

Department of Justice Letter on Keystroke Monitoring and Login Banners.

This document is comprised of two parts. The first is a scan of the Department of Justice memo on keystroke monitoring and login banners as it was passed to me. The second is the same document that has been passed through OCR software to extract the text into a machine readable form. ---W. J. Orvis



U.S. Department of Justice
Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

OCT 7 1992

Mr. James H. Burrows
Director, Computer Systems Laboratory
National Institute of Standards & Technology
U.S. Department of Commerce
B-154 Technology
Gaithersburg, Maryland 20899

Dear Mr. Burrows:

It has come to our attention that keystroke monitoring, a process whereby computer system administrators monitor both the keystrokes entered by a computer user and the computer's response, is being conducted by government agencies in an effort to protect their computer systems from intruders who access such systems without authority. We recognize that the unauthorized use of computers, particularly the insertion into a computer system of malicious code (e.g., viruses or worms) and backdoors (programming code that allows an intruder to reenter a system even if compromised passwords are changed), poses a serious threat to the integrity of that system and that keystroke monitoring is the most feasible means to assess and to repair the damage done by such activity. However, we have reviewed the legal propriety of such monitoring of the activities of intruders and, since you are responsible for providing computer security guidance to the federal government, I wish to share our legal conclusions with you. I would also appreciate it if you would, to the extent and in the manner you deem appropriate, circulate this letter to your colleagues in the federal government who are confronted with the keystroke monitoring issue.

The legality of such monitoring is governed by 18 U.S.C. § 2510 et seq. That statute was last amended in 1986, years before the words "virus" and "worm" became a part of our everyday vocabulary. Therefore, not surprisingly, the statute does not directly address the propriety of keystroke monitoring by system administrators.

Attorneys for the Department have engaged in a review of the statute and its legislative history. We believe that such keystroke monitoring of intruders may be defensible under the statute. However, the statute does not expressly authorize such monitoring. Moreover, no court has yet had an opportunity to rule on this issue. If the courts were to decide that such monitoring

1
2
3

is improper, it would potentially give rise to both criminal and civil liability for system administrators. Therefore, absent clear guidance from the courts, we believe it is advisable for system administrators who will be engaged in such monitoring to give notice to those who would be subject to monitoring that, by using the system, they are expressly consenting to such monitoring. Since it is important that unauthorized intruders be given notice, some form of banner notice at the time of signing on to the system is required. Simply providing written notice in advance to only authorized users will not be sufficient to place outside hackers on notice.

An agency's banner should give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring. The banner should also indicate to authorized users that they may be monitored during the effort to monitor the intruder (e.g., if a hacker is downloading a user's file, keystroke monitoring will intercept both the hacker's download command and the authorized user's file). We also understand that system administrators may in some cases monitor authorized users in the course of routine system maintenance. If this is the case, the banner should indicate this fact. An example of an appropriate banner might be as follows:

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Obviously, each agency may want to tailor the banner to its precise needs. In addition to giving notice to users that keystroke monitoring may occur, the system administrator might decide that the banner should also contain a statement explaining the need for such monitoring (e.g., "To protect the system from unauthorized use and to insure that the system is functioning properly, system administrators monitor this system").

Lastly, we would note that the long-term monitoring of individuals using a system without authority, or in excess of their authority, should not be conducted routinely. The monitoring of

such individuals should be limited to the extent reasonable and necessary to determine whether and how the system is being abused. Once that determination is made, the matter should be reported to law enforcement for consideration as to whether court orders authorizing continued monitoring should be obtained.

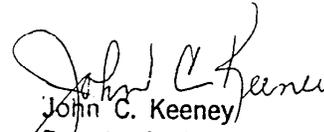
In sum, we believe that each banner should be crafted by the agency involved to fulfill its specific needs. At a minimum, however, those individuals who are using computers without or in excess of their authority, and those authorized users who are subject to monitoring, should be told expressly that by using the system they are consenting to such monitoring.

Your cooperation in this matter is appreciated.

