CRACKING THE DEPARTMENT OF COMMERCE'S ENCRYPTION EXPORT REGULATIONS

Peter K. Hoffmann[†]

On January 12, 2000, the United States Department of Commerce Bureau of Export Administration issued revised encryption export regulations, implementing a change in encryption export policy announced by the White House in September 1999.[1] The previous regulations were challenged in the federal courts as a violation of First Amendment rights.[2] Parties interested in revised encryption policies included not only advocates of privacy and free-speech, but also national security and law enforcement officials, and high-tech industry representatives. A subcommittee of President Clinton's Export Council recommended the regulations for an overhaul[3] and the new regulations were the subject of popular legislative proposals in both the House of Representatives and the Senate.[4] As will be discussed, prior to the White House announcement, the previous encryption regulations had already been the source of contention in all three branches of the federal government.

The Federal Judiciary:

On May 6, 1999, a divided Ninth Circuit panel initially upheld a graduate student's successful facial challenge to provisions of early versions of the Export Administration Regulations ("EAR").[5] The student brought the challenge after the State Department determined that publication of his cryptographic source code and related academic research was subject to federal licensing as "munitions."[6] The court held that the EAR's provisions limiting the distribution of encryption software were facially invalid as a prior restraint on speech, and enjoined government enforcement.[7] The Ninth Circuit explained that the provisions violated the First Amendment "because the prepublication licensing regime challenged here applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards . . . ."[8]

The Ninth Circuit's original decision was a major victory for opponents of the Administration's encryption export policy. Tara Lemmey, Electronic Frontier Foundation's Executive Director stated that the decision "is a giant step forward in bringing down export controls and it goes further than any of the legislation that has been talked about so far because none [of those bills] address the First Amendment issues."[9] As a result of the ruling, the domestic use of encryption technology was expected to increase dramatically because liability for posting source code on the Internet was virtually eliminated.[10]

Aside from *Bernstein*, only two other cases have addressed whether exporting encryption software source code is sufficiently expressive to merit First Amendment protection.[11] In *Junger v. Daley*, an Ohio federal district court ruled that "although encryption source code may occasionally be expressive, its export is not protected conduct under the First Amendment."[12] However, the Sixth Circuit reversed this decision, holding that source code is protected under the First Amendment.[13] In *Karn v. United States Department of State*, although not reaching the question of whether source codes without accompanying comments are protected by the First Amendment, a D.C. district court noted that "[s]ource codes are merely a means of commanding a computer to perform a function" and are thus not protected by the First Amendment.[14]

In response to the *Bernstein* ruling, the United States filed a petition asking the full Ninth Circuit to reverse the panel's decision.[15] The Government warned that the decision would "gravely compromise the ability of the United States to control the export of encryption products to potentially

hostile foreign parties."[16] Furthermore, the Government disputed the merits of the decision. According to the Government, controls on the export of encryption source code were "not 'directed narrowly and'" specifically at the export of encryption source code as an expressive activity, and are therefore not subject to the First Amendment's procedural safeguards.[17] Furthermore, the Government argued that export control is "too blunt a censorship instrument to warrant judicial intervention prior to an allegation of actual misuse. . . ."[18] Alternatively, the appellants suggested that "[e]ven if the export controls on encryption source code were facially unconstitutional, which they are not, the panel majority erred by ruling that the export controls on encryption source code are not severable from those applicable to other encryption products."[19]

On September 30, 1999, the Ninth Circuit ordered that *Bernstein* be reheard by the en banc court, and withdrew the panel's decision.[20] The visiting judge who cast the deciding vote in the earlier panel decision had stated that "[t]he importance of this case suggests that it may be appropriate for review by the United States Supreme Court."[21] Other commentators have since predicted that the case will ultimately be heard by the Supreme Court.[22]

Congress:

