The Heartland Institute
Investigative Report
April 20, 2012
INVESTIGATIVE REPORT

Protek International, Inc. ("Protek") was retained to investigate whether a document posted on the Internet entitled "Confidential Memo: 2012 Heartland Climate Strategy" ("Memo") is a document originating at The Heartland Institute ("Heartland").

Protek is a Chicago-area firm specializing in investigations and computer forensics services established in 2005 by Daniel Bellich and Keith Chval. Bellich is a highly awarded veteran of 27 years in the F.B.I. During his tenure he had a wide range of responsibilities including investigating complex white collar crimes and internal affairs investigations. Chval previously served as a prosecutor, forming and supervising the Illinois Attorney General’s computer crimes unit, one of the first specialized units of its kind in the country. Ronald Weiss is the lead computer forensics examiner assigned to this matter. He holds the EnCE computer forensics certification conferred by Guidance Software, Inc. Weiss previously supervised the Illinois Attorney General’s Springfield regional computer forensics laboratory from 2004 to 2005, and was subsequently employed by Computer Sciences Corporation, detailed to the Department of Defense’s Cyber Investigations Training Academy training the Department’s computer forensic examiners and investigators. Further descriptions of Mr. Chval’s, Mr. Bellich’s, and Mr. Weiss’s backgrounds and qualifications are attached.

Protek began its investigation on February 16, 2012. The investigation included conducting interviews of Heartland personnel, collecting and analyzing over 7.8 TerraBytes of electronically stored information ("ESI") which consisted of the universe of Heartland Chicago office user created files and email ("the Heartland System"), as well as examining the Memo itself.

Based upon our investigation and computer forensic analysis, our conclusion is that the Memo was not created on Heartland’s computer systems and never existed there, or within Heartland’s email systems, prior to its posting online on February 14, 2012.

INVESTIGATIVE AND COMPUTER FORENSICS OBJECTIVE

Heartland personnel informed Protek that a document was posted on-line on February 14, 2012 which was being described as a confidential Heartland document. Heartland stated that it was not a Heartland document and asked Protek to determine whether the Memo originated on the Heartland System.
SUMMARY OF KEY EVENTS RELATED TO THE MEMORANDUM

Between January 27, 2012 and February 8, 2012, someone using an email address falsely purported to belong to a Heartland board member obtained electronic copies of certain Heartland documents (the “Heartland Documents”). On February 14, 2012, an individual using a GMail account of “heartlandinsider@gmail.com” distributed the Heartland Documents and the Memo to some number of individuals, claiming all of the documents to be from Heartland. Those documents then appear to have been first posted online the same day, including at “www.desmogblog.com.”

HEARTLAND PERSONNEL DENY BOTH AUTHORSHIP AND PRIOR KNOWLEDGE

Protek met with and conducted interviews of several Heartland employees subsequent to the February 14 online publication of the purported Heartland documents, focusing on those who were part of the e-mail communications and transmission of documents in response to their online solicitation. In addition, Protek also interviewed senior officers of Heartland including Joseph Bast, Diane Bast, and Kevin Fitzgerald. Everyone interviewed by Protek stated that they had either not seen the Memo, or had not seen it prior to its being posted online on February 14th and all denied creating it as well.

SEARCHES OF HEARTLAND’S SYSTEMS: EMAIL

Protek conducted extensive, advanced forensic searches for the Memo across the entire universe of Heartland email data present on its Exchange server. Heartland manages all Institute in-bound and out-bound email through its Exchange 2003 server. The server was located within Heartland’s office suite.

Email Preservation

To both preserve and collect the email data prior to conducting searches, Protek personnel first copied out Heartland’s entire Exchange Node Database, or “NDB” data folder, to include the Exchange Data Base (“EDB”), in a forensically sound manner to ensure that no changes to the data were made through this process. FTK Imager, by Access Data Corp., a tool generally accepted for such use within the computer forensics community, was used to perform this task. Hash values of original and copied data sets were used to verify data integrity. All email data within the NDB data folder for all Heartland employees was collected. The approximate volume of email data collected was 55.6 GigaBytes. Chain of custody documentation was initiated upon collection of the email data, and has been maintained through to present storage of the data within Protek’s secured evidence storage facility.
Protek used specialized tools, including EnCase, by Guidance Software, Inc., X-Ways Forensics, by X-Ways Software Technology AG, and NeedleFinder, by Equivalent Data, Inc., all tools generally accepted for such use within the computer forensics and electronic discovery industries, to search for emails or attachments that might be, or might contain, the Memo either in whole or in part.

Protek’s search of Heartland’s email data to attempt to find the Memo, and any prior or partial version of it was comprehensive. Rather than searching the email of only select employees from whom the Memo or information could reasonably have been expected to come, Protek searched the entire universe of email data from Heartland’s Exchange NDB folder, to include the email of every Heartland employee in the office. Rather than rely upon simply searching by file name, or by searching for files on the Heartland System with hash values that match that of the Memo, Protek created search expressions from content within the Memo in order to provide for the greatest granularity in searching, and therefore the greatest likelihood of finding the Memo, any prior iteration of it, and any fragments thereof.

