

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK

---

NATIONAL DAY LABORER ORGANIZING  
NETWORK, et al.,

Plaintiffs,

v.

U.S. IMMIGRATION AND CUSTOMS  
ENFORCEMENT AGENCY, et al.,

Defendants.

---

Civil Action No.10-CV-3488 (SAS)

**FIFTH DECLARATION OF DAVID M. HARDY**

I, David M. Hardy, declare as follows:

(1) This declaration is submitted in accordance with the proceedings held before this Court on March 8, 2011, during which the Court ordered defendant agencies to provide supplemental declarations which specifically address the questions raised by plaintiffs in their February 28, 2011 letter to the Court. In the discussion which follows, the FBI will respond to the questions posed by plaintiffs, although we note that many of the responses will re-articulate statements made in my four prior declarations submitted in this case.<sup>1</sup>

---

<sup>1</sup> See November 12, 2010 ["First"] Hardy Declaration (explained the FBI's search for records responsive to plaintiffs' FOIA request); January 26, 2011 Second Hardy Declaration (explained the search cut-off date which the FBI used); January 28, 2011 Third Hardy [Vaughn] Declaration (inadvertently dated January 28, 2010) (justified the application of FOIA exemptions for the FBI's January 17, 2011 release); and February 18, 2011 Fourth Hardy Declaration (explained the FBI's technological limitations of FBI's FOIPA Document Processing System "FDPS" and why FBI is unable to comply with Court's February 7 and February 15, 2011 Orders).

**A. *Provide details regarding technical aspects of the FBI's standard process and technology used in response to FOIA requests***

***I. Early Workflow and Manual Processing Description***

(2) Upon receipt of a Freedom of Information Act ("FOIA") request, the FBI's Record/Information Dissemination Section ("RIDS"), RMD, formally acknowledges the request via written letter, and then conducts a search of the indices of its Central Records System ("CRS") to determine whether it has any records responsive to the FOIA request. Once a file is identified as potentially responsive to the FOIA request, the file is retrieved and manually reviewed by a FOIA analyst to determine whether the file contains documents responsive to the request. Assuming the file is indeed responsive to the request, the file is photocopied, and a FOIA analyst reviews the paper copy to determine if any material needs to be withheld pursuant to the Privacy Act or any FOIA exemptions or exclusions. RIDS also analyzes the FOIA request to determine whether responsive records are reasonably likely to be located anywhere other than a CRS file. If so, RIDS will contact the relevant locations and instruct them to conduct an independent search and to send RIDS any responsive records located. RIDS requests the official paper copy of such records. If there is no such copy, RIDS will accept an electronic copy.

(3) Prior to the use of the current document processing system, the FBI relied solely on manual processing of paper documents by "browning out" information by hand with a marking pen as the means to redact information. Thus, for any exempt material in a responsive file, the FBI FOIA analyst used a colored marker to delete the exempt material and handwrote the appropriate exemption in the margins of the responsive document. The analyst would then physically re-copy the processed pages using a photocopier with a special filter to ensure that no

one could lift the “brown outs” over the deleted material. Finally, the processed copies of the documents would be mailed to the requester. See “FOIA (Freedom of Information Act) - The Privacy Act and Changes to the FOIA,” [www.faqs.org/espionage/Ep-Fo/FOIA-Freedom-of-Information-Act](http://www.faqs.org/espionage/Ep-Fo/FOIA-Freedom-of-Information-Act).

## ***II. Current Version of FOIPA Document Processing System***

(4) The FBI currently employs a Highland Technologies Inc., HighView software product, version 3.0.4, customized to enable the FBI to track and monitor its high-volume, fast-paced FOIA/Privacy Act processing of classified (up to “Secret”) and law enforcement sensitive documents. Dubbed the “FOIPA Document Processing System or ‘FDPS,’” the software is a client-server application<sup>2</sup> that has been built from the base version of the COTS product HighView and customized for the FBI’s use. The client portion of the application is compatible with all 32-bit versions of the Windows operating system (including Windows 95/98/ME/NT/2000/XP). The server portion of the application includes an Oracle 11g database and application repositories. FDPS resides on the internal FBI network which is specifically designed to handle documents classified up to the “SECRET” level. FDPS enables RIDS to electronically track, monitor, and process FOIA requests while meeting the security requirements for classification review and the integrity of FBI data as granted under the systems Authority to Operate (“ATO”) from the FBI Security Division.

