Decl., ¶¶26–29, 141.

Fourth, EAR does not define "cryptographic function," "encryption function," etc. EAR draws a line between "encryption" and "authentication" without explaining how to determine which software falls on the "encryption" side of the line.[16] EAR does not explain, for example, whether a mathematical function useful for both encryption and authentication, or useful for encryption, authentication, and other applications, constitutes an "encryption function"; or whether software designed purely for authentication, but easily modifiable for encryption, constitutes "encryption software." *See* Bernstein Decl., ¶¶137–139.

The government's actions under ITAR and EAR have not clarified the picture. The government controlled Prof. Bernstein's "Snuffle," which could be combined with third-party cryptographic software named "Snefru" to protect information against eavesdropping, even though the government did not control "Snefru" itself. *Id.*, ¶94. The government controlled a paper explaining Snuffle, and then subsequently changed its mind. *Id.*, ¶¶95–100. On at least two occasions, the government controlled software that was merely attachable to third-party "encryption software." Declaration of Brian Behlendorf, AER 81–83 (1996); Declaration of

---

15 *See* 15 C.F.R. §772.1, definition of "program"; 15 C.F.R. §772.1, definition of "software".

16 *See* 15 C.F.R. §774, Supplement 1, ECCN 5A002.a.1.

John Liebman, AER 500–513 (1997).

For these reasons, Prof. Bernstein estimates that reviewing all his desired publications under EAR would take more than fifty hours per year. Bernstein Decl., ¶142.

Prof. Bernstein could instead have his computer send the government a notice of *every* change to his web pages. However, if he had done this starting in December 2000, his computer would already have sent notifications to the government on more than three thousand occasions. *See* Bernstein Decl., ¶25. Prof. Bernstein fears that the government would attempt to prosecute him under 15 C.F.R. §764.2(h), which prohibits taking any action "with intent to evade" EAR. Bernstein Decl., ¶143.

G. Licensing for Assembly-Language Programs

Certain languages called "assembly languages" are particularly well suited for high-speed computation, which in turn is crucial for cryptographic protection of the Internet. *See* Bernstein Decl., ¶¶37, 51, 74, 87.

Assembly-language programs are not "compiled."[17] EAR's definitions of "encryption source code" and "encryption object code" are limited to "compiled" instructions,[18] so they do not include assembly-language programs. The major new EAR exception is limited to "encryption source code" and "object code" compiled from it,[19] so it does not apply to assembly-language programs.

Consequently, EAR continues to require licenses for the publication of assembly-language "EI" software. Prof. Bernstein has refrained from publishing such software. Bernstein Decl., ¶147.

Prof. Bernstein could artificially build a compiled language with the same expressiveness as assembly language, and translate his assembly-language software into that language. *Id.*, ¶148. However, the same approach would also subvert the government's active licensing system for "object code" that is not compiled from publicly available "encryption source

---

17 Second Supplemental Complaint, ¶102; Answer, ¶102.

18 15 C.F.R. §772.1, definition of "encryption source code"; 15 C.F.R. §772.1, definition of "encryption object code".

19 15 C.F.R. §740.13(e)(1); 15 C.F.R. §740.13(e)(2).

code"; Prof. Bernstein fears that the government would attempt to prosecute him under 15 C.F.R. §764.2(h). Bernstein Decl., ¶148.

H. Licensing for Answering Questions

EAR continues to impose two overlapping license requirements for answering questions from people writing "EI" software. First, 15 C.F.R. §744.9(a) prohibits providing unlicensed "technical assistance ... to foreign persons with the intent to aid a foreign person in the development or manufacture outside the United States" of "EI" software. Second, 15 C.F.R. §736.2(b)(1) prohibits unlicensed "export" and "reexport" of controlled "technical assistance."

15 C.F.R. §736.2(b)(1) is broader than §744.9(a) in several ways. It is not limited to activities "outside the United States." It has no intent requirement. It is not limited to software "controlled for EI reasons." It applies, for example, to software "[d]esigned or modified to provide" certain high levels of computer security as specified in 15 C.F.R. §774, Supplement 1, ECCN 5A002.a.6, whether or not that software provides "encryption functions."

