Cloud-Based Public Records Pose New Challenges for Access

STEVE ZANSBERG

New York Governor Andrew Cuomo authorizes all state employees to destroy tens of thousands of e-mail records in which public business is discussed.[1] Florida Governor Rick Scott and his staff use "private" Gmail accounts to keep their official communications from being publicly scrutinized on the governor's highly touted "Project Sunburst" transparency website.[2] Pennsylvania Governor Tom Corbett deletes his e-mails every two weeks, specifically so that they will not be subject to that state's Right to Know Law (RTKL);[3] Corbett's key higher education adviser deleted his e-mails daily and later resigned after he responded to RTKL requests by producing only five e-mails for his entire first year in office.[4] Colorado's state legislature adopts a "read and delete" policy for all legislative staff e-mails.[5] It seems every day brings forth another crafty maneuver by government officials to evade accountability and transparency mandates[6] through data destruction, manipulation, or obfuscation.[7]

More information concerning the operations of government is being generated on a daily basis today than at any time previously—for example, in the predigital age, when pen, paper, and typewriter were the methods of written communications.[8] And, in many instances, the cost of providing copies of that information has plummeted to practically zero. Yet, despite the exponential growth in the amount of data and the ease of storing and accessing it, ironically, these communications and data storage technologies have simultaneously raised new barriers to citizens' ability to inspect those records under freedom of information (FOI) laws.

This article examines three related issues that digitized government records pose for citizens and journalists who wish to mine the burgeoning data repository to keep tabs on "what their government is up to":[9] (1) are e-mails and texts discussing public business, that are exchanged or housed on nongovernmental servers or devices, subject to disclosure under open records laws?; (2) what obligation do government employees have to retain e-mails and other electronically stored information so that they are available for inspection?; and (3) are citizens entitled to inspect and obtain copies of digital records in their "native format," including database files and "metadata"?

Control: *Whose* Records Are They?

Government entities across the nation are allowing, and even encouraging, public employees to utilize handheld devices not paid for by the government to communicate about public business; these governmental bodies are also retaining third-party vendors (e.g., Gmail, Yahoo!, etc.) to provide and maintain e-mail or text messaging accounts that are completely separate from, and inaccessible to, government servers.[10] Thus, increasingly, courts and state attorneys general are being called upon to answer whether electronic records housed on such "private" communications devices and servers are subject to the states' public records statutes, or are simply beyond their reach.

As with many issues discussed in this article, the application (or non-application) of various records laws to a particular category of record (here, e-mails discussing "public business" that are housed exclusively on a nongovernmental server or device) depends, in large part, on how the relevant statute defines "public record."[11] Most states have a version of a definition that defines public records as (1) any "writing," usually defined quite broadly to include any written communication "regardless of physical form or characteristics"; (2) that is "made, maintained, or kept" by a government employee or over which a government agency has either physical custody or a right of access; and (3) whose content bears some logical connection to the conduct of public business.[12] Thus, electronic communications that address "purely private," nongovernmental matters, have been found *not* to be "public records," even if they are exchanged over, and/or housed upon, government-funded communications devices (because all three conditions above must be satisfied).[13]

This article addresses whether the converse is true: is a record that is "made, maintained, or kept" by a government employee, acting in an official capacity,[14] and whose content *does* concern his or her official conduct, a "public record" even though it does not reside (and perhaps never *did* reside) on a government-provided or – funded device or data repository? (See table 1.)

