Decl. of William P. Crowell, Sept. 10, 1997 in Bernstein v. Commerce

This is a series of page images from a fax machine.

You can view or print this page for a full copy of the document. It will take a while to download all 7 pages.

If you want to view or print this document in pieces, you can download the individual image files, named "page01.gif", "page02.gif", etc. (01 through 07).

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

DANIEL J. BERNSTEIN	)	
Plaintiff - Appellee ,	)	
v.	)	No. _____
UNITED STATES DEPARTMENT OF COMMERCE et al.	)	(D.C. No. C-95-0582 MHP)
Defendants-Appellants	)	

DECLARATION OF WILLIAM P. CROWELL, NATIONAL SECURITY AGENCY, IN SUPPORT OF EMERGENCY MOTION FOR A STAY OF INJUNCTION PENDING APPEAL

I, William P. Crowell, do hereby state and declare as follows:

1. I am the Deputy Director of the National Security Agency ("NSA"). I have held that position since February 2, 1994. As the Deputy Director of NSA, I am the highest ranking civilian in the Agency and my responsibility is to oversee the management of NSA. Prior to my current position, I served as the Deputy Director for Operations from October 1991 to February 1994, and prior to that I held numerous other senior positions throughout the Agency. The Operations Directorate is the NSA organization which contains the Encryption Export Control Branch, the Branch which provides technical advice to the Department of Commerce regarding the classification and licensing of cryptographic products for exportation. This declaration is submitted in support of the government's motion for a stay of the district court's injunction pending appeal in this action. All of the statements made

herein are based on my personal knowledge and information obtained in the course of my official duties.

I. The National Security Agency

2. The National Security Agency/Central Security Service was established by Presidential directive in 1952 as a separately organized agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense. NSA has two primary missions: (1) to conduct the signals intelligence ("SIGINT") activities of the United States Government; and (2) to carry out the responsibilities of the Secretary of Defense concerning the security of communications systems for the United States Government.

3. NSA's SIGINT mission is conducted through sophisticated collection technologies that allow NSA to obtain information from foreign electromagnetic signals. Base on information derived from these activities, NSA provides reports on a rapid-response basis to national policymakers, military commanders, and other entities throughout the federal government. This information has proven to be highly reliable and essential to the national defense, national security, and the conduct of the foreign affairs of the United States. Encryption[1] used by foreign intelligence targets, in an effort to ensure that their communications remain secret from everyone except the intended recipient, can have a debilitating effect on NSA's ability to collect and report such critical foreign intelligence. A core NSA activity is "cryptanalysis" -- the science of reading "ciphertext" (i.e., determining the content of encrypted

1. "Encryption" is the process of transforming the original text of a message into a text that is not understandable and, thus, whose content is hidden. This is referred to as transforming "plaintext" to "ciphertext." "Decryption" is the process of transforming ciphertext back to plaintext (original text).

messages). For this reason, and because of NSA's unique technical knowledge and skills in all aspects of cryptography, NSA is called upon to provide technical analysis and input regarding the export control of cryptographic products.

4. Policies concerning the export control of cryptographic products are based on the fact that the proliferation of such products will make it easier for foreign intelligence targets to deny the United States Government access to information vital to national security interests. Cryptographic products, including software, have various intelligence applications. As demonstrated throughout history, encryption has been used to conceal foreign military communications, on the battlefield, aboard ships and submarines, or in other military settings.[2] Encryption is also used to conceal other foreign communications that have foreign policy and national security significance for the United States. For example, encryption can be used to conceal communications overseas of terrorists, drug smugglers, or foreign governments or entities intent on taking hostile action against U.S. facilities, personnel, or security interests.

II. NSA Technical Evaluation of Snuffle

5. On July 23, 1992, the National Security Agency received a copy of Daniel Bernstein's "Snuffle 5.0" encryption software program for a determination as to whether it was subject to export licensing controls for cryptographic software than administered by the Department of State. Snuffle 5.0 is cryptographic software in source code form that implements Dr. Bernstein's "Snuffle" cryptographic algorithm. Some background is necessary. A "cryptographic algorithm" is a mathematical

---

2. See, e.g., *The Code Breakers: The Story of Secret Writing*, by David Kahn (MacMillan Publishing Inc. 1967).

function or equation that can be applied to transform data into an unintelligible form (i.e., into ciphertext). A cryptographic "source code" is a computer program that expresses a cryptographic algorithm in a precise set of operating instructions that enable a computer to perform cryptographic functions. "Fortran" and "C" are examples of computer programming languages used by computer programmers for writing source code that enable a cryptographic algorithm to be used on a computer. Source code can, in turn, be "compiled" by another computer program into "object code," which is a series of "ones" and "zeros" that may directly be executed by a computer. Software compilers to automatically perform this conversion function are commonly available at computer retail outlets. With such software loaded, compiling source code into object code is a trivial task that can take a matter of seconds. Therefore, for purposes of export controls, there is little meaningful distinction between encryption source code and object code, since source code can easily, readily, and quickly be turned into object code executable on a computer to encrypt information.

