

**Thomas M. Susman**

**Ropes & Gray LLP**

**Washington, DC**

Paper delivered at the  
**5<sup>th</sup> International Conference of Information Commissioners**

**Access to Information in Electronic Form:  
The U.S. Experience Under the Freedom of Information Act**

**I. INTRODUCTION**

The United States Congress in 1996 enacted the Electronic Freedom of Information Act Amendments of 1996<sup>1</sup> (eFOIA) to resolve some of the problems that had arisen in the course of applying the 1966 Freedom of Information Act<sup>2</sup> (FOIA) to information maintained in electronic formats. The new statute addressed three issues that had been subject to dispute by explicitly requiring records maintained in electronic format to be made available under FOIA; by requiring agencies to make a “reasonable effort” to comply with requests to furnish records in formats selected by the requesting party; and by requiring agencies to note the location and extent of deletions made on an electronic record when released with redactions made of exempt material.<sup>3</sup>

---

<sup>1</sup> Public Law No. 104-231, 110 Stat. 3048.

<sup>2</sup> 5 U.S.C. § 552 (2007).

<sup>3</sup> The amendments also imposed requirements on agencies regarding expedited and multitrack processing of FOIA requests, attempted to reduce delays due to agency backlogs, extended the initial deadline for responding to requests from 10 to 20 working days, and expanded reporting and electronic dissemination requirements.

A 1989 Conference on Electronic Public Information<sup>4</sup> and a 1988 recommendation of the Administrative Conference of the U.S.<sup>5</sup> had identified a number of other areas of controversy regarding application of FOIA to electronic information: whether software, electronic mail, and databases are records subject to FOIA; what constitutes a reasonable search of electronic information under FOIA; and whether programming involves the creation of new records and is therefore not required by FOIA. E-FOIA left many of these issues unresolved; some of them remain so today. The controversies over programming and searching have receded: retrieval of data from electronic files and databases has become routine, and whether a search is reasonable can ordinarily be addressed without resort to parsing fine lines surrounding computer programming. This paper addresses the three other areas that continue to prove vexing to requesters and agencies alike: access to entire databases, access to e-mail, and access to software. The discussion of databases occupies a large portion of this paper because it is drawn largely from the author's participation in an on-going FOIA case on this subject.

## **II. ACCESS TO ENTIRE DATABASES**

A case currently pending in the U.S. federal court in New York demonstrates many of the difficulties encountered by persons requesting data from electronic databases under FOIA. In this case, the plaintiffs are two professors from Syracuse University who direct the Transactional Records Access Clearinghouse (TRAC). TRAC is a data-gathering, data-research, and data-distribution organization whose purpose is to make information about the federal government's civil enforcement and regulatory efforts, along with information on related staffing and spending, accessible and understandable to the public. It accomplishes its purpose principally using FOIA.

TRAC is seeking to obtain information from a case management database, known as "CASES," maintained by the Civil Division of the Department of Justice (DOJ).<sup>6</sup> The CASES database tracks all cases involving that Division. For example, the database

---

<sup>4</sup> HENRY H. PERRITT, JR., ELECTRONIC PUBLIC INFORMATION AND THE PUBLIC'S RIGHT TO KNOW (1990) (reporting on the proceedings of a Washington, DC conference held October 23-24, 1989).

<sup>5</sup> "Federal agency use of computers in acquiring and releasing information," 1 C.F.R. § 305.88-10 (1988). The first effort to address this subject in a comprehensive manner appears in "Electronic Collection and Dissemination of Information by Federal Agencies: A Policy Review," H.R. Rep. No. 560, 99th Cong., 2d Sess. (1986).

<sup>6</sup> Long v. Department of Justice, Case No. 5:06-cv-1086 (N.D.N.Y. 2007).

includes records containing various case identifiers and descriptors, names of plaintiffs and defendants, client federal agencies, assigned attorneys, case dispositions, monetary relief sought and awarded, and the time expended by DOJ staff, as well as a copy of the physical case files available for the case. CASES is used by the Civil Division to manage its litigation workload and to generate statistical, management, and budget information.