15 C.F.R. §736.2(b)(1) is narrower than §744.9(a) in one way. "Publicly available technology" is not "subject to the EAR,"[20] and is therefore exempt from 15 C.F.R. §736.2(b)(1), which applies only to items "subject to the EAR." There is no comparable "subject to the EAR" requirement in §744.9(a).

To obey 15 C.F.R. §744.9(a) and §736.2(b)(1), Prof. Bernstein has refrained from answering various questions on the sci.crypt Internet newsgroup. *See* Bernstein Decl., ¶¶149–155.

I. Licensing for Postings to Sci.Crypt

15 C.F.R. §740.13(e)(3) limits §740.13(e) as follows: "You may not knowingly export or reexport source code or products developed with this source code to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria." 15 C.F.R. §772.1 defines "knowledge" to include "not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence."

[20] *See* 15 C.F.R. §734.3(b)(3).

Prof. Bernstein "knows," under this definition, that anything he posts to the sci.crypt Internet newsgroup is automatically sent to, *inter alia*, certain universities in Iran. Bernstein Decl., ¶157. 15 C.F.R. §740.13(e)(4) states that various forms of Internet publication "would not establish 'knowledge' of a prohibited export or reexport"; but Prof. Bernstein's knowledge has already been established by other means. Bernstein Decl., ¶158.

Consequently, Prof. Bernstein cannot use 15 C.F.R. §740.13(e)(1) to post "EI" software to sci.crypt; he is required to apply for a license.

J. Licensing for Scientific Journals on the Internet

There are two definitions of "published" in EAR. First, 15 C.F.R. §734.7(b) states that "[s]oftware and information is published when it is available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution. See Supplement No. 1 to this part, Questions G(1) through G(3)."

Second, 15 C.F.R. §734.7(a) states that "[i]nformation is 'published' when it becomes generally accessible to the interested public in any form, including (1) Publication ... either free or at a price that does not exceed the cost of reproduction and distribution (See Supplement No. 1 to this part, Questions A(1) through A(6)); (2) Ready availability at libraries ...; (3) Patents ...; and (4) Release at an ... open gathering."

The Supplements state, as examples, that a $15,000 set of manuals that could have been published for $500 does not qualify as being "published,"[21] and that items whose price includes "recovery for development, design, or acquisition" are not "published."[22]

In fact, publishing houses set prices to cover not only the costs of reproduction and distribution, but also author compensation, acquisition costs, editorial costs, illustration costs, design costs, typesetting costs, promotion costs, and profit. O'Reilly Decl., ¶¶6–10. Books, journals, and other items published by publishing houses therefore generally do not qualify as "published" under EAR.

---

21 *See* 15 C.F.R. §734, Supplement 1, Question A(5).

22 *See* 15 C.F.R. §734, Supplement 1, Question G(2); Question I(2).

EAR exempts "printed" publications,[23] so publishing houses remain free to publish controlled information in printed scientific journals. However, that publication does not suffice to make the journal contents "published" under EAR's definition, so Internet publication of the same information remains controlled.

A non-"published" item is still "publicly available," and thus subject to various EAR exceptions, if it arises during, or results from, "fundamental research." *See* 15 C.F.R. §734.3(b)(3). However, Prof. Bernstein also publishes non-research work. Bernstein Decl., ¶160. A non-"published" item can also be "publicly available" by being "educational," but 15 C.F.R. §734.9 defines "educational" narrowly as "released by instruction in catalog courses and associated teaching laboratories of academic institutions."

In light of EAR's restrictive definition of "published," Prof. Bernstein is refraining from preparing non-research "EI" work for journal publication. Bernstein Decl., ¶162.

ARGUMENT

IV. EAR BURDENS SPEECH

EAR burdens publication and other communication of information in the form of "software" and "technical assistance." EAR prohibits various disclosures at scientific conferences; it requires that private email and web publications be reviewed and, in some situations, sent to the government; and it sometimes requires licensing for assembly-language programs, answers to questions, postings to sci.crypt, and electronic scientific journals.