6. Snuffle cryptographic source code is freestanding, that is, it has not been incorporated into a particular software application, such as word processing or electronic mail. In such a form, Snuffle source code could be incorporated in a variety of ways into a variety of software applications to provide a data confidentiality function. Cryptographic software, like Dr. Bernstein's Snuffle software, is considered to be a functioning cryptographic product because such software is itself the commodity that can be used to, and is essential to, encrypting data on a computer system. It is not merely "know how" that explains how cryptography works, or a description of scientific ideas or information related to cryptography. Nor is source

code like a "blueprint" diagraming how a particular item is to be built, or information that describes the separate parts or ingredients that go into building an item. Nor does source code merely "describe" how the software functions. Rather, source code like Snuffle is the actual commodity that, when compiled, enables a computer to perform a cryptographic function for general data confidentiality -- that is, to encrypt and decrypt communications. Such software constitutes the "engine" for a cryptographic function that transforms information from plaintext into ciphertext.

III. District Court Injunction

7. The district court's order issuing a limited stay pending appeal left in place an injunction against the government from enforcing the Export Administration Regulations' export licensing requirements with respect to the appellee, Daniel J. Bernstein, and his Snuffle 5.0 software, and any updated versions of this software that implement the same cryptographic system. Dr. Bernstein described the functional capacity of his "Snuffle 5.0" software, stating it allows individuals to exchange encrypted text with "zero-delay," meaning that "Snuffle can be used for interactive conversations: each character typed by one person can be encrypted, sent to the person, and decrypted by the other person immediately." He added that Snuffle "can be used for various applications requiring (private key cryptography) including the example above of interactive text exchange."

8. The district court's order would allow Dr. Bernstein to export Snuffle 5.0 and updated versions of Snuffle 5.0 that have never been presented to the government for any assessment of the national security impact of such software. This would permit Dr. Bernstein to modify and enhance the practical application and use of his software. Also, as noted Snuffle 5.0 is presently "free-standing," and Dr. Bernstein could modify

the software to enable it to easily interface with existing standard computer applications, such as word processing and electronic mail. In addition, it is possible that Snuffle could also be modified and updated for commercial applications and use. In sum, the injunction not only permits Dr. Bernstein to export Snuffle 5.0, a type of encryption software that the President has determined should be subject to export licensing controls for national security and foreign policy reasons, but also extends to "updated versions" of the original Snuffle cryptographic system. This would enable plaintiff to create and export new and better products that could significantly increase the practical use and availability abroad of his software programs.

9. As stated in the Declaration of William A. Reinsch, one version of Snuffle is now apparently available overseas on the Internet. This does not negate the need for export controls on Dr. Bernstein's Snuffle software programs. As noted, modified and improved versions of Snuffle would be exportable under the district court's order. Also, multiple means exist for exporting cryptographic software, not merely through Internet transmission. Although an export by such means poses a harm to the government's interests, such a harm is compounded by further unlimited export by any means, for any purposes, to any person, entity, group, or government, and in any quantity.

10. Beyond this, as the President noted, "facts and questions concerning the foreign availability of such encryption products cannot be made subject to public disclosure or judicial review without revealing or implicating classified information that could harm United States national security and foreign policy interests." E.O. 13026, § 1(a). Facts concerning the NSA's ability to gather intelligence information abroad, including dealing with the threat of foreign available encryption, are among

the most sensitive and classified national security information that cannot be publicly disclosed. The United States is not the sole possessor of sophisticated encryption in the world -- a fact that the NSA must deal with every day in carrying out its critical mission. That mission is inherently complicated if more and better sophisticated encryption products from the United States are made readily available overseas, by any means of export, for any purpose (commercial or otherwise), to any person, entity, group, or government, and in any quantity. While precise estimates would be difficult to make until it is known how a particular encryption product, will be deployed, the uncontrolled export of encryption products heretofore subject to licensing, such as Snuffle and its upgrades, can certainly be expected to further harm the governments's critical mission of obtaining intelligence information abroad on national security and military matters. For these reasons, I believe the injunction entered by the district court creates a serious risk of irreparable harm to the interests of the United States.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: September 8, 1997

William Crowell

WILLIAM P. CROWELL