There are two subcategories within public business records kept on privately funded systems: (1) records kept or maintained on a server or in a records repository operated and controlled by an "outside vendor," beyond the physical possession or actual custody of the government (e.g., Gmail, Verizon, BlackBerry, or Sprint Communications)but on behalf of a government agency; and (2) records kept or maintained exclusively in a "personal" account or device belonging to a public official or employee,

Steve Zansberg is a partner in the Denver, Colorado office of Levine Sullivan Koch & Schulz, LLP, the immediate past chair of the Forum, and the president of the Colorado Freedom of Information Coalition. *The author thanks two LSKS summer associates, Ariel Glickman (George Washington University School of Law, J.D. 2016) and Rebecca Guiterman (NYU School of Law, J.D. 2015), for their research assistance on this article.*

Table 1: Public vs. Private Records

Location of the Record	Content of the Record		
	Purely "Private"/ No Official Business	Public Business	
On Publicly Funded Device or System	(Generally) Not a Public Record[15]	Public Record	
On Privately Funded Device or System	Not a Public Record	(Generally) Public Record	
		On Third-Party Vendor's System	On Government Employee's "Personal" Drive

but not accessible to the government employer, other than through that official's or employee's consent. Both sets of cases will be discussed below.

Under traditional notions of which public records "belong" to the government, and therefore to the public, the answer to the question posed above Table 1 is emphatically and unequivocally, "yes." To understand why, you need only consider how the answer would be determined in another context, before the advent of electronic communications. Suppose a governor, mayor, or city police chief transmits official government communications—e.g., orders or directives to subordinate public employees or policy statements to constituents—using his or her own personal stationery (not official government letterhead), envelope, and stamps, and thereafter maintains copies of all such written correspondence only in a personal filing cabinet at his or her private residence or, alternatively, off government premises at a privately owned document warehouse. Without question, all such writings were (1) "made, maintained, or kept" by a government official, acting in his or her official capacity; (2) their content is directly related to official governmental functions; and (3) those writings are within the possession, custody, or control of the government employee (and therefore, under the traditional rules of agency, are available to the government employer). Thus, under the three-part test that generally applies under public records statutes, those writings—though not transmitted via, nor stored within, government-provided media—are nonetheless "public records." Not surprisingly, several courts that have addressed this question in the context of digitized records have resorted, by analogy, to "life before the digital era," and have reached the same conclusion.[16]

The key question in these cases—whether e-mails (and other electronic records) stored on servers and/or devices not *owned* by the government—turns, in large measure, on whether under the applicable statutory text those records are deemed to be within the possession, custody, *or control* of the government entity from whom the records are sought. With respect to the records residing only on individuals' "personal" accounts or devices, there is also an ancillary question whether a governmental search of a government official's or employee's "personal" account and/or device would constitute an unreasonable search or seizure in violation of the Fourth Amendment.

"We'd Love to Give You Those Records, but We Don't Have Them"

There is a fair degree of consensus in the case law that public records stored on nongovernmental accounts *on behalf of the government entity*, to which the government retains a contractual right of access, are that entity's public records. *Flagg v. City of Detroit*[17] provides one of the most extensive and well-reasoned explanations of why e-mails, text messages, and other electronic "public records" maintained by a third-party vendor *for the benefit of* a government entity are within the "control" of the government, and are therefore required to be produced by that government entity in response to a records request.

Flagg involved a records request under civil discovery rules on the City of Detroit for text messages sent or received by former Mayor Kwame Kilpatrick, all of which resided in a message archive on the servers of Skytel, a private messaging service provider. None of the messages at issue resided on any city-owned server. U.S. District Court Judge Gerald E. Rosen found that because, presumably, the city had a contractual right to access the archived messages maintained by SkyTel, the city had sufficient "control" over those messages to require the city to produce them in response to a records request. Although the ruling arose under the federal rules governing civil discovery, the court expressly drew upon case law applying Michigan's Freedom of Information Act (FOIA):

> Because at least some of the text messages maintained by SkyTel are "public records" within the meaning of Michigan's FOIA, it would be problematic, to say the least, to conclude that the City lacks a legal right to obtain these records as necessary to discharge its statutory duty of disclosure. Such a conclusion also would be contrary to the pertinent Michigan case law. First, the Michigan courts have

> held that the FOIA duty of disclosure, like the Rule 34 duty of production, extends to public records within the possession *or control* of a public body.[18]