---

<sup>2</sup> A client-server application is a form of network computing in which each component is either a “client” or a “server.” The server computer manages disk drives, printers and traffic on the network. Client computers are workstations which use the server for its resources, whether these are files, applications or processing power.

***III. More Detailed Description of the Workflow Process Used Today***

(5) I have previously described the FBI's use of FDPS to fulfill its statutory FOIA and Privacy Act obligations. See [First] Hardy Declaration, ¶¶ 27-28. As I mentioned earlier, a vast majority of the material responsive to FOIA/Privacy Act requests is still maintained by the FBI in original paper format as part of the FBI's official federal records system. The FBI's paper records are physically located in a number of different offices, including: FBIHQ, the Alexandria, Virginia Records Center ("ARC"); any of the 56 field offices and associated Resident Agencies throughout the country; and overseas Legal Attaches.

(6) Today, the FBI receives FOIA/Privacy Act requests by regular mail, e-mail or fax. Requests are entered into the FDPS application along with all correspondence related to the requests; the request letter and related correspondence are scanned into the FDPS repository as a Tagged Image File Format ("TIFF") image utilizing a Windows client workstation. This is accomplished through an interface within the FDPS application and scanner attached directly to the client workstations. The entry of this information into FDPS results in the creation of tracking information (FOIPA #, requester information, date of receipt, FBI Employee Identification, etc.) relevant to the request, and ensures that all related documentation remains intact throughout the process, creating the required information for further processing actions. FBI indices (CRS as well as the manual indices) are searched by a FOIA analyst to identify potentially responsive records. Further searches are ordered depending on the nature of the FOIA request and whether there are any other locations where responsive records are reasonably likely to be located. Responsive records are retrieved from the relevant locations throughout the FBI



and sent to RMD in Winchester, Virginia for centralized uploading to FDPS for eventual review, processing and release of non-exempt information.

***IV. Method Used for Conversion of Documents to ".tiff" or ".pdf"***

(7) All responsive hard-copy documents are scanned and imported into FDPS as TIFF images and any electronic media (e.g., Word, Excel, Corel, Portable Document Format (PDF), PowerPoint) are imported via a conversion interface to TIFF format. The FDPS application is coded to convert all documents for processing purposes to a flattened TIFF image format. The FOIPA information and images are stored in Oracle repositories and image servers designated for the FDPS system.

(8) As an initial matter, the FDPS application is designed such that it is compatible only with TIFF images. Documents can be reviewed and redacted only if they are in TIFF format. Moreover, conversion to TIFF ensures protection of FBI and other government agency equities, protection of national security information, and maintenance of classified information. The digitization of electronic documents to TIFF format does not preserve any metadata. In fact, the conversion of electronic documents to TIFF images is specifically designed to *affirmatively* strip metadata in order to ensure that no classified and/or law enforcement sensitive information is inadvertently released to the public.<sup>3</sup> This process also removes any true "parent-child" relationships among the documents due to the fact that the image that is retained is a flattened image. At most, the process is able to produce a "TIFF" image of an e-mail which may be

---

<sup>3</sup> For example, the metadata associated with a document may contain the names of custodians, which may be exempt under FOIA exemptions (b)6 and/or (b)7(C).

immediately followed by a "TIFF" image of a document embedded in that e-mail (e.g., Excel, Word, .pdf, etc.).

(9) Documents in their native electronic formats (PowerPoint, Excel, Word), unlike TIFFs, are editable and could allow for the required redactions to be reverse-engineered, exposing the critical information that must be protected.<sup>4</sup> One such recent example is an inadvertent release of information made by the Transportation Security Administration ("TSA"), of a standard operating procedures manual. TSA processed the document by drawing black boxes on top of those portions deemed "Sensitive Security Information" ("SSI") in a native PDF version of the document. TSA later discovered that the blacked out redactions could be ignored by the a particular PDF viewer, making the previously redacted text readable. Maintaining records in their native format and deleting information exempt under the FOIA is not a viable alternative when dealing with sensitive information that, under FOIA, must not be released.

