SCIENTIFIC/EDUCATIONAL/NEWS.MEDIA
00 FREE PAGES
JUN 30 2009
04

Dear Stephanie,

This letter follows up on our Friday discussion (June 19) among staff at the Department of Energy and The Associated Press regarding terms under which DOE will provide AP with its database reflecting Web visits by agency computer users as recorded by Web filtering software. Below please find AP's proposal, which we believe balances the concerns DOE staff expressed with the principle that overly broad restrictions would effectively undermine the request.

Before getting into details, I'd like to say that I have been encouraged by DOE's openness to working out an arrangement. The agency's approach thus far appears to be right in line with Attorney General Holder's guidance in March that, among other things, "open government requires agencies to work proactively and respond to requests promptly." I am confident that we can soon reach an agreeable framework.

A) First, a recap. In broadest terms, AP seeks the following information: Each row of the database is a unique Web site visit. The columns of the database would include but not necessarily be limited to: URL address visited; URL connectivity start time; URL connectivity termination time; what software-assigned URL address "category code" the URL address falls into; and a way of identifying which computer visited the site without identifying the computer user (if for security reasons not actual IP addresses, some code that will allow us to bundle together URL visits and associate them with one computer or one user).

B) Next, let me summarize four specific classes of concerns that DOE staff expressed on our June 19 call:

1- PRIVACY: Sites that could compromise the personal privacy of DOE computer users;

2- BLOCKED: Sites DOE is blocking for reasons that might not be immediately clear (example given was an apparently rose growing enthusiasts' site which in fact contains malicious code);

3- PROCUREMENT: Sites that reflect procurement activity;

4- RESEARCH: Sites that reflect new technology research;

C) Below is AP's proposal for how to deal with each of these concerns. Please note that I have grouped Nos. 3 and 4 under a general "confidential" activities rubric; that makes sense because while different in their particulars, they share this core attribute.

-- AP's PRIVACY Proposal: We acknowledge and appreciate federal employees' right to personal privacy and do not request information that has a legitimate chance of compromising that privacy.

There are two ways privacy could, theoretically, be compromised: (1) the revealing of information such as a logon or PIN or the tying of an individually identified user -- for example, by a computer's IP address, if that IP address is static; or (2) a Web site that reveals something private about that individual user, if that Web site can be directly associated with that individual user.

We believe both issues are readily addressed. Regarding the first concern, the database we have described does not record any information such as logons or PIN numbers, and thus there is no risk that this kind of information would be contained in what DOE provides AP. We see how, in limited cases, the second concern above could be an issue. Thus, we propose that DOE does not include in the database information that could individually identify a user. At the same time, we do request a way to associate different URL requests with the requesting computer. If DOE assigns a static IP address to its computers, we request that DOE replaces each IP individual address with a numerical code, beginning at 1; so, for example, a DOE user's computer at IP address 12.345.678.90 would become user 1, the user at IP address 12.345.678.91 would become user 2 and so forth. If DOE assigns dynamic IP addresses to its computers, we would like to discuss some way to associate individual computers or individual users with their URL requests in a way that protects their personal privacy. Whatever the case -- dynamic or static – we propose a solution that would eliminate the chance that anyone could figure out which individual user is going to which specific Web sites based on IP address, thus solving the second privacy concern.

-- AP's BLOCKED Proposal: The AP's request does include Web site connections that users attempted to make but that were blocked by the filtering program. One feature of the filtering program is routine (daily, if not more

FOIA - 2009 - 00517

often) updates to reflect known malicious sites. That list is available to any user. It is hard to envision how providing AP with blocked attempts by DOE users would reveal anything about DOE's own security measures. If, however, DOE has added any sites to its blacklist, *independent of the list maintained by the software provider*, we would accept the redacting of the specific URL on any attempted connection to those DOE-added sites, as long as the category code for the URL for which the connection attempt was not successful was still listed.

-- AP's CONFIDENTIAL ACTIVITES Proposal: DOE should be able to withhold individual URLs (but not category codes for the URLs) for confidential procurement and confidential new technology research Web requests, within reasonable limits. These are the URLs that AP proposes can be redacted (but not category codes for the URLs):

a) URLs that reflect aspects of a specific, and currently *active* procurement matters that have not yet been resolved;
b) URLs that reflect procurement or new technology research which is not otherwise open or known to the public. That is, DOE cannot withhold a URL if it is part of a public proposal, bidding or procurement process;
c) The URL cannot be part of research which is otherwise part of normal operations or otherwise accessed in other capacities (and would therefore give no hint as to whether it was accessed for procurement only);
d) In all cases, for any URL that is redacted, we request that the category code be included.

We believe that the parameters set forth above effectively address DOE's concerns while not being so restrictive as to eviscerate AP's request. We also believe these limits are in accord with our understanding of FOIA, the relevant law, and FOIA's presumption of disclosure, including as reiterated recently by President Obama and Attorney General Holder. We also recognize that DOE may wish to respond with further thoughts, and we welcome that communication.

Thanks again for the time and care you are paying this important request.

Best regards,

Justin

Justin Pritchard
Reporter
Based in AP's Los Angeles Bureau
(o) 213-346-3192 -- (c) 213-280-2263