After summarizing that case law, the court concluded:

> [Case law applying Michigan's FOIA] provides a compelling basis for concluding that the Defendant City has control, within the meaning of Rule 34(a)(1), over any "public records" that might be retained by third party SkyTel under its contract with the City.
>
> [W]hile the record does not disclose the terms of the City's contracts with SkyTel, . . . the Court assumes that the City has at least some sort of contractual right of access to the text messages preserved by SkyTel in the course of its contractual relationship with the City.[19]

Thus, in jurisdictions where the definition of "public records" or "agency records" includes an explicit or implicit "possession, custody, *or control*" criterion, the fact that a government entity has a contractual right to access records maintained on its behalf by an outside vendor (whether a paper records "cold storage" warehouse, or a cloud-based provider like Gmail) should require the government entity to exercise its right of access to make available such records in response to a request for inspection from the public.

This approach has been followed by courts applying the federal FOIA, which provides public access only to "agency records" but does not define what *is* an agency record.[20] Under that statute, several courts have held that when an executive branch agency has the right to obtain a document from a nongovernmental outside vendor, the agency has "constructive control" over such records, rendering them "agency records" subject to the FOIA.[21]

"Those Records Belong to Me, Not to My Government Employer"

The far more contentious issue to date is whether records discussing public business maintained exclusively on an individual government official's personal account and/or device is a public record *of* the government employer. As demonstrated below, the majority of courts that have addressed the issue have determined that *all* records generated or received by a public official acting in his or her official capacity, in which official public business is discussed, are the appropriate "property" of the government employer; thus, such records, even if housed on nongovernmental devices or accounts, should properly be deemed the public records *of the government*, not the individual. However, not all courts have reached this conclusion.

Applying the federal FOIA, one federal court held that e-mails maintained by a government employee exclusively in his nongovernmental (university) account were *not* "agency records" because they were not within the agency's "control" as defined by the court.[22] This ruling is at odds with other courts' recognition that there is "no basis" in the FOIA or its legislative history to view an agency employee as "distinct from his [or her] department [or agency] for FOIA purposes."[23] Under these precedents, if a federal agency employee creates, receives, or maintains an electronic record in the course of fulfilling or carrying out his or her duties on behalf of the agency,[24] those records are subject to a FOIA request on the agency, even if the record is maintained exclusively in the employee's "personal" account or device.[25] Summarizing this body of case law, two commentators recently concluded: "Common sense, case law, and FOIA's plain language compel the conclusion that, irrespective of federal executive branch agencies' employees' reasons for using personal e-mail accounts or personal communications devices to conduct agency-related business within the scope of their employment, their work-related communications must be subject to FOIA's disclosure provisions."[26]

Judges in nine states (Alaska, Arizona, Arkansas, Illinois, New York, Ohio, Pennsylvania, Virginia, and Washington)[27] and the District of Columbia have held that if the content of an e-mail, text message, or other electronic record sent or received by a government employee relates to the conduct of governmental business, it is subject to those states' open records acts; the actual physical location of such a writing is immaterial.

In July 2014, the Superior Court for the District of Columbia, applying D.C.'s FOIA,[28] held that D.C. councilmembers' e-mails maintained exclusively on so-called "private" accounts were public records subject to the Act.[29] Judge Stuart G. Nash held that e-mails of Dianne Barnes, maintained in her personal e-mail account while acting in her capacity as commissioner of D.C.'s Advisory Neighborhood Commission, were "prepared, owned, used, in the possession of, or retained by a public body" and were therefore "public records" of the Commission under the Act.