While First Amendment advocates battled the Government in court, members of Congress introduced legislation aimed at overhauling the encryption export regulations. In the House, Representative Bob Goodlatte (R-Virginia) introduced H.R. 850, the Security and Freedom through Encryption ("SAFE") Act, on February 25, 1999, with over 200 co-sponsors.[23] The bill was favorably reported with amendments by the House Judiciary Committee, Committee on Commerce, Committee on International Relations, Committee on Armed Services, and the Committee on Intelligence (Permanent).[24] The bill was reported and committed to the House on July 23, 1999.[25] Before the Administration announced its new encryption export policy, the SAFE Act was scheduled for floor action and appeared headed toward passage with many bipartisan co-sponsors.[26]

There are many notable provisions in the proposed SAFE Act. First, the proposed Act sets forth criteria for the export of encryption products utilizing a key-length of 64 bits or less.[27] The SAFE Act also contains provisions that limit review of encryption products to a one-time review within 45 days;[28] require exporters to provide the names and addresses of its "distribution chain partners" and, if available, to identify the end-user or use of the product;[29] require all exporters and their distribution chain partners to report the names and addresses of the next purchaser in the distribution chain;[30] and require exporters to report to the Secretary of Commerce when the exporter believes that the exported products or services is being diverted to a use or user not approved for export, or when the exporter has detected pirating of the technology or intellectual property.[31] The proposed Act also authorizes the President to control the export of all dual-use encryption products;[32] to deny without prior judicial review the export of any encryption product that is deemed to be contrary to the national security interests;[33] to allow export under license exception of encryption products utilizing key-lengths greater than the maximum-strength level (currently set at 64 bits) in any case when it would be in accord with the national security interest of the United States;[34] and to waive, without judicial review, any provision relating to the export of encryption products for national security purposes, provided he reports to the relevant Congressional committees within fifteen days.[35] Finally, the proposed Act establishes the Encryption Industry and Information Security Board composed of six government officials and six representatives from the private sector to advise the President on encryption policy and technological advancements.[36]

Following the introduction of the SAFE Act, Senator McCain introduced the Promote Reliable On-Line Transactions to Encourage Commerce and Trade Act of 1999 ("PROTECT") with five co-sponsors on April 14, 1999.[37] The bill, currently co-sponsored by four Democratic and three Republican Senators, was placed on the legislative calendar on August 5, 1999.[38]

PROTECT's notable provisions would decontrol encryption products utilizing a key length of 64 bits or less;[39] limit the Commerce Department's review of license applications to a one-time, fifteen-day technical review;[40] and allow exports of encryption products utilizing a key-length greater than 64 bits to export under license exception if the Secretary of Commerce determines that it is exportable under the Export Administration Act,[41] or if the Encryption Advisory Board[42] determines that the products or service is or will be available within 12 months from a foreign supplier;[43] and authorize the President to override any decision, without judicial review, for purposes of national security.[44]

The Clinton Administration opposed both the House and the Senate bills. It explained that both the SAFE and PROTECT Acts were objectionable because they "stripped away the things that are essential for national security: a meaningful technical review of encryption products before they're exported, and reporting about where they have gone and how they've been installed after the fact."[45] In addition, neither bill includes a provision requiring all encryption products to allow law enforcement officials to covertly decode any message.[46] Therefore, the Administration announced that President Clinton would veto any legislation "that does not protect national security and law enforcement interests."[47]

To avoid a potential veto, the Administration announced the development of a new policy on September 16, 1999.[48] Deputy National Security Advisor Jim Steinberg stated that the Administration believes the strategy employed by its new regulation "provides a more balanced approach to the issue than the proposals that are now before Congress. . . . [The Administration is] look[ing] forward to working with Congress to implement a solution that meets the needs of all those involved."[49] The strategy appears to have worked. In response to the Administration's announcement, Rep. Zoe Lofgren, a supporter of the SAFE Act, urged that any further action on that bill be delayed until the new regulations were announced.[50] Accordingly, members of Congress urged President Clinton to consider the provisions of the SAFE Act when drafting the regulations, noting that House Bill 850 avoids the distinction between retail and other products drawn by the draft regulation by considering various indicia, including whether the encryption product is "widely available."[51]