In 2004, TRAC requested an electronic copy of the records in CASES pertaining to the DOJ's civil court cases filed or pending since October 1, 1999. TRAC also requested descriptive information about the database, including table schema and definitions of codes used, records describing the scope of cases included in the database, changes to the database during the designated period, current data input and users' manuals, descriptions of reports regularly prepared using the database, and records describing procedures used to ensure data quality.<sup>7</sup>

Three years later a lawsuit was filed, and there have been lengthy discussions between the parties resulting in releases of a large portion of the requested data. However, numerous issues still remain, highlighting several issues common to FOIA requests for electronic databases. First, government agencies' procedures and personnel are often ill-equipped to respond to FOIA requests involving large, complex, electronic databases. Second, FOIA requires agencies to conduct a reasonable search for responsive records, but databases create a unique challenge in this area because sometimes agencies are not fully aware of the scope of their own databases and are unable or reluctant to provide the requester with an "audit trail" explaining their search parameters and methods. Third, many common exceptions to disclosure under FOIA take on new meaning in the context of an electronic database. Finally, technical difficulties often arise related to the form and formatting of the data.

## **A. Constraints on Agency Responses to FOIA Requests for Databases**

### **1. Lack of procedures specific to electronic requests**

The TRAC request was processed by the Freedom of Information and Privacy Acts Office of the Civil Division, which handles all FOIA requests for Civil Division records. The TRAC requesters were never permitted to communicate directly with the technical

---

<sup>7</sup> As a nonprofit organization with a history of widespread dissemination of information relevant to government administration, TRAC was granted a waiver of fees ordinarily imposed under FOIA.

staff of the Office of Management Information (OMI), which maintains the CASES system, to discuss the best approaches for responding to their request and for providing the results in the most suitable format for delivery.<sup>8</sup> This resulted in years of delay, as the technical staff wrote programs to extract data that did not respond to what the requesters were seeking. The requesters, who are database experts, could have assisted in streamlining the data extraction process but were never allowed to do so. This experience demonstrates that, at least in the case of highly technical electronic requests, the earlier the requester is involved in or at least fully informed about the process of data extraction, the better the long-term benefit in terms of cost, time, and accuracy for both parties.

## **2. Personnel constraints**

Limitations on agency personnel may result in an inadequate response to a FOIA database request. OMI is understaffed and often contracts much of the search work to outside companies, leading to further confusion. Additionally, the limited OMI staff may not always be qualified to handle the request. OMI made an initial attempt to extract data from CASES in March 2006. After this was completed, OMI realized that the programming code identified only selected closed cases, whereas the requester was seeking both closed and open cases. OMI then needed to rewrite the code, but by that time the technical staff person who had written the code for the March 2006 production was no longer employed in OMI and had left no record of the code used the first time. The new staff had to start from scratch to write new code and process the results, which took an OMI employee working with a contractor and another staff person from July until November 2006 to complete. Yet, even on that try, OMI failed to create a code that would identify the records that had been redacted, so in January 2007 OMI started writing a third code to show redactions. This pattern of understaffing (and under-qualified) staff only resulted in more wasted time for everyone involved in the process.

## **3. Computer system constraints**

Another problem encountered in by TRAC has been the limitations of the database itself. The CASES database requested by TRAC was outdated, poorly managed, and not

---

<sup>8</sup> These discussions did occur through a very helpful Civil Division litigator staffed on the civil suit filed in the Northern District of New York. However, even the most lucid game of information telephone (requester speaks with attorney, attorney speaks with DOJ litigator, DOJ litigator speaks with OMI technical staff) is no substitute for a direct conversation between requester and technology staff.

designed to be responsive to the types of searches necessary to respond to FOIA requests. In the course of responding to TRAC's request, the Department of Justice has had to review and significantly revise the database to address many of its shortcomings. However, there are obviously limits to what an agency will and should be required to do to remedy the shortcomings of its database. In these situations, the agency may respond that it is unduly burdensome to respond to the request if it would involve conducting a search that is not reasonably possible in the given database.

For example, in People for the American Way Foundation v. Department of Justice,<sup>9</sup> the plaintiff sought documents from the Executive Office for the United States Attorneys pertaining to sealed cases relating to post-9/11 immigrant detainees. The agency informed plaintiff that the search was unreasonably burdensome, as the databases used to manage cases did not identify sealed cases nor immigrant status, so any search would have to be done by hand in each U.S. Attorney's Office. In short, the limitation of the database made a straight-forward electronic search impossible. The database simply did not track the relevant terms to enable responses to FOIA requests. Since sealed cases will almost always be subject to a FOIA exemption, tracking the sealed status of a case would inevitably make it easier to respond to FOIA requests; unfortunately, most agency databases are not designed with FOIA in mind.