In addition to the above judicial opinions, the attorneys general in 10 states (Alaska, Florida, Illinois, Maryland, New Mexico, North Dakota, Oklahoma, Oregon, Texas, and Wisconsin) have issued formal opinions stating that e-mail messages created, sent, or received by government officials that discuss public business are public records under those states' FOI laws, regardless of the physical location or records repository where such e-mail messages reside.[30]

Recently, the Texas Court of Appeals twice addressed whether e-mails of government employees maintained exclusively in personal accounts are subject to that state's Public Information Act (PIA).[31] In *Adkisson v. Abbott*, the court of appeals affirmed both the Texas attorney general's and the Travis County District Court's ruling that a county commissioner's e-mails in which he discussed public business were public records under the PIA.[32]

> If the information in the official-capacity e-mails contained in the Commissioner's personal e-mail accounts 1) is collected, assembled, or maintained for the County; 2) is connected "with the transaction of official business" for the County; and 3) the County either owns or has a right of access to the information, then the information is

public information under the statutory definition.[33]

Commissioner Adkisson did not contest that the e-mails requested by the *San Antonio Express-News* were connected with the transaction of official business; instead, he argued that they were not collected, assembled, or maintained for Bexar County and that Bexar County had no right to access his official-capacity e-mails stored off of county computers.[34] The court rejected Adkisson's first argument:

> To conclude otherwise would lead to the absurd result that the Commissioner could conduct all his official County business correspondence through his personal e-mail accounts without it being subject to the PIA, even if the same correspondence would be subject to the PIA if he used his County e-mail account.[35]

Relying on the county's records management administrative policy, the court further concluded that:

> any local government records collected, assembled, or maintained in the Commissioner's e-mail accounts *belongs to the County, not to the Commissioner in his individual capacity*. Conducting County business through a personal e-mail account instead of through an official County e-mail account does not change the County's ownership of the local government records created or received by the Commissioner as a County government officer.[36]

The court also rejected Adkisson's claim that inspection of the official business e-mails in his personal account would constitute an invasion of his personal privacy, noting that Adkisson had failed "to explain how the release of documents concerning the transaction of official business could be confidential."[37]

But how much pressure can a government agency bring on its employees to provide the agency the records that reside entirely outside of the government's filing systems? In the second of the two rulings, the Texas Court of Appeals answered by saying, essentially, "none." After a citizen, Stephanie Allala, asked to inspect the e-mails of the City of El Paso's councilmembers, and specifically "any public business emails that may have been conducted on the personal email accounts of these individuals," the state's attorney general opined that such records were, in fact, subject to the Texas PIA.[38] Accordingly, the City of El Paso produced to Allala all of the e-mails it had retrieved, upon request, from the city councilors, and then stated it had fully complied with her request. Allala challenged the city's representation, and sought discovery to determine how assiduously the city councilors—one of whom had stated in writing he would *not* produce his "private emails" *absent a court order*—had complied with the City's request that they search their personal e-mail accounts and produce responsive records. The court of appeals stated that the city could not compel the city councilors to comply with its request, and so the city had satisfied *its* burden to produce *its* responsive records to Allala.

Both the *Adkisson* and *Allala* cases were decided under the prior (2010) version of the Texas PIA. In 2013, that statute was amended expressly to clarify that:

> "public information" means information that is written, produced, collected, assembled, or maintained . . . by an individual officer or employee of a governmental body in the officer's or employee's official capacity and the information pertains to official business of the governmental body[; in addition, this definition] applies to and includes any electronic communication created, transmitted, received, or maintained *on any device* if the communication is in connection with the transaction of official business.[39]

Absent such a legislative "fix" to this ruling, perhaps the appropriate—and necessary—procedural step is to name each of the agency's employees (or here, the individual city councilors) as defendants, and ask the court to order each of them, individually, to retrieve the "public records" in their personal possession, just as the El Paso city councilor had stated would be necessary to compel his compliance with the law.