The Clinton Administration:

During the month prior to the Clinton Administration's announcement, the encryption subcommittee of President Clinton's Export Council recommended the elimination of most export controls on encryption products in order to allow U.S. companies to compete with foreign vendors.[52] The subcommittee's recommendations for the liberalization of encryption export policy included easing controls on the export of encryption products to banks, health care organizations, and e-commerce merchants located outside of the United States, and eliminating the export approval process for the export of encryption products to "non-threatening" countries.[53] The Administration's new strategy is intended to "update and simplify export controls on encryption"[54] and embodies three principles that emerged from a review "conducted in consultation with industry and privacy groups and the Congress."[55] First, the new policy would involve only "a one-time technical review of encryption products in advance of sale . . . ."[56] Second, the post-export reporting system would be streamlined.[57] Third, the process

would permit “the government to review the exports of strong encryption to foreign government and military organizations and to nations of concern.”[58] A report to the President by Secretary of Defense William Cohen, Attorney General Janet Reno, Director of the Office of Management and Budget Jacob J. Lew, and Secretary of Commerce William Daley explained that “[w]ith these three principles in place, the Federal Government would remove almost all export restrictions on encryption products.”[59]

Furthermore, the Administration announced that its new policy was to be coupled with steps ensuring “that law enforcement has the legal tools, personnel, and equipment necessary to investigate crime in an encrypted world.”[60] Accordingly, the Administration explained that under the “new framework for export controls, the national security organizations will need to develop new technical tools and capabilities to deal with the rapid expansion of encrypted communications in support of its mission responsibilities. The Congress will need to support such new tools and technical capabilities through necessary appropriations.”[61] To address law enforcement concerns, the Administration introduced CESA legislation largely centered on the establishment of a Technical Support Center; a concept suggested by industry as a vehicle for cooperation between government and industry.[62] Congress, however, has yet to take any action on the Administration's proposed legislation.

The Administration indicated that it intended to have the revised regulations codified by “December 15, 1999, following consultations on the details with affected stakeholders[,]”[63] which would include “consult[ing] with industry to ensure that the reporting requirements will be streamlined to reflect business models and practices and will be based on what companies normally collect.”[64] Industrial representatives hailed the announcement as a very positive step toward enabling domestic vendors of encryption products to compete worldwide.[65] However, the draft regulations circulated by the Administration in November, 1999 received a largely negative reaction from privacy advocates and members of Congress.[66] These parties complained that the regulations discriminated against Internet sales of encryption products, and poorly defined what would qualify as a “foreign government or entity” to which strong encryption sales are restricted.[67]

In response, the Administration postponed the December release of the regulations, and set a new deadline of January 14, 2000.[68] William Reinsch, the U.S. Commerce Department Undersecretary for Export Administration, explained that the new draft rules would include relaxed limits on source code, chips and toolkits.[69] On January 14, 2000, the Administration released the new encryption export regulations.[70] The encryption regulations:

- allow the export and reexport of any encryption commodity or software to individuals, commercial firms, and other non-government end-users in all destinations[;]
- allow[] exports and reexports of retail encryption commodities and software to all end-users in all destinations[;]
- [enable] [t]elecommunications and Internet service providers [to] obtain and use any encryption product under this license exception to provide encryption services[;]
- [allow export under license exception of commercial encryption source code, encryption toolkits and components] “for commercial production or sale of products developed using source code[;]”
- [relax Internet posting restrictions on publicly available encryption source code;
- permit export of encryption source code without prior review and only written notification;
- eliminate the requirement that foreign employees of U.S. companies working in the United

States must obtain an export license in order to work on encryption;

- streamline post-export reporting requirements; and
- implement agreements under the Wassenaar Arrangement by decontrolling] "mass market encryption products up to and including 64-bits [and] certain 512-bit key management products."[71]