Sincerely,

Robert S. Mueller, III
Assistant Attorney General
Criminal Division

By:


John C. Keeney
Deputy Assistant Attorney General
Criminal Division



U.S. Department of Justice
Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

OCT 7 1992

Mr. James H. Burrows
Director, Computer Systems Laboratory
National Institute of Standards & Technology
U.S. Department of Commerce
B-154 Technology
Gaithersburg, Maryland 20899

Dear Mr. Burrows:

It has come to our attention that keystroke monitoring, a process whereby computer system administrators monitor both the keystrokes entered by a computer user and the computer's response, is being conducted by government agencies in an effort to protect their computer systems from intruders who access such systems without authority. We recognize that the unauthorized use of computers, particularly the insertion into a computer system of malicious code (e.g., viruses or worms) and backdoors (programming code that allows an intruder to reenter a system even if compromised passwords are changed), poses a serious threat to the integrity of that system and that keystroke monitoring is the most feasible means to assess and to repair the damage done by such activity. However, we have reviewed the legal propriety of such monitoring of the activities of intruders and, since you are responsible for providing computer security guidance to the federal government, I wish to share our legal conclusions with you. I would also appreciate it if you would, to the extent and in the manner you deem appropriate, circulate this letter to your colleagues in the federal government who are confronted with the keystroke monitoring issue.

The legality of such monitoring is governed by 18 U.S.C. § 2510 et seq. That statute was last amended in 1986, years before the words "virus" and "worm" became a part of our everyday vocabulary. Therefore, not surprisingly, the statute does not directly address the propriety of keystroke monitoring by system administrators.

Attorneys for the Department have engaged in a review of the statute and its legislative history. We believe that such keystroke monitoring of intruders may be defensible under the statute. However, the statute does not expressly authorize such monitoring. Moreover, no court has yet had an opportunity to rule on this issue. If the courts were to decide that such monitoring is improper, it would potentially give rise to both criminal and civil liability for system administrators. Therefore, absent clear guidance from the courts, we believe it is advisable for system administrators who will be engaged in such monitoring to give notice to those who would be subject to monitoring that, by using the system, they are expressly consenting to such monitoring. Since it is important that unauthorized intruders be given notice, some form of banner notice at the time of signing on to the system is required. Simply providing written notice in advance to, only authorized users will not be sufficient to place outside hackers on notice.

An agency's banner should give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring. The banner should also indicate to authorized users that they may be monitored during the effort to monitor the intruder (e.g., if a hacker is downloading a user's file, keystroke monitoring will intercept both the hacker's download command and the authorized user's file). We also understand that system administrators may in some cases monitor authorized users in the course of routine system maintenance. If this is the case, the banner should indicate this fact. An example of an appropriate banner might be as follows:

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Obviously, each agency may want to tailor the banner to its precise needs. In addition to giving notice to users that keystroke monitoring may occur, the system administrator might decide that the banner should also contain a statement explaining the need for such monitoring (e.g., "To protect the system from unauthorized use and to insure that the system is

functioning properly, system administrators monitor this system").

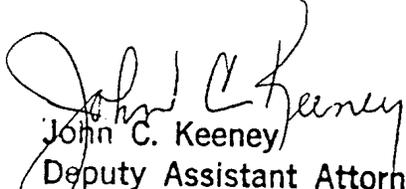
Lastly, we would note that the long-term monitoring of individuals using a system without authority, or in excess of their authority, should not be conducted routinely. The monitoring of such individuals should be limited to the extent reasonable and necessary to determine whether and how the system is being abused. Once that determination is made, the matter should be reported to law enforcement for consideration as to whether court orders authorizing continued monitoring should be obtained.

In some, we believe that each banner should be crafted by the agency involved to fulfill its specific needs. At a minimum, however, those individuals who are using computers without or in excess of their authority, and those authorized users who are subject to monitoring, should be told expressly that by using the system they are consenting to such monitoring.

Your cooperation in this matter is appreciated.

Sincerely,

Robert S. Mueller, III
Assistant Attorney General
Criminal Division

By: 
John C. Keeney
Deputy Assistant Attorney General
Criminal Division