From: [redacted] <[redacted]@MIT.EDU>
Sent: Wednesday, January 5, 2011 3:51 PM
To: [redacted] <[redacted]@ithaka.org>
Cc: [redacted] <[redacted]@mit.edu>; [redacted] <[redacted]@mit.edu>; [redacted] <[redacted]@mit.edu>; [redacted] <[redacted]@mit.edu>; [redacted] <[redacted]@mit.edu>
Subject: Update from MIT on excessive use case

[redacted],
I've just had an update from [redacted] of our network security team. The investigation has moved beyond MIT and is now being handled by law enforcement, including federal law enforcement. It is likely that the individual involved will be identified. At least one external hard drive that was being used to store the JSTOR content has been secured. The machine through which the misuse occurred is still live, pending further steps in the investigation, as noted this morning.

We have begun sending out the messages to our staff and community to alert them to an upcoming change in JSTOR access to take effect Monday or Tuesday. Once we confirm to you – most likely on Monday -- that we've made the necessary configuration changes on this end, we will ask you to update MIT's authorized IP ranges to include only the address of our proxy server: 18.7.29.240.

One fact that emerged in the investigation is that JSTOR's block of 18.55.6.* was not working. After you reported that a block was in place, JSTOR content was still being downloaded through an address in that IP range.

We'll be in touch early next week to confirm the timing of the switch. Please let me know if you have any other questions at this time.

Best,
[redacted]

[redacted]
[redacted]
MIT Libraries
P [redacted]
[redacted]@mit.edu
http://libraries.mit.edu/scholarly