In addition, the new regulations maintain a mandatory one-time product review by BXA in most cases,[72] as well as the existing "[r]estrictions on terrorist supporting states (Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria), their nationals and other sanctioned entities are not changed by this rule."[73] The Government will review the viability of the regulation and accept comments from the public for 120 days.[74] Thereafter, a final revised rule will be issued. While the initial reaction to the regulations has been quite positive,[75] supporters of the congressional legislation have indicated that they will "be watching carefully to make sure that the regulations released [on January 12, 2000] are implemented properly and in a timely manner[,]" and warned that Congress "remains ready to take up the [SAFE Act.]"[76]

It remains to be seen how the new regulations, if finalized in their present form, will affect the *Bernstein* case.[77] While the revised regulations address the posting of source code on the Internet, the American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center have announced that they are dissatisfied and intend to continue to advance the issue in the courts.[78] The Ninth Circuit granted a Department of Justice request for a delay of the hearing in order to determine the impact of the new regulations on the case and re-scheduled oral argument for March 21, 2000.[79]

---

† B.A. (Economics), 1995, Colby College; J.D. (anticipated), 2001, Boston University School of Law.

[1] United States Department of Commerce, *Press Release: Commerce Announces Streamlined Encryption Export Regulations* (Jan. 12, 2000) <http://204.193.246.62/public.nsf/docs/60D6B47456BB389F852 568640078B6C0>.

[2] *Compare* Bernstein v. United States Dep't of Justice, 176 F.3d 1132, 1145 (9th Cir. 1999) (holding that the encryption export regulations are facially invalid as a prior restraint on speech), *and* Junger v. Daley, No. 98-4045, 2000 WL 343566, at *4 (6th Cir. Apr. 4, 2000) ("Because computer source code is an expressive means for exchanging information and ideas about computer programming, we hold that it is protected by the First Amendment."), *with* Karn v. United States Dep't of State, 925 F. Supp. 1, 9 n.19 (D.D.C. 1996) (implying that source codes without comments are not necessarily "speech" under the First Amendment).

[3] *See* Maria Seminerio, *Clinton Panel: Open Crypto Controls*, ZDNET NEWS, Aug. 27, 1999, *available in* 1999 WL 14537993.

[4] *See* H.R. 2616, 106th Cong. (1999); S. 854, 106th Cong. (1999); S. 798, 106th Cong. (1999); H.R. 850, 106th Cong. (1999).

[5] *See Bernstein*, 176 F.3d at 1145.

[6] *See id*. at 1136.

[7] *See id*. at 1145.

[8] *Id*.

[9] Declan McCullagh, *Landmark Ruling on Encryption*, WIRED NEWS, May 6, 1999 (visited May 10, 2000) <www.wired.com/news/politics/0,1283,19553-2,00.html> (alteration in original).

[10] *See id*. According to Professor Michael Froomkin, if the decision is upheld, residents of California, Washington, or Oregon (states within the Ninth Circuit) "can post source code on the Internet without fear. . . ." *Id*. Professor Froomkin also predicted "a lot more cryptographic use domestically. People are going to start building it into products. . . ." *Id.*

[11] *See* Junger v. Daley, 8 F. Supp. 2d 708, 715 (N.D. Ohio 1998); Karn v. United States Dep't. of State, 925 F. Supp. 1, 9-10 (D.D.C. 1996).

[12] 8 F. Supp. 2d at 715.

[13] *See* Junger v. Daley, No. 98-4045, 2000 WL 343566, at *4 (6th Cir. Apr. 4, 2000).

[14] *Karn*, 925 F. Supp. at 9 n.19.

[15] *See* Appellants' Petition for Panel Hearing and Rehearing En Banc at 1, Bernstein v. United States Dep't of Commerce, 192 F.3d 1308 (9th Cir. 1999) (No. 97-16686).

[16] *Id*.

[17] *Id*. at 12.

[18] *Id.* (internal citation omitted).

[19] *Id*. at 13.

[20] *See* Bernstein v. United States Dep't of Justice, 192 F.3d 1308, 1309 (9th Cir. 1999)

[21] Bernstein v. United States Dep't of Justice, 176 F.3d 1132, 1147 (9th Cir. 1999) (J. Bright, concurring).