As a result, the requester must find a creative way to get around the limitations of the database. In People for the American Way, the parties engaged in settlement negotiations to try to frame a database search that would yield the relevant records or limit the scope of the hand search. Searches of the database were conducted using specific terrorism-related identifiers and habeas corpus codes, which yielded 69,000 potentially responsive files. The plaintiff then agreed to remove 25,000 habeas cases and proposed that the agency screen the remaining 44,000 using PACER, an online system containing information about all public cases in federal courts, which would enable the agency to identify those cases that were not listed on PACER. A hand search would then be conducted of the cases not listed in PACER to determine if they were sealed. The agency said this would be too burdensome and also rejected other proposals to limit the search. The court agreed that a manual search of all 44,000 records would be unduly burdensome, but found that a PACER search of those records to identify which cases had

---

<sup>9</sup> 451 F. Supp. 2d 6 (D.D.C. 2006).

been sealed would not be burdensome. The court reserved judgment on whether a subsequent manual search of the files identified by PACER would be burdensome since it did not know how many files would be found. It thus proposed that the parties return to court if they disagreed over the reasonableness of the manual search.

The problem of technological constraints to responding to FOIA requests reached its zenith in a request and subsequent lawsuit by the Center for Public Integrity for data on Foreign Agents Registration Act (FARA) registrants from DOJ's Foreign Agents Registration Unit. The agency responded to the request that its computer system was so fragile that simply making a copy of the database could result in loss of data.<sup>10</sup> (The requester dismissed its lawsuit when DOJ made a commitment that a new database would be installed in a reasonable period of time.)

The experience in TRAC and other cases revealing inadequate procedures, personnel, and computer systems raises the question whether FOIA obligates government agencies to make improvements in these areas to enable better responses to FOIA requests. This issue has not been decided by the courts.

## **B. Reasonableness of Search**

Also at issue in the TRAC case is the reasonableness of DOJ's search for responsive records. FOIA requires agencies to conduct a reasonable search. To challenge the reasonableness of a search, a requester must identify specific problems with the search the agency has conducted. However, to do this, the requester needs information about the scope of the search, or audit trail.

For example, in Servicemembers Legal Defense Network v. Department of Defense,<sup>11</sup> a nonprofit organization sought records from the Departments of Defense and Justice relating to alleged government surveillance of individuals and groups opposed to the government's policy on gays and lesbians in the military. The belief that this surveillance may have occurred was based upon press reports of a Defense Department document mentioning the surveillance. The agencies conducted searches and made limited releases of information, but the plaintiff believed that other documents existed, so

---

<sup>10</sup> See discussion at <http://www.publicintegrity.org/report.aspx?aid=332>.

<sup>11</sup> 471 F. Supp. 2d 78 (D.D.C. 2007).

it challenged the adequacy of these searches. The court granted summary judgment for defendants and dismissed the case after finding, based on the agencies' declarations, that although initial searches may have been inadequate, the agencies eventually agreed to use appropriate search terms and searched relevant databases and files that were "likely to possess the requested information." The court held that the agencies did not have to search every database possible, but only those likely to contain responsive information; the mere possibility that other responsive documents existed did not render the search unreasonable. This case demonstrates the need for plaintiffs to identify a concrete flaw in the way that an agency searched for requested information to succeed in challenging the reasonableness of a search.

A problem in database cases is how to obtain the search parameters used by an agency. In Servicemembers, the agencies disclosed simple keyword searches of databases in their declarations. Requesters should be provided access to an audit trail to be sure that an agency has extracted the entire database and not just a portion. For instance, in TRAC, DOJ was not even aware of the full scope of the database that had been requested. In January 2007, over two years after the initial FOIA, the agency discovered that the CASES database contained nearly 100 previously unreleased tables that were either in the core database or part of specialized modules used by particular branches of the Civil Division. These tables were hidden because the agency did not have an accurate and comprehensive catalog of all the tables and fields, which it has had to create in the course of responding to the FOIA request. The agency's own lack of awareness of the parameters of its database makes it difficult for the FOIA requester to evaluate whether the agency's search was reasonable, since to do so requires information about the scope of the search and the database being searched.