This Court held in *Bernstein I*, 922 F. Supp. at 1434–36, that "software," at least in the form of "source code," is speech for purposes of First Amendment analysis. The Sixth Circuit subsequently reached the same conclusion in another EAR challenge, *Junger v. Daley*, 209 F.3d 481, 484 (6th Cir. 2000). The Second Circuit subsequently held that "software," whether "source code" or "object code," is speech. *Universal City v. Reimerdes*, 273 F.3d 429, 445–446 (2d Cir. 2001).

"Technical assistance" is speech for all the same reasons that "software" is speech.

[23] 15 C.F.R. §734.3(b)(2); §734.3(b)(3), Note.

V. EAR IS CONTENT-BASED

A. A Regulation of Speech Is Content-Based If Its Burdens Are Determined by Content or Motivated by Content

If a regulation of speech is facially content-based, i.e., imposes burdens determined by the content of the speech, then the regulation is content-based. *See Cincinnati v. Discovery Network*, 507 U.S. 410, 429 (1993) (holding that a ban on sidewalk distribution of "commercial handbills" was content-based because "whether any particular newsrack falls within the ban is determined by the content of the publication resting inside that newsrack"); *Burson v. Freeman*, 504 U.S. 191, 197, 217 (1992) (plurality opinion of Blackmun, J., joined by Rehnquist, C.J., and White and Kennedy, JJ., and dissenting opinion of Stevens, J., joined by O'Connor and Souter, JJ.) (holding that strict scrutiny was required for a prohibition on display of "campaign materials" near polling places because the regulation was "facially content-based"); *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 643 (1994) (analyzing, as the first step in the content-based/content-neutral decision, whether the challenged regulations "on their face" imposed burdens with "reference to the content of speech").

If a regulation of speech is facially content-neutral but has a content-based purpose, i.e., is motivated by the content of the speech, then the regulation is content-based. *See United States v. Eichman*, 496 U.S. 310, 315 (1990) (holding that a flag-mutilation law was content-based because, despite having "no explicit content-based limitation on the scope of prohibited conduct," it had a content-based purpose); *Turner*, 512 U.S. at 642 ("even a regulation neutral on its face may be content-based if its manifest purpose is to regulate speech because of the message it conveys").

If a regulation of speech is facially content-neutral *and* has a content-neutral purpose, then the regulation is content-neutral. *See United States v. O'Brien*, 391 U.S. 367 (1968) (draft-card-destruction law); *Clark v. Community for Creative Non-Violence*, 468 U.S. 288 (1984) (camping law); *United States v. Albertini*, 472 U.S. 675 (1985) (prohibition against entering military base); *Ward v. Rock Against Racism*, 491 U.S. 781 (1989) (sound-volume regulation); *Turner*, 512 U.S. 622 (cable-television channel-allocation rules).

B. EAR Imposes Burdens Determined by Content and Motivated by Content

EAR is content-based for two reasons. First, it is facially content-based: it imposes burdens determined by content. Second, it has a content-based purpose: it imposes burdens motivated by content.

15 C.F.R. §774, Supplement 1, ECCN 5D002, on its face, selects a specific type of information for control. First it limits its attention to "software," i.e., instructions "convertible into" computer-comprehensible form. Then, through the definitions in 5A002, it narrows its attention to instructions that fit within certain small categories: being "[d]esigned or modified to use 'cryptography'," providing certain high levels of computer security, etc. Then it exempts instructions for "authentication or digital signature," instructions below certain minimum levels of cryptographic strength, instructions for cryptographic protection of pay-television billing, instructions for intellectual-property protection, etc. *See* 5A002.

As in *Discovery Network*, 507 U.S. at 429, whether any particular document falls within 5D002 is determined by the content of that document. Checking whether a document contains strong cryptographic non-authentication computer-comprehensible instructions means engaging in a detailed inspection of content. In short, 5D002 is facially content-based, and therefore content-based.

Analogous comments apply to 15 C.F.R. §774, Supplement 1, ECCN 5E002, which, on its face, selects 5A002-related and 5D002-related "technical assistance" and "technical data" for control. 5E002 is facially content-based, and therefore content-based.