[22] *See* John Scheinman, *Government Trying to Maneuver in Bernstein Encryption Fight*, ELECTRONIC COM. NEWS, Oct. 18, 1999, *available in* 1999 WL 6502819. "The fight probably will wind up before the Supreme Court, says David Sobel, general counsel for the Electronic Privacy Information Center, a Washington-based public interest research group." *Id*.; Brenda Sandburg, *Ninth Circuit Set to Review Encryption Case En Banc*, RECORDER, Oct. 1, 1999, *available in* LEXIS, News Group File (reporting that Bernstein's attorney believes the question of Internet access to encrypted technology "may ultimately be left to the U.S. Supreme Court to decide.").

[23] *See* H.R. 850, 106th Cong. (1999).

[24] *See id*.

[25] *See id*.

[26] *See* Rep. Richard Armey, *Personal Privacy*, CONG. PRESS RELEASES, Dec. 6, 1999, *available in* LEXIS, News Group File.

[27] *See* H.R. 850 § 302(a).

[28] *See id.* § 302(a)(1), (b).

[29] *See id.* § 302(a)(4)(B), (5).

[30] *See id.* § 305(c)(3).

[31] *See id.* § 305(c)(1)-(2).

[32] *See id.* § 301(a).

[33] *See id.* § 301(b).

[34] *See id.* § 303.

[35] *See id.* § 305(e)(1).

[36] *See id.* § 306.

[37] *See* S. 798, 106th Cong. (1999).

[38] *See id.*

[39] *See id.* § 503.

[40] *See id.* § 504(b).

[41] *See id.* § 505(a)(1).

[42] The Encryption Advisory Board is created by Export Administration Act to make recommendations to the Secretary of Commerce. *See id.* § 505(b).

[43] *See id.* § 505(a)(2)(C).

[44] *See id.* § 502(a).

[45] White House, Office of the Press Secretary, *Press Briefing by Administration Officials on Encryption*, , at 8, *available in* 1999 WL 722459 (quoting Deputy Secretary of Defense John Hamre that as indicating that these elements are essential to national security).

[46] *See Senate Panel Favors Stronger Encryption*, ZDNET NEWS, June 23, 1999 (visited May 10, 2000) <www.zdnet.com/zdnn/stories/news/0,4586,2281181,00.html>.

[47] *Press* White House, Office of the Press Secretary, *supra* note 45, at 2 (quoting Deputy National Security Advisor Jim Steinberg).

[48] *See id*. at 1, 2.

[49] *Id*. at 2.

[50] *See* Robert MacMillan, *Crypto Delay Evokes Caution, Hope*, NEWSBYTES PM, Dec. 14, 1999, *available in* LEXIS, News Group File.

[51] *See* Rep. Zoe Lofgren, *Draft Encryption Regulations*, CONG. PRESS RELEASES, Dec. 6, 1999, *available in* LEXIS, News Group File; *see also* Rep. Patrick J. Kennedy et al., *Draft Regulations on Encryption Export Controls*, CONG. PRESS RELEASES, Dec. 13, 1999, *available in* LEXIS, News Group File (publishing a letter to Congress signed by nine Representatives).

[52] *See* Seminerio, *supra* note 3.

[53] *See id*.

[54] White House, Office of the Press Secretary, *Administration Announces New Approach to Encryption*, at 1 (Sept. 16, 1999), *available in* 1999 WL 721387.

[55] *Id*.

[56] *Id*.

[57] *See id*.

[58] *Id*.

[59] White House, Office of the Press Secretary, *Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace*, at 1(Sept. 16, 1999), *available in* 1999 WL 722453.

[60] White House, Office of the Press Secretary, *supra* note 54, at 2.

[61] White House, Office of the Press Secretary, *supra* note 59, at 10; *see* White House, Office of the Press Secretary, *supra* note 45, at 9 (quoting Deputy Secretary Hamre). "[A]ll three parts of th[e] framework are essential. We must have a strong commitment to security products, security infrastructure. We need to buy that. We have to have a new regime for export control, and we also need to have stronger tools for law enforcement." *Id*.