### **C. Application of Common Exemptions to Database Requests**

Exemptions may apply to information contained in databases in the same manner as to other kinds of records subject to disclosure under FOIA.<sup>12</sup> If names and other personal identifying information appears, then the exemption protecting against unwarranted invasions of personal privacy may apply. Likewise, exemptions relating to law enforcement activities or to trade secret or other confidential commercial information may be applicable. FOIA also has an exemption that protects essentially trivial internal

---

<sup>12</sup> The 9 exemptions are contained in 5 U.S.C. § 552(b).

administrative matters (Exemption 2); while some agencies have attempted to use this exemption to protect databases on the theory that they were designed solely for internal use, the courts have rejected this claim.<sup>13</sup>

#### **D. Form and Formatting Issues**

##### **1. Separability of exempt information**

Another problem encountered in the database context is that information that should be released may be co-mingled with exempt information in the same database. Where there is both exempt and nonexempt information, an agency should separate or redact the exempt information, but this can be difficult in a database. In TRAC, a major problem has arisen with sealed cases. The Department of Justice sought to redact records for any case that had been sealed at any point; however, many cases are only partially sealed or are later unsealed and the agency had no reliable way of identifying which cases were still currently sealed in their entirety. This problem is similar to the one encountered in People for the American Way, discussed above, where the requester found a creative way around the database limitation, which the court in part endorsed.

In Los Angeles Times Communications LLC v. Department of Labor,<sup>14</sup> a newspaper sought information from government databases pertaining to civilian contractors who were killed or injured while supporting military operations in Iraq and Afghanistan. The agencies released some information but withheld: (1) names, addresses, genders, dates of death, and employers of the deceased contractors from the United States and countries other than Iraq and Afghanistan; (2) the names, genders, dates of injury, and employers of injured American contractors; and (3) the names, addresses, genders, dates of injury, and employers of injured foreign contractors from countries other than Iraq and Afghanistan. The basis for the withholding was Exemption 6, protecting personal information. The court found that the disclosure of identifying information as to contractors currently residing in Iraq or Afghanistan was not warranted given the risks to their personal safety that disclosure would create. While the court did not find that these risks applied to contractors residing outside Iraq and Afghanistan, it determined that there was no way to ascertain the current residence of the contractor from the database.

---

<sup>13</sup> *E.g.*, Abraham & Rose, PLC v. United States, 131 F.3d 1075 (6th Cir. 1998) (IRS database of federal tax liens).

<sup>14</sup> 483 F. Supp. 2d 975 (C.D. Cal. 2007).

The court therefore allowed the agency to withhold all of the identifying information for all contractors. This case demonstrates that without adequate information that perhaps should be integral to the database, an agency may be able to withhold all of the information, both exempt and nonexempt, since the latter cannot be reasonably segregated.

## **2. Identification of Redactions**

Identification of redactions has also been an issue in the TRAC case. This has been a more practical problem, because the Department of Justice has agreed in theory (as required by eFOIA) to show asterisks to indicate redacted fields; however, agency responses have been elusive on this point. As mentioned above, the first two releases did not show redactions; it took a third effort to write a code that would show redactions.

## **III. ACCESS TO E-MAIL**

E-mail is subject to disclosure under FOIA if it can be reasonably retrieved. Several issues arise related to access to e-mail under FOIA. First, an agency is only expected to disclose those e-mails in its possession at the time of a FOIA request. Thus, both agency and national archiving policies play an important role in determining whether e-mails are preserved for disclosure under FOIA and in what format agencies are permitted to maintain e-mail records and related metadata. The application of federal recordkeeping requirements for the preservation of e-mail also influences courts' analysis of whether an agency's search for documents in response to a FOIA request is reasonable. Lastly, government employees' use of public e-mail systems to transmit personal information and use of private web-based e-mail systems to conduct government business raise challenging issues under FOIA.

### **A. E-mail Preservation**

#### **1. Recordkeeping requirements**

FOIA "does not impose a document retention requirement on agencies," but instead requires an agency to disclose only those documents that it possesses at the time of a FOIA request.<sup>15</sup> Thus, in the United States, the National Archives and Records Administration (NARA) regulations related to document retention and destruction play a significant role in determining whether e-mails are preserved for disclosure under

---

<sup>15</sup> Landmark Legal Found. v. EPA, 272 F. Supp. 2d 59, 66 (D.D.C. 2003).

FOIA.<sup>16</sup> These regulations permit agencies to destroy electronic records "only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules."<sup>17</sup> General Records Schedule (GRS) 20 permits agencies to delete e-mails from users' electronic mailboxes after copying them to a recordkeeping system that meets certain specifications related to accessibility, security, and accuracy.<sup>18</sup> The time period for which the e-mail records must be retained in the recordkeeping system is governed by the applicable NARA-approved schedule and thus varies by agency and by type of record.