Specifically, Protek constructed and ran the following search expressions across this data:

- Confidential Memo 2012 Heartland
- Dissuading teachers from
- Revkin at DotEarth
- Dr. Wojick $100,000

These terms were constructed to create the highest probability of finding the Memo intact, any prior iterations of it, or any fragments thereof, if they existed, anywhere within Heartland’s email data. Rather than using less powerful search methodologies such as searching for a file name, or by a hash value “digital fingerprint” of the file, both of which can be intentionally or inadvertently defeated by minimal changes to the file, Protek created expressions from verbiage within the Memo. One would have to delete this specific verbiage within the file, or email, in order to defeat the search expression.

For all of the search expressions, there were approximately 593 total hits within the email data, which break down per search expression as follows:

<table>
<thead>
<tr>
<th>Search Expression</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential Memo 2012 Heartland</td>
<td>536</td>
</tr>
<tr>
<td>Dissuading teachers from</td>
<td>12</td>
</tr>
<tr>
<td>Revkin at DotEarth</td>
<td>18</td>
</tr>
<tr>
<td>Dr. Wojick $100,000</td>
<td>27</td>
</tr>
</tbody>
</table>
A review of the files within which the hits occurred, and the blocks of text surrounding hits that occurred within unstructured unallocated space areas establishes that none were found to have been created prior to when the Memo was posted online, February 14, 2012. The substantive content of the email communications and the related attachments are consistent with Heartland staff members reacting once they were aware of the online postings, and not with creation of the Memo on Heartland systems.

Neither the Memo, nor any prior versions or fragments of it, were found to have existed within Heartland’s Exchange NDB folder prior to the February 14th online posting. Nothing was found through the searches of the Heartland email data to suggest that the Memo was created at Heartland, or ever existed there prior to February 14, 2012.

SEARCHES OF HEARTLAND SYSTEM: SERVER AND HARD DRIVE ESI

Consistent with searches of Heartland’s email data, Protek conducted extensive, advanced forensic searches for the Memo across the Heartland System’s entire user data universe.

ESI Preservation

To both preserve and collect all employee-created ESI on the Heartland System, Protek created full forensic images of all Heartland workstation computers, and also collected user-created ESI from Heartland servers in a forensically sound manner. In addition, Diane and Joseph Bast voluntarily provided access to their privately owned computers, which were imaged and searched using the same methodology as for the Heartland owned computers. These computers consisted of a Dell Dimension 3000, a Dell Dimension 2400, and a Dell Inspiron 530.

In all, forensic images were made of thirty-two Heartland Chicago office computer workstations, as well as the Bast’s privately owned computers. A full forensic image creates an exact duplicate of a system’s hard drive, to literally capture every “1” and “0,” exactly as they exist on the original. This includes fragments of previously existing data found in what is commonly referred to as “unallocated space.”

To authenticate that the forensic image is exactly the same as the content of the original hard drive, an algorithm that generates a 128 character value is run against each set of data. The resultant value is called a “hash value,” in this case, an “MD5 Hash Value.” If the hash values of the two sets of data match, they are considered to be exactly the same, and the forensic image is verified as an exact copy of the original. In essence, a second original.

Protek conducted MD5 Hash Value comparisons of all thirty-five sets of original and forensic image data sets. The hash values for all matched. All thirty-five forensic images are verified to be accurate copies of the originals.
All server resident ESI was collected in a forensically sound manner, meaning that no changes were made to the ESI through the collection process, and Protek now maintains a set of the ESI exactly as it existed at the time of collection. Guidance Software’s EnCase Portable device, as well as its Enterprise electronic discovery tool, were used to collect the server resident ESI. Both tools are generally accepted for such use within the electronic discovery industry.

Note should be made that, in addition to the Chicago office, Heartland also maintains a Washington, D.C. office, and has referenced several satellite offices in its prior publications. Protek determined that it would be very unlikely for a Heartland document of the nature that the Memo purports to be to have been created at any of these locations, and therefore did not collect or search data from these locations. The bases for this determination includes that Heartland’s senior officers, who would be the most likely authors of such a document, work in the Chicago office. In addition, at least some of the information that would be needed to compose the Memo is resident only on the Heartland System.

In total, from all workstation and private computers and server resident ESI, Protek collected approximately 7.3 TerraBytes of data. For perspective, that’s equivalent to 1,932,735,284 pages of paper, which is approximately 3,865,470 reams of paper, which would require about 208 semi trucks for it to be hauled. It is a large volume of data.

Chain of custody documentation was created at the time of forensic imaging, and has been maintained through to the ESI’s current storage within Protek’s secured storage facility.

**Search Methodology**

Again maintaining consistency with searches of email data and the objective to conduct the most thorough search practicable, Protek applied the same comprehensive approach to searches of the server and workstation resident ESI.

To manage the volume of ESI to be searched, searches were focused upon the universe of file types generally associated with user-created text file types. These were identified by the following file extensions, .doc, .docx, .pdf, .rtf, and .wpd. Searches were also conducted within all .zip files.