Notwithstanding this trend of recent cases favoring the public's right to know, in March 2014, California's Court of Appeals ruled to the contrary, reversing a trial court's determination that the e-mails sent

How much pressure can a government agency bring on its employees to provide records that reside entirely outside of the government's filing systems?

and received by the mayor of San Jose, California, exclusively over a nongovernmental exchange server, were "public records" of the city under the California Public Records Act (CPRA). The case began in August 2009, when the *San Jose Mercury-News* received two e-mails from a San Jose city councilmember indicating that councilmembers were communicating during and after city council meetings in regard to a proposal to give "millions of city redevelopment dollars to former Mayor Tom McEnery."[40] The *Mercury-News* filed a complaint asking that the City of San Jose and the San Jose Redevelopment Agency, as well as city officials and former officials, be required to provide access to "e-mails, text messages, and other electronic information relating to public business, regardless of whether they were created or received on the City owned computers and servers or the City Officials' personal electronic devices."[41] In March 2013, the superior court held in favor of the *San Jose Mercury-News*, ruling that all

of the requested records were public records of a "local agency."[42]

However, in March 2014, the California Court of Appeals reversed, holding that the statute's definition of "local agency" did not include the agency's individual officers or employees: "It is the *agency* . . . that must prepare, own, use, or retain the writing in order for it to be a public record, [and thus] those writings that are not accessible by the City cannot be said to fall within the statutory definition."[43] The court held that the CPRA does not impose a duty on the city to produce messages stored on the personal electronic devices and accounts of its employees or officials that are inaccessible to the agency; nor is the city required to search those devices and accounts in response to a CPRA request. The court rejected the plaintiff's (and media amici's) argument that the city had "constructive control" over the mayor's and councilmembers' personal devices. Curiously, although the court acknowledged that in 2004 California's voters had passed Proposition 59, which declared that "the meetings of public bodies and *the writings of public officials and agencies* shall be open to public scrutiny,"[44] that language was not considered in the court's analysis.

Access to electronic records turns on how long the government is required to maintain copies of those records in which public business is discussed.

As this article goes to press, briefing is being prepared before the California Supreme Court[45] in this important case that will be closely watched by other courts throughout the nation.

"Privacy Rights" of Government Employees Should Not Bar Access to "Public Records"

As indicated above, some courts have expressed concern for public employees' privacy rights that would supposedly be implicated by a regime requiring government entities to search individuals' personal devices and Gmail accounts to locate writings that satisfy the definition of public records (those whose contents bear a "demonstrable connection" or "substantial nexus" to the discharge of official public duties). However, these concerns are properly limited only to the e-mails or records whose content is truly "private," i.e., those that do *not* satisfy the definition of "public record." No claim can be made by a public employee that his or her communications in his or her official capacity, discussing official public business, are subject to a reasonable expectation of personal privacy.[46] Thus, only purely *private* information—i.e., information that does not reflect or document the public employee's discharge of his or her official duties—is entitled to any expectation of privacy, and is outside the statutory definition of "public records."[47]

One way to minimize the intrusion on a public employee's legitimate privacy rights—by exposing his or her truly private e-mails to scrutiny by his or her government employer—is to impose upon the employee himself or herself the duty to search and provide access to public records housed in a personal account. Increasingly, states, cities, and municipalities are adopting policies requiring public employees to send public records from their personal accounts and devices to a government central repository.[48] Other government leaders have issued directives requiring public employees to restrict their use of personal devices to nongovernmental communications, so that all "public records" will be exchanged and housed on government-controlled media.[49]

Indeed, the it is this very concern for personal privacy interests and the "burden" of having government employees sort through electronic records to extract only those whose contents address public business that provides the strongest policy argument for why government employees, as a general policy/rule, should be required to maintain a separate account and/or electronic folders in which only their governmental IMs, texts, e-mails, and other records are stored. A rule of law that condones the intermingling of private and public records—whether electronic or paper form—to shield public records from inspection under FOI laws only incentivizes the intermingling of records. If a government official chooses to intersperse his or her public and private writings in a single account, device, or file cabinet, then he or she should not be heard to complain about the "administrative burden" of sorting those records into two piles, private and public, to comply with FOI mandates.