## **2. Format of recordkeeping systems**

GRS 20 permits agencies to adopt either electronic or paper recordkeeping systems for the storage of electronic records.<sup>19</sup> The recordkeeping system must capture certain metadata, including the names of the sender and recipient of an e-mail, as well as the date the e-mail was transmitted.<sup>20</sup> NARA adopted this metadata requirement in response to Armstrong v. Executive Office of the President,<sup>21</sup> in which the D.C. Circuit held that certain agencies' policies of printing out e-mails as the sole method of preserving e-mail records violated federal records laws because such print-outs failed to preserve all important elements of electronic records.<sup>22</sup>

## **3. Policy issues underlying recordkeeping requirements**

In Public Citizen v. Carlin, the D.C. Circuit upheld GRS 20 against a challenge by Public Citizen asserting that "hard copy records are not satisfactory replacements for records in electronic format."<sup>23</sup> This case highlights the policy issues that must be balanced when deciding in what format electronic records, including e-mails, should be preserved; the Public Citizen court categorized these issues as superiority issues and completeness issues.

---

<sup>16</sup> See 36 C.F.R. pt. 1234 (2007).

<sup>17</sup> 36 C.F.R. § 1234.34 (2007).

<sup>18</sup> NAT'L ARCHIVES & RECORDS ADMIN., GENERAL RECORDS SCHEDULE 20 (August 1995), available at <http://www.archives.gov/records-mgmt/ardor/grs20.html>; see also 36 C.F.R. § 1234.32 (2007).

<sup>19</sup> NAT'L ARCHIVES & RECORDS ADMIN., *supra* note 18.

<sup>20</sup> *Id.*; see also 36 C.F.R. § 1234.32 (2007).

<sup>21</sup> Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993).

<sup>22</sup> Jason R. Baron, *E-Mail Metadata in a Post-Armstrong World*, Paper Presented at the Third IEEE Metadata Conference (1999), available at <http://www.archives.gov/era/pdf/baron-email-metadata.pdf>.

<sup>23</sup> 184 F.3d 900 (D.C. Cir. 1999).

**(a) Superiority issues**

Centralized electronic recordkeeping systems are superior to paper systems in terms of "searching, manipulating, and indexing information."<sup>24</sup> In addition, electronic systems promote efficiency because multiple users may search an electronic system at the same time. These values must be balanced, however, with administrative considerations. An agency's primary purpose in adopting recordkeeping systems is to "conduct Government business," not to preserve records for the use of future researchers or FOIA requesters, and some agencies may find that paper recordkeeping systems are "most appropriate to the business of the agency."<sup>25</sup> In addition, agencies may face operational constraints that make the adoption of centralized electronic recordkeeping systems infeasible. NARA has chosen to balance these policies by encouraging, but not requiring, agencies to adopt electronic recordkeeping systems, and the court in Public Citizen approved this approach. For FOIA requesters, this means that e-mail records often may not be available in electronic format.

**(b) Completeness issues**

Paper records may not adequately capture all information contained in an electronic record. In Public Citizen, the Archivist and court responded that the metadata requirement in GRS 20 adequately addresses this concern, as it requires that recordkeeping systems preserve "all relevant transmission data" from e-mails. The court observed that Public Citizen had failed to identify any "information that may not be transferred when [an e-mail] record is copied to paper pursuant to the requirements of GRS 20."<sup>26</sup> Thus FOIA requesters should have access to relevant metadata associated with e-mails whether agencies maintain paper or electronic recordkeeping systems.

**4. Consequences of wrongful document destruction**

An agency is not liable under FOIA for failure to comply with federal record retention laws and regulations. Instead, if an agency wrongfully destroys documents that were in its possession at the time of a FOIA request and should have been disclosed, the agency may be required to pay the requester's attorneys fees caused by such destruction and to

---

<sup>24</sup> *Id.* at 908.

<sup>25</sup> *Id.* at 909-10.

<sup>26</sup> *Id.* at 910.

reconstruct the documents to the best of its ability.<sup>27</sup> In addition, if a court had previously ordered the agency to retain the documents, the agency may be held in contempt for destroying records.<sup>28</sup>

#### **B. Reasonableness of Searches for E-Mail Under FOIA**

NARA regulations not only dictate the records that federal agencies must maintain and the format in which those records are preserved, but federal recordkeeping requirements have influenced the way courts assess the reasonableness of a search for e-mails under FOIA. Courts are unlikely to deem a search reasonable unless an agency has searched its e-mail recordkeeping system, as demonstrated in Albino v. United States Postal Service. In that case, an agency employee responded to a request for e-mails under FOIA by asking the individuals whom the requester had identified in his FOIA request whether they had records of the requested e-mails. The court held that this search was inadequate, explaining that the agency should have also "enlist[ed] the help of information technology personnel," who "would have access to e-mail message archives."<sup>29</sup>