(10) The original scanned image created in FDPS is referred to as the "MASTER COPY" and these images are never modified from their original state. As the FOIA analysts redact information or add any other markings on the documents, "overlays" are created. These "overlays" are stored in the FDPS database with exact position coordinates. The combination of

---

<sup>4</sup> Examples of such "lifting" and unintended releases of information have occurred from time to time with documents produced in native formats. See, e.g., "FOIA Friday: Redactions – How Not To Do It, [www.annarbor.com/vielmetti/foia-friday-redaction-how-not-to-do-it](http://www.annarbor.com/vielmetti/foia-friday-redaction-how-not-to-do-it), (citing Interior Department, Fish and Wildlife Service release of a Microsoft Word document that had the "Track Changes" tool turned on and which enabled requesters to not only get the text that the agency had intended to release, but also prior versions of the file identifying deleted information and who made those edits).

the “MASTER COPY” and the multiple overlays produce what is referred to as the “REDACTED COPY.” When preparing responsive records for dissemination, the “REDACTED COPY” is utilized to merge all redactions and other markings onto the original image to create the final redacted images used for dissemination. This final version of the images is referred to as the “SEALED COPY.” As was the case with the “MASTER COPY,” the “SEALED COPY” is a flattened TIFF images from which the requester – or any other member of the public – is unable to edit or lift previously redacted information.

***V. Description of Fields Load Files May Contain***

(11) The FBI is unable to create load files using FDPS. As explained above, metadata is eliminated from the records when they are converted to TIFF images and loaded onto FDPS.

***VI. Available Alternative Processes Using That Technology/Software***

(12) There is no way to process documents using FDPS other than that described above.

***VII. Compatibility with Different Versions of Standard Review Platforms***

(13) FDPS is specifically intended not to be compatible with different versions of standard review platforms so as to maintain the integrity of the national security and law enforcement sensitive documents processed within the parameters of the system.

***B. Other Technology/Software Available to the FBI That Could be Used to Process, Review, Redact and Produce Metadata***

(14) There is no technology or software currently “available” to the FBI that could be used to process any metadata from the documents responsive to plaintiffs’ request. As indicated

in the Fourth Hardy Declaration, the use of the Clearwell software program to process the Excel spreadsheets was a one-time opportunity. The Financial Crimes Section, which purchased access to Clearwell version 6.1.15.0, informed RIDS that Clearwell had reached its maximum capacity as a result of its ongoing investigation.<sup>5</sup> See Fourth Hardy Declaration ¶ 8.

**C. *Records Collection Process and the Preservation of Document Structure and Metadata***

(15) The FBI's record collection process was previously described in my [First] and Fourth Hardy Declarations. See [First] Hardy Declaration ¶¶ 19-28 and Fourth Hardy Declaration, ¶¶ 3-6. Because the official FBI record is a paper record, no effort is made to collect metadata for records responsive to a FOIA request even when an electronic format exists. This is because FDPS requires all records – paper or electronic – to be converted to a TIFF format file for each page. Both the input and output from FDPS is a TIFF format file. When collecting responsive records for FOIA requests, the original official document (paper) is requested from the appropriate Field Office, Legat or Headquarters. If the original record does not exist in paper format, an electronic version can be used instead; however, regardless of the format of the

---

<sup>5</sup> Even if the Clearwell was available to RIDS, RIDS discovered that it could not use the program to comply with the court's order to produce metadata in redacted form. For example, when processing the Excel spreadsheets for this case, Clearwell produced a page of metadata that could not be redacted using the Clearwell software. In order to produce this information, RIDS had to create a new document containing just this metadata and thereafter assert the appropriate redactions over the metadata. I have also been advised that various field offices have independent instances of Concordance that are being used in active criminal investigations to identify and organize case-critical information, but it cannot be redeployed for use by RIDS in connection with this matter. Even if Concordance were made available to RIDS, it would nevertheless be an ineffective tool because it is incompatible with the TIFF images that RIDS works with to process documents responsive to FOIA/Privacy Act requests.




electronic record, that record is converted to a TIFF format file that does not retain metadata before processing in FDPS.

**D. *Technical Obstacles to Complying with the Court's Order***

(16) As we have demonstrated both in this declaration as well as the prior Hardy Declarations, RIDS – the section responsible for handling FOIA requests – does not have the technology to comply with this Court's order. The only experience the FBI has with metadata (either preserving, collecting, or processing) has been developed during the course of this litigation. As we have explained earlier, the processing of FOIA/Privacy Act requests in FDPS is squarely based on the review and processing of paper records which serve as the official FBI record. Moreover, even where electronic records are collected, they are necessarily converted to TIFF format for processing. Because the FBI's FDPS system was not created to serve – and is unable to serve – as an “e-discovery” tool, the FBI does not have the capability to expose and identify metadata in electronic records.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed this 23<sup>rd</sup> day of March, 2011.

  
 DAVID M. HARDY  
 Section Chief  
 Record/Information Dissemination Section  
 Records Management Division  
 Federal Bureau of Investigation  
 Winchester, Virginia