[62] *See* White House, Office of the Press Secretary, *supra* note 45, at 10 (quoting Attorney General Janet Reno).

> The stronger tools lie in the technical support center, because what we're trying to do is not create a new authority, we're trying to match technology to the existing authority, and we think after conversation with industry and the working relationship that we've developed with them that, through this technical support center, we will be able to do so.

Id.

[63] White House, Office of the Press Secretary, *supra* note 54, at 2.

[64] *See* White House, Office of the Press Secretary, *supra* note 45, at 5 (quoting Secretary of Commerce William M. Daley).

[65] *See, e.g.*, John Simons, *U.S. to Relax Restrictions on Encryption Technology*, WALL ST. J., Sept. 16, 1999, at B6. "'This is a great leap forward,' said Dan Scheinman, senior vice-president of legal and government affairs at Cisco Systems Inc., a big maker of networking gear in San Jose, Calif. 'Based on our current understanding, the industry can now compete on equal footing with our foreign competitors.'" *Id*.

[66] *See* MacMillan, *supra* note 50; Kennedy, *supra* note 51.

[67] *See* MacMillan, *supra* note 50; Kennedy, *supra* note 51.

[68] *See* Ted Bridis, *U.S. Delays New Export Rules on Data-Scrambling Software*, DESERET NEWS, Jan. 2, 2000, at M5, *available in* LEXIS, News Group File.

[69] *See id.*

[70] Revisions to Encryption Items, 65 Fed. Reg. 2492 (2000) (to be codified as amended at 15 C.F.R. pts. 734, 740, 742, 770, 772, and 774).

[71] *Id.* at 2492-94.

[72] *See id*.

[73] *Id.* at 2492.

[74] *See id*.

[75] *See e.g.*, John Schwartz, *U.S. Eases Encryption Export Rules*, WASHINGTON POST, Jan. 13, 2000 at E1.

> "This is good news for America," Ed Gillespie and Jack Quinn, who head a coalition called Americans for Computer Privacy (ACP), said in a statement. . . . "It's still more complex than I'd like to see," said Piper Cole, a Sun Microsystems Inc. executive involved in the negotiations with the White House over the policy, "but it's just a whole lot better and recognizes the realities of the marketplace and the networked world."

Id.

[76] Doug Brown, *Revised Crypto Rules Seen as Improvement*, ZDNET NEWS, Jan. 13, 2000, *available in* 2000 WL 4064337 (quoting Rep. Bob Goodlatte). "It's not perfect, but it's not bad. . . . Much of what we hoped to achieve through SAFE has been achieved through these regulations. . . . [I]t would be a mistake to move that bill, because we've gotten so much of what we'd hope to achieve." Schwartz, *supra* note 75.

[77] *See supra* notes 5-10, 15-22 and accompanying text (discussing Bernstein v. United States Dep't of Justice, 113 F.3d 1132 (9th Cir. 1999), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999)).

[78] *See* Electronic Frontier Foundation, *Civil Liberties Groups Say New Encryption Export Regulations Still Have Serious Constitutional Deficiencies* (January 13, 2000) <http://www.eff.org/11300_crypto_release. html>; Schwartz,

supra note 75.

> Because of its focus on paving the way for business to export encryption, [said Alan Davidson of the Center for Democracy and Technology], the new regulation "is not going to address all of the constitutional free speech and privacy concerns that have been raised" about past restrictions on encryption export.

Id.

> Barry Steinhardt, Associate Director for the ACLU, said, "The rules are a step forward, but they are still too complex and leave too many questions unanswered. Now that the Administration has tacitly admitted that it can't and shouldn't control the use of encryption, it should have announced a simple deregulation, rather than regulatory maze."

Electronic Frontier Foundation, *supra*.

[79] *See* Bernstein v. United States Dep't of Justice, No. 97-16686 (9th Cir. Oct. 28, 1999) (order granting rehearing).