Furthermore, the burdens imposed by 5D002 and 5E002 are plainly motivated by content. 15 C.F.R. §742.15 states that "EI" instructions are controlled because they "can be used" to maintain secrecy. In other words, the government justifies its regulation of certain documents by referring to the content of the documents: specifically, to the fact that the documents contain instructions that people can follow to achieve a particular result. In the words of *Turner*, 512 U.S. at 642, the "manifest purpose" of 5D002 and 5E002 "is to regulate speech because of the message it conveys." This is an independent reason that 5D002 and 5E002 are content-based.

EAR, in regulating instructions for the effects of following the instructions, is analogous to a hypothetical regulation prohibiting disclosure of chocolate-chip-cookie recipes that provide more than 10 grams of fat per cookie. The recipes are instructions; they are regulated for the effect of following the instructions. That effect is determined by the content of the instructions.[24] This hypothetical regulation is facially content-based, and it has a content-based purpose.

The Supreme Court has already rejected the notion that information usage is a content-neutral basis for regulation. In *Linmark Associates v. Willingboro*, 431 U.S. 85, 93–94 (1977), the Supreme Court struck down an ordinance prohibiting "For Sale" signs on houses:

> The township has not prohibited all lawn signs—or all lawn signs of a particular size or shape—in order to promote aesthetic values or any other value "unrelated to the suppression of free expression," *United States v. O'Brien* . . . Rather, Willingboro has proscribed particular types of signs based on their content because it fears their "primary" effect—that they will cause those receiving the information to act upon it. That the proscription applies only to one mode of communication, therefore, does not transform this into a "time, place, or manner" case.

The situation here is the same. The government regulates information based on its content, namely certain limited types of instructions, because it fears that those receiving the instructions will act upon them. Even if the regulation applied to only one mode of communication—which it does not; it burdens oral disclosures, Internet web pages, etc.—that would not transform it into a regulation subject to time-place-manner analysis or *O'Brien* analysis. *See also Forsyth County v. Nationalist Movement*, 505 U.S. 123, 134 (1992) (holding that "listeners' reaction to speech" is not a content-neutral basis for regulation).

This Court has already commented, in the context of ITAR, that "*O'Brien* does not

---

[24] Suppose, for example, that one recipe stating "Add 50 chocolate chips" is prohibited, while a nearly identical recipe stating "Add 7 chocolate chips" is allowed. The change in effect (from adding 50 chips to adding 7 chips) is caused by the change in content (from "50" to "7"). The analogy in *Universal City v. Reimerdes*, 273 F.3d 429, 454 (2d Cir. 2001), comparing the effect of following instructions to the effect of using a skeleton key while comparing the content of the instructions to the content of a slogan inscribed upon the key, is erroneous: the skeleton key effect is not determined by the slogan. *Universal* is distinguishable because, among other reasons, it was a copyright case; limitations on speech have been scrutinized less in the copyright context than in the context of pure government regulation. *See* Lemley and Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 Duke L.J. 147 (1998).

appear to provide the appropriate standard" for this case. *Bernstein I*, 922 F. Supp. at 1437. This Court has also noted a 1978 memorandum from the Department of Justice, Office of Legal Counsel, stating that a "more stringent constitutional analysis than the *O'Brien* test" is "mandated." *Id.*, n.17.

VI. EAR IS AN UNCONSTITUTIONAL CONTENT-BASED REGULATION OF SPEECH

A. Content-Based Regulations of Speech Are Unconstitutional If They Do Not Fall Within Certain Established Categories and Are Not Aimed Precisely at a Compelling Interest

The First Amendment has exceptions for certain established categories of undesirable content: for example, "the placing of a false representation in a written contract," *United States v. Barnett*, 667 F.2d 835, 842 (9th Cir. 1982); "obscenity," *Miller v. California*, 413 U.S. 15 (1973); and advocacy of violence, when the advocacy is "directed to inciting or producing imminent lawless action and is likely to incite or produce such action," *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969).