#### **C. Application of FOIA to Personal E-Mails Sent Via Public E-Mail Accounts**

At the federal level, agencies may withhold from disclosure personal e-mails under FOIA's Exemption 6, which exempts from disclosure records involving "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy."<sup>30</sup> In Yonemoto v. Department of Veterans Affairs, the court upheld the Department of Veterans Affairs' decision to redact portions of e-mails sent via a government e-mail server that discussed the personal feelings of the author, a government employee, towards co-worker Yonemoto.<sup>31</sup> To determine whether Exemption 6 applied, the court balanced the author's "personal interest in privacy against the public's interest in disclosure" to the extent that disclosure would further the primary purpose of FOIA – "contributing significantly to public understanding of the operations

---

<sup>27</sup> See, e.g., Landmark Legal Foundation v. EPA, 272 F. Supp. 2d 59, 66-68 (D.D.C. 2003).

<sup>28</sup> See generally Landmark Legal Foundation v. EPA, 272 F. Supp. 2d 70 (D.D.C. 2003).

<sup>29</sup> Albino v. USPS, No. 01-C-563-C, 2002 WL 32345674, at \*6-7 (W.D. Wis. May 20, 2002).

<sup>30</sup> 5 U.S.C. § 552(b)(6) (2007).

<sup>31</sup> Civ. No. 06-00378 BMK, 2007 WL 1310165 (D. Haw. 2007).

or activities of the government."<sup>32</sup> The court found that the "public . . . ha[d] no legitimate interest in the redacted portions of the emails" because disclosure would not "contribute significantly to public understanding of the operations or activities of the government."<sup>33</sup> However, where personal comments are inextricably intertwined with government business, or where they relate more significantly to government activities, Exemption 6 may not protect against disclosure.

State courts have also had to determine whether personal e-mails sent via government accounts qualify as "public records" under state public records laws. These courts have generally emphasized that the content of e-mails, rather than their physical location on public computers, should govern whether they must be disclosed. Thus, the Supreme Courts of Arizona and Arkansas have held that maintaining an e-mail on a government computer system is not determinative of its legal status.<sup>34</sup> In Pulaski County v. Arkansas Democrat-Gazette, Inc., Ron Quillin, the controller and director of administrative services of Pulaski County, Arkansas, was charged with embezzling government funds. During his time as controller, he entered into a romantic relationship with Jane Doe, an employee of Government e-Management Solutions (GEMS). At the same time, the city of Pulaski contracted with GEMS. The e-mails at issue in the case included romantic exchanges between Quillin and Doe. The Arkansas Supreme Court upheld the lower court's determination that these e-mails qualified as public records because "the romantic relationship between Quillin and Doe was indistinguishably intertwined with the business relationship between the County and GEMS."<sup>35</sup> Both this and the federal case above demonstrate the need for FOIA requesters to describe a specific connection between requested information and government activities when challenging an agency's decision to withhold personal information.

#### **D. Application of FOIA to e-mails sent via private e-mail accounts**

Increasingly, government officials are using private e-mail accounts and handheld devices to conduct government business, and thus an emerging issue is whether e-mails

---

<sup>32</sup> *Id.* at \*3-4 (quoting *U.S. Dep't of Def. v. Fed. Labor Relations Auth.*, 510 U.S. 487, 495 (1994)).

<sup>33</sup> *Id.* at \*4.

<sup>34</sup> *Griffis v. Pinal County*, 156 P.3d 418, 419-20 (Ariz. 2007); *Pulaski County v. Ark. Democrat-Gazette, Inc.*, No. 07-669, 2007 WL 2580466 (Ark. July 20, 2007).

<sup>35</sup> *Pulaski County v. Ark. Democrat-Gazette, Inc.*, No. 07-669, 2007 WL 2874774 (Ark. Oct. 4, 2007).

transmitted privately are subject to disclosure under public records laws.<sup>36</sup> If courts take a content-based approach as they have in the case of personal e-mails sent via public accounts, then business related e-mails sent through private accounts should be disclosed under FOIA. At least one state court has required such disclosure. In Dallas Morning News, L.P. v. City of Dallas, a district court judge ordered the city of Dallas to produce e-mails sent or received from city officials' personal computers and handheld devices related to a multi-million dollar tax abatement given by the city to Hunt Consolidated.<sup>37</sup> The judge adopted the position that e-mails related to city business qualify as public records "no matter where or how transacted," even if the city does not own the device through which such e-mails were transmitted and lacks access to the e-mails.<sup>38</sup>

This issue is sure to confront the federal government; not only do employees sometimes use personal e-mail accounts where agency systems are available,<sup>39</sup> but employees at the Department of Interior did not have access to government e-mail for a number of years after a federal judge ordered the agency's e-mail system to be taken off-line in the context of a legal action against the government.<sup>40</sup> Since FOIA requires that a record must be under the control of the agency to qualify as an agency record, the agency may well argue that these e-mails cannot be reached by a FOIA request. However, where a private e-mail account is used for government business and copies of communications are not retained by the agency, the agency should be required to retrieve requested e-mails from an Internet service provider.