Retention: "I'd Be Glad to Give You Those Records, Only We No Longer Have Them"

Both the federal FOIA and state public records laws provide a right of access only to those records that are in existence at the time of the request; the government is not required to generate a new record in response to a records request, nor to provide access to a record that no longer exists.[50] Thus, for many records requesters, the question of access to electronic records turns on how long the government is required to maintain copies of those records in which public business is discussed. (Notably, unlike paper records, which required affirmative physical action to destroy or discard, digital records—especially text and e-mail messages—have a built-in, automatic "shelf life" as a result of standardized "auto-delete" functions).

The answer to the question "how long must a record be kept?" frequently depends on a set of laws and policies extraneous to the FOI or "right to know" law.[51] The duty to retain public records generally is found in companion statutes that define "public records" for purposes of records preservation, as in a state archives.[52] Unfortunately, in many instances, these statutes, and the records retention schedules promulgated by state archivists thereunder, leave a tremendous amount of discretion to individual records custodians. Worse still, those custodians are often the very employees who generated and exchanged the e-communications. Yet they are given the authority to determine whether the records are of "preliminary or short-term informational value" or "lasting value" in documenting the workings of government agencies.[53]

At the federal level, the recent high-profile scandal involving the destruction of hundreds of e-mails that had been on the laptop computer of former (and embattled) IRS Commissioner Lois Lerner brought to the fore the issue of what obligations executive branch agencies have to retain electronic records. During congressional hearings exploring the loss of Lerner's e-mails, the U.S. archivist, David Ferriero, told the House Oversight and Government Reform Committee that the IRS "did not follow the law" when it failed to report that the e-mails had been lost.[54]

The Federal Records Act sets forth the executive branch agencies' duties to preserve records in accordance with the general records schedules promulgated by the National Archives and Records Administration (NARA).[55] It is the duty of each federal agency (270 of which are subject to the Federal Records Act) to propose disposition schedules for their records, and the vast bulk (95–97 percent) of records are eventually destroyed.[56] Under the Managing Government Records Directive adopted by the Obama administration in 2011, "[b]y the end of 2016, all agencies need to manage e-mail in automated, electronic ways."[57] In August 2013, NARA issued its guidance on e-mail management,[58] which sets forth what is referred to as a "capstone" approach: under this tiered system, all work-related e-mails of certain high-level department officials, who are deemed "capstone" employees, are to be maintained permanently by the agency; those of lower (mid-) level agency employees are to be preserved for seven years; and those of the more subordinate employees are to be retained for shorter periods of time, according to the agency's needs.[59]

As many government entities have discovered, failure to ensure that electronic records are properly maintained and preserved can give rise to additional burdens on such agencies to conduct adequate "search and retrieval" of records.[60] The consequences of *intentional* public records destruction can also prove quite costly. In 2012, a Colorado school district was ordered to pay $122,000 in attorneys' fees to the parents of a student after a school official had ordered several school employees to destroy thousands of e-mails and other public records.[61] In January 2014, Orange County, Florida, agreed to pay a coalition of citizen groups $90,000 to settle a lawsuit the media dubbed "textgate" after a criminal investigation concluded that the mayor and four county commissioners had violated state law when they deleted text messages that were public records.[62] And in 2009, the City of Venice, Florida, was ordered to pay $750,000 in attorneys' fees following the settlement of a lawsuit brought by a citizen's group that accused city councilmembers of having conducted illegal meetings via e-mail and then destroying or failing to preserve public records; that was on top of the $600,000 the city paid to defend the councilmembers in the suit.[63]

Even though storing digitized records is generally much cheaper than warehousing paper files, massive data storage imposes significant costs and administrative burden on governments, particularly in light of the tremendous volume of data that governments generate daily. Hence, government agencies at all levels—federal, state, and local—have a legitimate need to *not* "keep" everything in perpetuity. Most states' public records preservation and archives statutes dictate that the length of time for keeping records must be determined by the *content* of the record, not its format, medium, or title.[64] But the manner in which specific records retention schedules are promulgated and implemented, and particularly when e-records "expire" automatically, will continue to pose problems for public records requesters.