A content-based regulation that does not fall within any of the established categorical exceptions is unconstitutional unless it is aimed precisely at a compelling government interest.[25] In particular: (1) It is unconstitutional if it is not necessary to serve the interest, or is not narrowly tailored to serve the interest. *Arkansas Writers' Project, Inc. v. Ragland*, 481 U.S. 221, 231 (1987). (2) It is unconstitutional if it is overinclusive. *Simon & Schuster v. Crime Victims Bd.*, 502 U.S. 105, 122 (1991). (3) It is unconstitutional if it is underinclusive. *The Florida Star v. B. J. F.*, 491 U.S. 524, 540 (1989).

B. EAR Does Not Fall Within The Established Aiding-and-Abetting Category

The First Amendment does not protect communication that intentionally "aids and abets" criminal activity: for example, intentionally aiding illegal gambling, *United States v. Mendelsohn*, 896 F.2d 1183 (9th Cir. 1990); intentionally aiding tax evasion, *United States v. Buttorff*, 572 F.2d 619 (8th Cir. 1978); or intentionally aiding the manufacture of illegal drugs,

[25] *See generally Simon & Schuster v. Crime Victims Bd.*, 502 U.S. 105, 124 (1991) (Kennedy, J., concurring) (discussing role of "compelling interest" test in First Amendment case law).

United States v. Barnett, 667 F.2d 835 (9th Cir. 1982).

However, as the Supreme Court held this year, the "*prospect* of crime . . . by itself does not justify laws suppressing protected speech." *Ashcroft v. Free Speech Coalition*, 122 S. Ct. 1389, ___, 2002 U.S. LEXIS 2789, *22 (2002) (emphasis added).

There is no law against following the Internet-security instructions at issue in this case. EAR regulates disclosure of these instructions merely because the recipient *might* be a terrorist or other criminal.

Allowing such a tenuous connection to criminal activity would dramatically expand the aiding-and-abetting exception: the government would have power to regulate instructions for many other beneficial activities. As an extreme example, the government would have power to regulate publication of instructions teaching a man how to fish, on the grounds that terrorists would be more easily caught if they were starving.

i. The Established Aiding-and-Abetting Category Requires Specific Intent to Aid Criminal Activity

In holding that the First Amendment did not protect publication of a murder manual, the Fourth Circuit relied crucially on the defendants' admitted intent to aid murder:

> [P]erhaps most importantly, there will almost never be evidence proffered from which a jury even *could* reasonably conclude that the producer or publisher possessed the actual intent to assist criminal activity. In only the rarest case, as here where the publisher has stipulated in almost taunting defiance that it intended to assist murderers and other criminals, will there be evidence extraneous to the speech itself which would support a finding of the requisite intent.

Rice v. Paladin Enterprises Inc., 128 F.3d 233, 265 (4th Cir. 1997), *cert. denied*, 118 S. Ct. 1515 (1998).

Similarly, several courts have held that the First Amendment protects movies and music even though the movies and music might have aided or encouraged criminal activity. *E.g.*, *McCollum v. Columbia Broadcasting Sys., Inc.*, 202 Cal. App. 3d 989, 249 Cal. Rptr. 187 (Ct. App. 1988); *Bill v. Superior Court*, 137 Cal. App. 3d 1002, 187 Cal. Rptr. 625 (Ct. App. 1982); *Yakubowicz v. Paramount Pictures Corp.*, 404 Mass. 624, 536 N.E.2d 1067 (Mass. 1989);

Zamora v. Columbia Broadcasting Sys., Inc., 480 F. Supp. 199 (S.D. Fla. 1979).

As the Supreme Court recently observed: "There are many things innocent in themselves ... that might be used for immoral purposes, yet we would not expect those to be prohibited because they can be misused." *Ashcroft*, 122 S. Ct. at ___, 2002 U.S. LEXIS at *33.

All of these cases follow the rule that the First Amendment allows punishment of communication aiding criminal activity if, and only if, the communicator actually *intends* to aid criminal activity. As an example of this rule, the First Amendment would not protect someone who, intending to wreak havoc, publishes detailed instructions (whether "software" or not) for disabling the entire World Wide Web. But the First Amendment would protect an Internet-security researcher providing the same instructions to his colleagues for scientific discussion.

ii. EAR Does Not Require Specific Intent to Aid Criminal Activity

A few of EAR's prohibitions are limited by intent requirements; however, those intent requirements are not tied to criminal activity. 15 C.F.R. §744.9(a) prohibits, under certain circumstances, intentionally helping a foreigner write "encryption software"; but writing "encryption software" is lawful activity. 15 C.F.R. §764.2(h) prohibits taking any action with intent to evade the regulations; but such evasion is not tied to criminal activity, except through the circular argument that violations of the regulations are declared, by the regulations themselves, to be criminal.