Since private e-mail accounts used to conduct government business avoid capture in government recordkeeping systems, this also reduces the likelihood that these e-mails will be preserved. In addition, persons seeking access to the e-mails must either rely on

---

<sup>36</sup> See, e.g., Jo Mannies, *Government E-Mails Going Private*, STLTODAY.COM, Nov. 13, 2007.

<sup>37</sup> Order Granting Partial Summary Judgment, *Dallas Morning News, L.P. v. City of Dallas*, No. 06-06607-J (D.C. Dallas County Oct. 26, 2007); Jennifer LaFleur, *Ruling: Dallas Officials' E-Mails Must Be Turned Over*, DALLAS MORNING NEWS, Nov. 2, 2007.

<sup>38</sup> See LaFleur, *supra* note 37.

<sup>39</sup> White House employees during the current Bush administration apparently extensively used nongovernmental e-mail services (provided by the Republican National Committee). See House Comm. On Oversight and Government Reform, "The Use of RNC E-Mail Accounts by White House Officials," available at <http://oversight.house.gov/story.asp?ID=1362>. This issue is discussed in the context of the CREW case below.

<sup>40</sup> Shane Harris, "Court-ordered blackout leaves Interior employees without Internet, e-mail," Gov't Exec. (Dec. 14, 2001), available at <http://www.govexec.com/dailyfed/1201/121401h1.htm>.

a government official to disclose the existence of the e-mails voluntarily or must know from outside sources that they exist.<sup>41</sup> To address these concerns, some government bodies, including several presidential administrations and the Ohio Attorney General's Office, have adopted policies prohibiting the use of personal e-mail accounts or requiring employees to forward business e-mails sent on private accounts to a recordkeeping system.<sup>42</sup> These policies may not be effective in eliminating these concerns.

Citizens for Responsibility and Ethics in Washington (CREW) and several media outlets have recently asserted that some Bush Administration officials have used personal e-mail accounts to conduct presidential business in violation of the White House's stated policy that use of personal accounts is prohibited.<sup>43</sup> CREW is raising this and other issues related to the Bush Administration's failure to adopt an adequate recordkeeping system for the preservation of e-mails generally in a lawsuit that has been consolidated with a similar case brought by the National Security Archive.<sup>44</sup> The judge issued a temporary restraining order on November 12 requiring the defendants to "preserve media, no matter how described, presently in their possess [sic] or under their custody or control, that were created with the intention of preserving data in the event of its inadvertent destruction."<sup>45</sup> While this order covers back-up tapes used to preserve e-mails transmitted through government accounts, it is unlikely that this will ensure the preservation of e-mails transmitted through private accounts. If the use of private e-mail accounts allows agencies to circumvent disclosure under FOIA, either because recordkeeping systems fail to capture these e-mails or because the e-mails are not treated by courts as public or agency records subject to disclosure, FOIA requesters' access to government information will be limited.

---

<sup>41</sup> CITIZENS FOR RESPONSIBILITY AND ETHICS IN WASHINGTON, WITHOUT A TRACE: THE STORY BEHIND THE MISSING WHITE HOUSE E-MAILS AND THE VIOLATIONS OF THE PRESIDENTIAL RECORDS ACT (2007) [hereinafter CREW]; Mannies, *supra* note 36.

<sup>42</sup> CREW, *supra* note 41; LaFleur, *supra* note 37.

<sup>43</sup> See CREW, *supra* note 41 (citing several news articles discussing this issue).

<sup>44</sup> Complaint, Citizens for Responsibility and Ethics in Wash. v. Office of Admin., No. 07-01707 (HHK), (D.D.C. May 22, 2007); Complaint, Nat'l Sec. Archive v. Executive Office of the President, No. 07-01577 (HHK), (D.D.C. Sept. 5, 2007).

<sup>45</sup> Order, Citizens for Responsibility and Ethics in Wash. v. Office of Admin., No. 07-01707 (HHK), (D.D.C. Nov. 12, 2007).

