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

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

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

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 **DECLARATION OF BRUCE SCHNEIER IN SUPPORT OF PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT** HEARING DATE: August 2, 2002 TIME: JUDGE: Marilyn Hall Patel

I, BRUCE SCHNEIER, hereby declare:

1. I am the Chief Technical Officer of Counterpane Internet Security, Inc., a network-security monitoring company I founded in 1999. Before that, I was the President of Counterpane Systems, a consulting firm specializing in cryptography and computer security. I am the author of seven books on cryptography and computer security, including Applied Cryptography: Protocols, Algorithms, and Source Code in C, the second edition of which was

published in 1996 by John Wiley &Sons, and of E-Mail Security, published in 1995 by John Wiley &Sons. I have published dozens of academic papers on cryptography, and have lectured on the subject around the world. I have been a member of the board of directors of the International Association for Cryptologic Research, and have chaired several cryptography research conferences.

2. Except as expressly stated below, I have personal knowledge of the facts stated herein. If called upon to testify, I would competently testify to these facts.

The One-Time Pad

3. There is an encryption system, called the "one-time pad," that is provably unbreakable.

4. The system is suitable for hand use, and can be adapted for computers. Both the hand system and the computer system can be mathematically proven to be secure. That is, it is mathematically impossible for someone to break a message encrypted with a one-time pad. This impossibility is not based on technology, or understanding, or any future mathematical breakthroughs. A one-time pad is provably secure.

5. The hand system involves a key the same length as the message. The key is a series of letters. These key letters are "added" to the message letters "modulo 26": A + A = B, A + B = C, A + C = D, . . . , A + Z = A, B + A = C, B + B = D, etc. For example, if the message is ONETIMEPAD and the key sequence is TBFRGFARFM, then the encrypted message is IPKLPSFHGQ. This is because O + T = I, N + B = P, E + F = K, etc. At the other end, the receiver "subtracts" the key sequence from the encrypted message to recover the original message.

6. An eavesdropper who does not know the key sequence cannot decrypt the message. There is no amount of computing power or mathematical theory that can change this fact.

7. The computer system is the same as the hand system, except that bits (0 and 1) are used instead of letters. The message bits are added to the key bits “modulo 2” to create the encrypted message: 0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 0. The key bits are subtracted from the encrypted message to recover the original message.

8. To initialize the one-time pad, the sender and receiver meet and create a completely random stream of key letters (or bits). They can do this by flipping coins, rolling dice, etc. Both the sender and the receiver must keep copies of this key stream.

9. At a later time, when the sender wants to send a message, he encrypts it using the key stream previously generated and the algorithm described above. After doing so, he destroys the key stream and sends the message. The receiver uses the same key stream to recover the original message.

10. The eavesdropper cannot possibly break the encrypted message. Because every key sequence is equally likely, the eavesdropper has no information with which to analyze the encrypted message. To use the example above, assume that the eavesdropper recovered the message IPKLPSFHGQ. He has no way of knowing that the real key is TBFRGFARFM and the real message is ONETIMEPAD. The key and message could be POYYAEAAZX and SALMONEGGS, or BXFGBMTMXM and GREENFLUID. Because all keys of the same length are equally likely, the eavesdropper cannot tell which one is correct. This same reasoning holds true for bits as it does for letters.

11. Although unsuitable for most applications, a one-time pad can be used in practice to guarantee secrecy of low-volume communication among small groups of people. As an illustration (reported to be a real example, but also valid as a hypothetical example), the one-time pad can be used to guarantee secrecy of “hot line” messages between the government leaders in Washington and Moscow.

12. Because the key must be the same size as the message, the cost of setting up a one-time pad system grows with the volume of communication. Therefore, this technology does not scale to protecting billions of Internet messages. Modern cryptographic techniques do not have the same security guarantee, but they are much less expensive to use. On the other hand, people who want an absolute mathematical guarantee can get it.

13. These facts have been presented in textbooks for many years. Much of what I wrote here is adapted from my 1994 book: Applied Cryptography. The invention of the one-time pad is generally credited to Gilbert Vernam and Joseph Mauborgne in 1917.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct and that this declaration was executed on this _____ day of April, 2002.

____

BRUCE SCHNEIER