A few of EAR's prohibitions are limited by "knowledge" requirements. However, the definition of "knowledge" in 15 C.F.R. §772.1 sweeps far beyond intent into "awareness of a high probability of ... existence or future occurrence." Furthermore, even if "knowledge" were narrowed to actual intent, these requirements would not be tied to criminal activity. 15 C.F.R. §764.2(e) is analogous to 15 C.F.R. §764.2(h). 15 C.F.R. §740.13(e)(3) prohibits "knowing" transfers to Iran et al.; but the government cannot credibly claim that most Iranians are criminals.

Most of EAR's prohibitions are limited by neither intent nor "knowledge."

To summarize, in the words used by the Supreme Court to describe the statute struck down in *Ashcroft*, *supra*: "The evil in question depends upon the actor's unlawful conduct,

conduct defined as criminal quite apart from any link to the speech in question. ... The objective is to prohibit illegal conduct, but this restriction goes well beyond that interest by restricting the speech available to law-abiding adults." 122 S. Ct. at ___, 2002 U.S. LEXIS at *35.

C. EAR Does Not Fall Within Any Other Established Category

EAR does not fit within the established First Amendment exceptions for obscenity, various forms of deceptive speech, advocacy of violence, etc.

D. EAR Does Not Aim Precisely at a Compelling Interest

EAR cannot meet the compelling-interest test. It is, measured against any compelling government interest, either underinclusive, overinclusive, or both. The distinctions drawn in EAR—"printed material" versus other forms of communication; instructions in the form of "technical assistance" versus instructions in the form of "software"; researchers at universities versus researchers elsewhere; publications for the price of "reproduction and distribution" versus publications where the author receives royalties; and so on—are not tied to any compelling government interest. As this Court observed in *Bernstein III*, after the Defendants stated[26] that a "critical national security interest of the United States is to maintain an effective capability to gather foreign intelligence information":

> Defendants claim that encryption poses unique and serious threats to national security, yet the printed matter exception belies this rationale by making encryption freely available to only those foreigners who are technologically sophisticated. Defendants conceded at oral argument that the effect of this dichotomy would be to make it more difficult only for the more inept.

Bernstein v. Department of State et al., 974 F. Supp. 1288, 1306 (N.D. Cal. 1997).

The Defendants have asserted without justification that "the governmental interest in controlling the export of encryption software is compelling."[27] The Supreme Court has already held that this circular type of "interest" must be rejected:

---

[26] Defendants' Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss, at 2 (1995).

[27] Defendants' Memorandum of Points and Authorities in Support of Defendants' Motion for Summary Judgment, at 25, n.27 (1996).

> [T]he Board has taken the *effect* of the statute and posited that effect as the State's interest. If accepted, this sort of circular defense can sidestep judicial review of almost any statute, because it makes all statutes look narrowly tailored. ... "Every content-based discrimination could be upheld by simply observing that the state is anxious to regulate the designated category of speech."

Simon & Schuster v. Crime Victims Bd., 502 U.S. 105, 120 (1991) (internal citations omitted; emphasis in original).

VII. EAR IS UNCONSTITUTIONALLY OVERBROAD

"The Government may not suppress lawful speech as the means to suppress unlawful speech. ... The overbreadth doctrine prohibits the Government from banning unprotected speech if a substantial amount of protected speech is prohibited or chilled in the process." *Ashcroft*, 122 S. Ct. at ___, 2002 U.S. LEXIS at *39.