## IV. ACCESS TO SOFTWARE

### A. Application of the Definition of "Agency Record" to Software

Software can be an indispensable tool for a requester wanting to make meaningful use of other information disclosed under FOIA. However, requesters seeking access to software under FOIA face several challenges. First, agencies often contract with private parties to obtain software, and under these contracts the private party generally reserves certain intellectual property rights in the software. Where agencies do not have full intellectual property rights over software, several courts have held that agencies lack adequate control over the software, and thus it fails to qualify as an “agency record” under FOIA.<sup>46</sup> Applying this principle broadly could undermine FOIA: it is a basic proposition that an agency cannot agree to maintain confidentiality if the statute requires disclosure, and yet contracts or licenses reserving private control over software are nothing more than just such agreements. The best resolution may be to make the agency data directly accessible to all, so that a requester would not have to acquire the software to access the database.

This issue arose in the context of the FARA database dispute mentioned earlier.<sup>47</sup> The requester had dismissed its lawsuit to obtain the outdated database when DOJ said it would provide a working copy of the new database when available. However, DOJ then said the new database could be provided only in a format that would require the requester to license the software at substantial expense, and even then the software would require extensive modifications to work with the new database.<sup>48</sup> This dispute was resolved when DOJ earlier this year made the database accessible to all through a dedicated FARA search site.<sup>49</sup>

Second, one court has held that software is not an “agency record” under FOIA because it “does not illuminate the structure, operation, or decision-making structure” of an

---

<sup>46</sup> *Gilmore v. U.S. Dep’t of Energy*, 4 F. Supp. 2d 912, 917-19 (N.D. Cal. 1998); *Tax Analysts v. U.S. Dep’t of Justice*, 913, F. Supp. 599 (D.D.C. 1996), *aff’d without opinion*, 107 F.3d 923 (D.C. Cir. 1997), *cert. denied*, 522 U.S. 931 (1997).

<sup>47</sup> See discussion accompanying note 10.

<sup>48</sup> See discussion at <http://www.publicintegrity.org/lobby/report.aspx?aid=735>.

<sup>49</sup> <http://www.usdoj.gov/criminal/fara/links/search.html>.

agency.<sup>50</sup> In Gilmore v. U.S. Department of Energy, the requester sought disclosure of CLERVER software, conferencing technology “that allows people in different geographical locations to simultaneously collaborate on complex technical drawings and schematics using their desktop computers.”<sup>51</sup> The court held that the CLERVER software failed to illuminate the agency's operations or processes because it “was not designed to be unique or responsive to any particular database, nor does CLERVER contain any database of information about DOE’s operations.”<sup>52</sup>

#### **B. Software as Confidential Commercial Information**

Even if an agency has sufficient control over software that illuminates the agency’s operations or structure so that the software qualifies as an “agency record,” software may often fall under FOIA Exemption 4, which protects trade secrets and other commercial information that is privileged or confidential. A record is confidential if disclosure would “cause substantial harm to the competitive position of the person from whom the information was obtained.”<sup>53</sup> Disclosure of software may possibly satisfy this test because making software available through FOIA could discourage persons from purchasing or licensing the software on their own. In addition, the Gilmore court raised concerns that fewer businesses would enter into agreements with government agencies to develop software if the software could be freely distributed under FOIA.<sup>54</sup>

#### **V. CONCLUSION**

While this paper highlights some of the challenges associated with the government's disclosure of electronic information under FOIA, it is not meant to suggest that agencies should be excused from responding fully to FOIA requests in the face of technological challenges or personnel constraints. To the contrary, technological advances present an opportunity to overcome what were previously insurmountable challenges associated with the extraction of data from databases, the preservation and retrieval of e-mails, and the protection of proprietary software.

---

<sup>50</sup> *Gilmore*, 4 F. Supp. 2d at 920.

<sup>51</sup> *Id.* at 916.

<sup>52</sup> *Id.* at 921.

<sup>53</sup> *Id.* at 922.

<sup>54</sup> *Id.* at 922-23.

Instead of continuing to rely on records maintenance and preservation systems that were designed without consideration of public access, government agencies should be expected to invest in systems that accommodate public access to government information. Instead of passively awaiting requests for electronic information, agencies should configure systems for direct public access, proactively providing searchable databases to meet public demands.

Government officials seldom view disclosure or dissemination as central to agency missions, and this has in turn led to hesitation, if not hostility, to devoting resources to FOIA administration. Public access to electronic information may pose some of the more complex problems, but it also holds some of the greatest promise for expanding government transparency.

---