CINDY A. COHN, ESQ.; SBN 145997
McGLASHAN & SARRAIL
Professional Corporation
177 Bovet Road, Sixth Floor
San Mateo, CA 94402
Tel: (415) 341-2585
Fax: (415) 341-1395

LEE TIEN, ESQ.; SBN 148216
1452 Curtis Street
Berkeley, CA 94702
Tel: (510) 525-0817

Attorneys for Plaintiff
Daniel J. Bernstein

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN )
) C 95-00582 MHP
Plaintiff, )
) DECLARATION OF
v. ) MATTHEW BISHOP
) )
UNITED STATES DEPARTMENT OF )
STATE et al., ) )
Defendants. )
) _____)

I, MATTHEW BISHOP, hereby declare:
1. I am currently an assistant professor of computer science at the University of California at Davis. I have been a fulltime professional computer scientist since 1984, when I graduated from Purdue University. I have worked in the area of computer security since 1979, and have taught computer security at the graduate and undergraduate level since 1987 when I joined the faculty at Dartmouth College.
2. From 1984 to 1987 I was a research scientist at the Research Institute for Advanced Computer Science at NASA Ames Research Center, and I helped implement security measures for the computers at the Numerical Aerodynamic Simulation supercomputing facility at NASA Ames Research Center.
3. Computer and network security has three aspects: 1) confidentiality, the ability to keep data private; 2) authentication, the ability to identify both the sender of a message and that the message did not change in transit; and 3) availability, that the message could be sent and received. Of these three, the first two require cryptography, yet only the first, confidentiality, is controlled by the ITAR.
4. Confidentiality technology can be best understood through analogy. Let's say you and I want to send messages to one another but keep anyone else from seeing them. Since this is a legal document, let's say you are my attorney and we are discussing information which is privileged. How can we do this?
5. Cryptography is analogous to putting the messages into a locked safe and having a courier carry the safe between us. We know the combination, but no-one else does. The only way the privileged information can become known is if one of us reveals the combination or the information. The courier information cannot reveal the information even by accident; the protection is very clear and clean. This technique is called "physical protection" because an attacker (who is trying to get the information) can't get access to the physical medium over which the message is conveyed - in this case, the paper it's written on. To do so, the

attacker would have to cut through the safe.
6. Our solution of the safe may be theoretically possible, but it's unrealistic. (Look at what couriers charge for carrying 2-pound packages!) Cryptography provides more practical physical protection. Instead of using a safe, the sender simply uses mathematics to scramble the message; the recipient unscrambles it. Now, if the courier accidentally mislays the message, the confidential information will be indecipherable to anyone but you or me. Note this also means we want a strong scrambler, just like we would want a strong safe. If it's not strong enough, the message can be read (with effort) by someone else. And if lots of money or an important issue were at stake, the effort would be worthwhile.
7. Now, back to computer networks. While couriers carry messages in their hands, computer networks carry messages in wires and radio waves. How can we keep those messages confidential as they fly through the air on radio waves or through telephone wires? The same way: we scramble those messages. Then, even if someone else intercepts those messages, that person cannot read them, and our communication is still confidential.
8. Now, why is this important on the Internet? One clear reason is commerce, since no one will want to put their credit card number or bank information out into public. Yet putting this information into an unscrambled Internet message effectively makes it publicly available, or at least available to anyone on any system that the message passes through on the way to its destination. Since an Internet message passes through many computer systems, any person with access to any of those computer systems could read an unscrambled credit card number and use it. Even though such misuse of credit card numbers is a crime, it still happens, and is quite painful to deal with.
9. Another important use of cryptography in my work is the protection of sensitive research data as it is shared between me and my research colleagues. A major part of my research is the study of vulnerabilities in computer systems: why they arise and how to fix them, and how to prevent them from recurring in future systems. In order to understand the origin of vulnerabilities, they must be collected and classified, and the information that my colleagues and I exchange often includes attack scripts, which are "cookbooks" for breaking into computer systems. These demonstrate that a vulnerability exists, and from the script we can determine precisely what the vulnerability is.
10. My colleagues and I have been exchanging data over the Internet since 1985, because its ability to move data quickly from one point to another is very convenient. Without the Internet, we would have to mail floppy disks to one another, adding days -- if not weeks --to our exchanges.
11. I exchange this data only with research colleagues I know very well and trust highly, although some of them are not U.S. citizens. I would not want this information available to people I don't know, since if they were irresponsible or malicious they could do incalculable damage to many computer systems. So, before sending the data (which is stored on systems not on the Internet), I use cryptography to scramble the data on the system which is not connected to the Internet, move the scrambled text to a system on the Internet, and then send that. I shudder to think how we could handle this information without encryption!
12. Now, how does the ITAR impact all this? ITAR treats cryptographic software as a munition, meaning you need government permission to export strong cryptographic software.
13. This means that I can't use strong cryptography to send my research data to foreign colleagues or my credit card number to merchants and instead either use weak cryptography or must find other, less efficient means to transport my data. If I use weak cryptography unknown interlopers can easily intercept my data. If I use other means, my work is greatly complicated and slowed, since I cannot use the same mode of communication for U.S. and foreign colleagues unless the foreign colleagues have somehow obtained the same cryptography, written a program compatible with my enciphering program, and done without my giving them any software.
14. I fear that ITAR's restrictions aid criminals who want access to confidential Internet data by preventing me and others from properly protecting this information when we send it to others on the Internet. This leaves information ranging from credit card numbers to sensitive computer security research data much more vulnerable to criminals. I hope the above shows why.
I declare under penalty of perjury that the foregoing is true and correct.

Dated:_____ _____
MATTHEW BISHOP