A substantially overbroad regulation may be challenged and invalidated on its face, whether or not the challenger's activities are protected by the First Amendment. *See, e.g., Foti v. City of Menlo Park*, 146 F.3d 629, 635 (9th Cir. 1998); *Bd. of Airport Com'rs of Los Angeles v. Jews for Jesus, Inc.*, 482 U.S. 569, 573–74 (1987) (invalidating a regulation on its face as overbroad without considering an as-applied challenge); *Sec'y of State of Md. v. J. H. Munson Co.*, 467 U.S. 947, 958 (1984) (allowing the plaintiff to bring a facial challenge "whether or not its own First Amendment rights are at stake").

EAR's failure to require criminal intent is a facial deficiency infecting every application of the regulations to speech. The portions of EAR that target speech—most importantly, 15 C.F.R. §774, Supplement 1, ECCN 5D002 and 5E002—can never be applied consistently with the First Amendment. These portions can and should be invalidated on their face.

VIII. EAR IS UNCONSTITUTIONALLY VAGUE

A regulation is void for vagueness if its prohibitions are not clearly defined. *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). The required degree of clarity is increased for regulations of speech, particularly content-based regulations of speech allowing severe criminal sanctions. *Reno v. ACLU*, 521 U.S. 844, 871–72 (1997).

Several relevant portions of EAR are unconstitutionally vague. First, 15 C.F.R. §744.9(a)

states that "mere teaching or discussion of information about cryptography" would not "establish" the requisite intent. Does "mere teaching or discussion of information about cryptography" include teaching a detailed course on cryptography, with software handouts? Does it include tutoring students in such a course? What is the difference between tutoring and consulting?

Second, the definition of "program" in 15 C.F.R. §772.1 includes all instructions "convertible" into computer-comprehensible form. What types of conversions are allowed? Which of the Snuffle-related documents DJBCJF-2, DJBCJF-3, DJBCJF-4, DJBCJF-5, and DJBCJF-6 are "software"? *See* Bernstein Decl., ¶¶95–100.

Third, the definition of 5D002 relies on the undefined phrases "cryptographic function," "encryption function," "encryption feature," and "authentication." Which of these phrases apply to a pseudorandom number generator? The P-224 Diffie-Hellman key-exchange function? Snefru, and Snuffle? *See* Bernstein Decl., ¶¶79, 83–85, 88–90.

IX. EAR IS AN UNCONSTITUTIONAL PRIOR RESTRAINT

"[P]rior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights." *Nebraska Press Assn. v. Stuart*, 427 U.S. 539, 559 (1976). As this Court commented in *Bernstein II*: "The danger inherent in prior restraints is largely procedural, in that they bypass the judicial process and locate in a government official the delicate responsibility of passing on the permissibility of speech." *Bernstein v. Department of State et al.*, 945 F. Supp. 1279, 1287 (N.D. Cal. 1996).

Facial challenges to licensing schemes are permitted whenever the censor has "substantial power to discriminate based on the content or viewpoint of speech by suppressing disfavored speech or disliked speakers": in particular, when the licensing schemes target (1) speech or (2) conduct commonly associated with speech. *Lakewood v. Plain Dealer Publishing Co.*, 486 U.S. 750, 760 (1988).

The Supreme Court has placed several procedural requirements upon licensing schemes. First, if the licensing scheme is content-based, it must force the censor to go to court and to bear the burden in court of justifying each license denial. *Freedman v. Maryland*, 380 U.S. 51 (1965).

Second, the licensing scheme must specify a short time limit for each license decision and a mechanism for expeditious judicial review. *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 226–227 (1990); *Riley v. National Federation of Blind of N.C., Inc.*, 487 U.S. 781 (1988); *Freedman*, 380 U.S. 51. A court may reach this issue, exactly as this Court did in *Bernstein II* and *Bernstein III*, without deciding whether the scheme is content-based. *FW/PBS*, 493 U.S. 215.

Third, the licensing scheme must contain "adequate standards to guide the official's decision and render it subject to effective judicial review." *Thomas v. Chicago Park District*, 534 U.S. 316, ___ (2002); *Niemotko v. Maryland*, 340 U.S. 268, 271 (1951).