In addition to searching across “active” ESI, that being what the operating system is actively managing and which a user would typically see when sitting down at their computer, Protek also ran the search expressions across what is commonly referred to as “unallocated space.” This is the storage area of a hard drive that is not being actively managed by the operating system. It is where previously existing files that have since been deleted, and fragments thereof, or even data that a user never even saved (e.g., the user viewed a file, but never saved it to their hard drive), would exist.
Protek ran the same search expressions across the server and workstation ESI as were run across the email data:

- Confidential Memo 2012 Heartland
- Dissuading teachers from
- Revkin at DotEarth
- Dr. Wojick $100,000

In total, there were 1099 hits responsive to the search expressions, which break down as follows:

<table>
<thead>
<tr>
<th>Search Expression</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential Memo 2012 Heartland</td>
<td>196</td>
</tr>
<tr>
<td>Dissuading teachers from</td>
<td>485</td>
</tr>
<tr>
<td>Revkin at DotEarth</td>
<td>357</td>
</tr>
<tr>
<td>Dr. Wojick $100,000</td>
<td>61</td>
</tr>
</tbody>
</table>

A review of the files within which the hits occurred, and the blocks of text surrounding hits that occurred within unstructured unallocated space areas establishes that none were found to have been created prior to when the Memo was posted online, February 14, 2012. The substantive content of the files, or surrounding data in the case of hits in unallocated space, is consistent with Heartland staff members reacting once they were aware of the online postings, and not with creation of the Memo on Heartland System. In addition, all search expression hits occurring within Internet History-related data were all post-February 14th and therefore would not relate to creation of the Memo prior to that date.

Neither the Memo, nor any prior versions or fragments of it, were found to have existed within the Heartland System prior to the February 14th online posting. Nothing was found through the searches of the Heartland System to suggest that the Memo was created at Heartland, or ever existed there prior to February 14, 2012.

**INTERNAL METADATA OF MEMO DOES NOT SUPPORT AUTHENTICITY**

Protek obtained a copy of the Memo for analysis purposes from the “desmogblog” site’s post because it appears to have been one of the first to post it on February 14th, and therefore would be least likely to be degraded by multiple copies and re-posts. The name of the “pdf” file obtained is “2012 Climate Strategy.pdf.”

Typically, an electronic file contains many fields of metadata which can provide a great deal of information about the file, including date and time for when it was originally created, last modified, and last written, the application used to create it, including version...
of the application, operating system of the system upon which it was created, author, and a host of other identifying information.

However, inspection of the Memo’s metadata reveals that it is a scan of a hard copy document to pdf format, rather than the conversion of an electronic document into pdf format. If it were the latter, metadata useful for identifying where and when a document was created, and by whom, would likely be carried forward into the new pdf file’s metadata. In the case of the Memo as posted to desmogblog.com, no metadata from the original electronic file from which the scanned hard copy presumably came is available for inspection.

The Memo scan stands in contrast to the other electronic files Peter Gleick has admitted to disseminating through his February 14th “heartlandinsider” email which represents all attached documents, including the Memo, to be from Heartland. The other attached electronic files all include the kind of metadata that would permit an investigation of the original file, and that would have been critical in attempting to ascertain the authenticity of the Memo.

However, although the metadata from the original electronic Memo file was not carried forward through the scanning to pdf format process, there is metadata associated with the “new” electronic pdf file that was posted on desmogblog. The desmogblog’s Memo’s metadata reveals file Create and Modify date and time stamps for the pdf file of February 13, 2012, at 12:41:52 Pacific Time.

The metadata also includes information that indicates that the scanned Memo file was created by an Epson device. Heartland officials told Protek that it did not have any Epson devices. Protek inspected Heartland’s offices while on-site collecting email and other ESI and searched for, but did not find, an Epson device. In addition, the system Registries of the Bas’s’ privately owned computers were examined and no Epson devices were found to have been attached.

CONCLUSION

On the basis of our comprehensive investigation and searching of Heartland’s email and other ESI, we conclude that the Memo did not originate on the Heartland System. It was not created on the Heartland System and was never present there prior to its February 14, 2012 posting online.

The comprehensive searches of Heartland’s entire Exchange email data, as well as the entire universe of its Heartland System user-created ESI, corroborates Heartland’s employees’ representations that they were not aware of the Memo prior to February 14th, and that it was not created at Heartland. All relevant hits responsive to the search
expressions run across all the data are from after the February 14th posting and are consistent with Heartland employees acting in response to the incident. Moreover, internal metadata from the Memo pdf file, as posted at desmogblog, do not permit an investigation of the Memo’s origins. This metadata merely indicates that the Memo was created through a scan on an Epson device, which was not found in Heartland’s offices, or to have been attached to any of the Basts’ computers.

On the basis of these findings, Protek concludes that the Memo was not created on the Heartland System, and never existed there prior to February 14, 2012.

###

Report submitted by: [Signature] ; Date: 4/20/12

[Signature] ; Date: 4/20/12