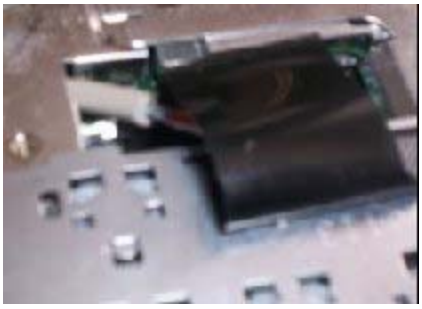
Since posting this article, there has been overwhelming attempts to disprove this threat to our privacy. To the extent that I had to rename the link to avoid so many hits.
To me, any attempt so massive designed to turn a credible story into a so called hoax is pretty convincing evidence that someone out there doesn't want the truth to be known.
To all people attempting to destroy this story's credibility, it is possible to do this, and it is being done. The KeyLogger business is real, Look up KeyGhost on Google.. The US government has been admitting to spying on US citizens using the massive AT&T servers to log and record EVERY email that is sent in this country and listening to any phone calls that might interest them, are you so gullible that you really think the industry that makes computers couldn't be forced to build in these devices ? Think for yourselves people. Do not trust a government that blatantly admits to violating the laws that provide your right to privacy.

GOVERNMENT AND COMPUTER MANUFACTURERS CAUGHT INSTALLING HARD-WIRED KEYSTROKE LOGGERS INTO ALL NEW LAPTOP COMPUTERS!

Turner Radio Network | October 4, 2005

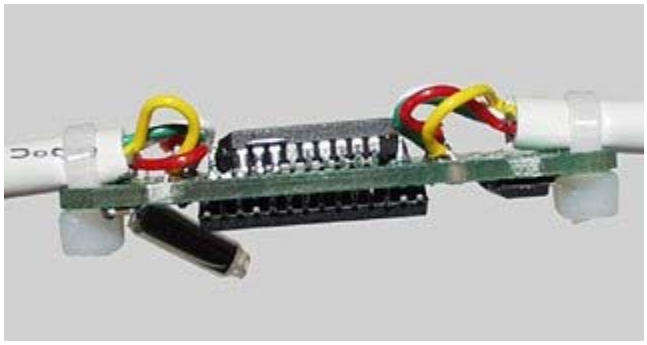
Devices capture everything you ever type, then can send it via your ethernet card to the Dept. of Homeland Security without your knowledge, consent or a search warrant each time you log onto the internet!



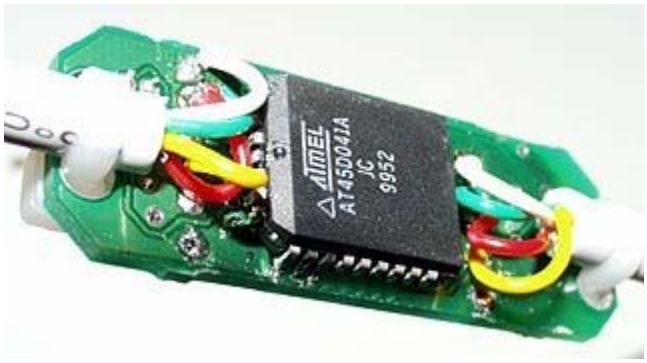
Freedom Of Information Act Requests For Explanation From DHS, refused.

I was opening up my almost brand new laptop, to replace a broken PCMCIA slot riser on the motherboard. As soon as I got the keyboard off, I noticed a small cable running from the keyboard connection underneath a piece of metal protecting the motherboard.

I figured "No Big Deal", and continued with the dissasembly. But when I got the metal panels off, I saw a small white heatshink-wrapped package. Being ever-curious, I sliced the heatshrink open. I found a little circuit board inside.



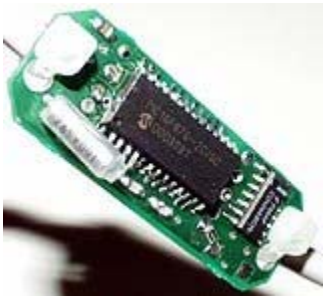
Being an EE by trade, this piqued my curiosity considerably. On one side of the board, one Atmel AT45D041A four megabit Flash memory chip.



On the other side, one Microchip Technology PIC16F876 Programmable Interrupt Controller, along with a little Fairchild Semiconductor CD4066BCM quad bilateral switch.

Looking further, I saw that the other end of the cable was connected to the integrated ethernet board.

What could this mean? I called the manufacturer's tech support about it, and they said, and I quote, "The intregrated service tag identifier is there for assisting customers in the event of lost or misplaced personal information." He then hung up.



A little more research, and I found that that board spliced in between the keyboard and the ethernet chip is little more than a Keyghost **hardware keylogger** .

The reasons a computer manufacturer would put this in their laptops can only be left up to your imagination. It would be very impractical to hand-anylze the logs, and very CPU-intensive to do so on a computer for every person that purchased a laptop. Why are these keyloggers here? I recently almost found out.

I called the police, as having a keylogger unknown to me in my laptop is a serious offense. They told me to call the Department of Homeland Security. At this point, I am in disbelief. Why would the DHS have a keylogger in my laptop? It was surreal.

So I called them, and they told me to submit a Freedom of Information Act request. This is what I got back:

DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
WASHINGTON, D.C. 20223

Freedom of Information and Privacy Acts Branch
245 Murray Drive
Building 410
Washington, D.C. 20223

[redacted]

File Number: [redacted]

Dear Mr. [redacted]

We have reviewed your Freedom of Information Act request, and have found that the requested records are exempt from being disclosed under FOIA. The decision to withhold this information may be appealed in writing to the Secretary of the Department of Homeland Security. Any appeal should include the reasons for reconsideration, a copy of this letter, and should be postmarked no later than 60 days from the date of this letter.

If you have any questions, please contact [redacted] at [redacted]

Sincerely,

Kathy J. Lyerly
SAIC
Freedom of Information &
Privacy Acts Officer

Under the Freedom Of Information Act (FOIA) the only items exempt from public disclosure are items relating to "law enforcement tools and techniques" and "items relating to national security."

The real life implications of this are plain: Computer manufacturers appear to be cooperating with the Department of Homeland Security to make every person who buys a new computer subject to **immediate, unrestricted government recording of everything they do on those computers! EVERYTHING !**

This information can be sent to DHS, online, without your knowledge or consent, without a search warrant or even probable cause! That's why this device is hard-wired directly into the ethernet card, which communicates over the internet!

I am not certain how long this information will be permitted to remain online for all the world to see before the government takes some type of action to attempt to have it removed from public view. I URGE you to take copy of this page immediately and spread this information to everyone you know immediately! The more people who find out about this, the more can protect themselves and raise a HUGE outcry to force government and computer manufacturers to immediately CEASE installing these devices in new computers!