EAR, despite the addition of 15 C.F.R. §740.13(e)(1), is still a licensing scheme. In particular, 5D002 and 5E002, when read in light of the remaining provisions of EAR, are licensing schemes specifically targeting speech. They give the censor substantial power to discriminate based on the content of the speech. They flunk every one of the procedural tests: they have no provisions for judicial review, they do not guarantee fast licensing decisions, and they place unbridled discretion into the hands of the censor. Consequently, they are facially unconstitutional prior restraints.

The logic here is the same as the logic already used by this Court, and the Ninth Circuit, in holding that the previous version of EAR was an unconstitutional prior restraint. *See Bernstein III*, 974 F. Supp. at 1308; *Bernstein IV*, 176 F.3d at 1145. None of EAR's procedural failures have been fixed.

X. EAR IS AN UNCONSTITUTIONAL REGULATION OF ASSOCIATION AND ASSEMBLY

The First Amendment protects the "inseparable" freedoms of speech, assembly, association, and petition. *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 911 (1982). "The right of peaceable assembly is a right cognate to those of free speech and free press and is equally fundamental." *De Jonge v. State of Oregon*, 299 U.S. 353, 364 (1937).

These rights are not limited to political activities. The First Amendment protects an association hiring an attorney. *Mine Workers v. Illinois Bar Assn.*, 389 U.S. 217, 223 (1967). The freedoms of assembly and association protect a group of three people meeting on a sidewalk,

even if those people engage in "annoying" behavior. *Coates v. City of Cincinnati*, 402 U.S. 611, 618 (1971). The freedom of "expressive association" protects any association that engages in expressive activity, public or private. *See Boy Scouts of America v. Dale*, 530 U.S. 640, 653, 656 (2000).

In *Thomas v. Collins*, 323 U.S. 516 (1945), the Supreme Court held that a registration requirement for making a public speech violated the rights of free speech and free assembly. In that case, as in this case, the harm caused by the law was amplified by the timing of the required notification. Thomas was a union organizer visiting Texas to give a speech soliciting new union membership applications. He was served with a restraining order six hours before his speech. The law required that Thomas send mail to the Secretary of State of Texas, and wait for a response, *before* giving his speech; evidently that would have taken more than six hours.

EAR unconstitutionally abridges the freedoms of assembly and association, not just speech, by imposing burdens upon scientific conferences. See Section III.D. Conferences are the essence of expressive association.

XI. EAR IS AN UNCONSTITUTIONAL SEARCH AND SEIZURE

The Fourth Amendment provides as follows: "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Where the seizure of "things" is based upon "the ideas which they contain," the Supreme Court has repeatedly held that a warrant is not only necessary, but also must describe the targeted "things" with "the most scrupulous exactitude." *Stanford v. Texas*, 379 U.S. 476, 485 (1965); *see Roaden v. Kentucky*, 413 U.S. 496 (1973); *Lee Art Theatre, Inc. v. Virginia*, 392 U.S. 636 (1968).

The Fourth Amendment is a privacy right, not merely a property right. "[T]he Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements." *Katz v. United States*, 389 U.S. 347, 353 (1967).

These protections would become meaningless if the government could make a law requiring that people provide copies of all information to the government without even being asked, or if the government could make a law requiring government video cameras in private homes. The government would be able to collect information centrally to search at its leisure, ignoring the Fourth Amendment requirement of judicial scrutiny.

EAR's notification and licensing requirements are not limited to public information; EAR also demands copies of private information. EAR provides no procedural safeguards to control this privacy intrusion: there is no requirement that the government obtain a warrant, that application for a warrant be based upon probable cause, or that the warrant describe, with "the most scrupulous exactitude," the information to be seized. Consequently, EAR violates the Fourth Amendment.

EAR also violates the Fourth Amendment indirectly, to the extent that it interferes with the privacy rights of the legitimate *users* of cryptography. As the Ninth Circuit commented in *Bernstein IV*, 176 F.3d at 1146:

> The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment. . . . While we leave for another day the resolution of these difficult issues, it is important to point out that Bernstein's is a suit not merely concerning a small group of scientists laboring in an esoteric field, but also touches on the public interest broadly defined.

CONCLUSION

For the foregoing reasons, Plaintiff's Motion for Summary Judgment should be granted.

Respectfully submitted,

KARL OLSON