The conclusion of the 2009 report on this subject by the Reporters Committee for Freedom of the Press (RCFP) is as relevant and accurate today as when it was published five years ago: "E-mail retention policies likely will generate increasing amounts of litigation—and deservedly so. In states where the issue has not been settled by statute or case law, there are effectively no bright-line legal mandates requiring officials to retain e-mail [or other digitized] records for a given period of time."[65]

Production: "Of Course You Can Have Our Database; We'll *Print It Out* for You"

Another issue that often arises is whether the public is entitled to access the electronic records *in the same format* in which the government maintains the data. FOIA case law prior to the "digital era" sheds some light on this question: federal courts recognized that a request to inspect (and listen to) an *audio* recording is not satisfied by obtaining access only to a written transcript of the recording, precisely because the "quantum of information" on the recording (voice fluctuations, pauses, and inflection) is lost in the transcription process.[66] However, when the *quantum of information* remained unchanged—as when a set of data points is transferred from a computer tape to a microfiche—the courts held that there was no "right" under the FOIA to demand access to the tape itself.[67] However, subsequently (and after the FOIA was amended in 1996),[68] federal courts have disagreed with this analysis, and have required federal agencies, such as NOAA, to provide access to information kept in a digitized form, finding that a paper printout of the same data set does not provide access to the particular "agency record" sought.[69]

But how much effort must the government expend to make its records available to the public? The federal FOIA provides that an agency shall make a record available "in any form or format requested by the person *if the record is readily reproducible by the agency* in that form or format."[70] The Justice Department's Office of Information Policy has stated that the onus is on the records requester to dictate the format in which he or she wishes to receive an agency record.[71] Further, agencies should make "reasonable efforts" to produce a record in a requested format if it is "readily reproducible" in that form.[72] Many federal courts adhere to the standard for reasonableness announced by the Ninth Circuit in *TPS, Inc. v. U.S. Department of Defense*: a record is readily reproducible if an agency already has the means to create and convert documents into a specific format even if it does not routinely do so for purposes of responding to FOIA requests.[73]

Some, but not all, states' open records laws expressly guarantee the right to obtain records in a particular format if so requested.[74] For example, Mississippi's statute provides that "[a]

public body shall provide a copy of the record in the format requested if the public body maintains the record in that format."[75] Notwithstanding these legislative directives to provide access to digitized records in their native format, many government entities have refused to do so. Common excuses include concern about security of the data[76] and the "burden" of redacting nonpublic information,[77] such as Social Security numbers.

State and federal courts called upon to enforce these directives have not been consistent in doing so. Some courts have upheld the right of the requester to receive information in the particular medium requested, liberally construing the relevant FOI law,[78] while other courts have adhered to a very narrow interpretation of what is "readily reproducible."[79] Several state courts have distinguished case law applying the federal FOIA because it has been interpreted to provide access only to "information," as opposed to state statutes that guarantee the right to access the very "public records" in the hands of the government.[80]

In 1992, Ohio's Supreme Court provided a clear and compelling explication of why access to information—in the same form and format in whichis is maintained by the the government—is *required* to fulfill the purposes of a "public records" act:

> [A] public agency should not be permitted to require the public to exhaust massive amounts of time and resources in order to replicate the value added to the public records through the creation and storage on tape of a data base containing such records.
> . . . .
> Here, the added value is not only the organization of the data, but also the compression of the data into a form that allows greater ease of public access. Thus, in keeping with the expressed intent of the General Assembly to provide broad access to public records, we hold that a governmental agency must allow the copying of the portions of computer tapes to which the public is entitled, if the person requesting the information has presented a legitimate reason why a paper copy of the records would be *insufficient or impracticable*, and if such person assumes the expense of copying.[81]

"Electronic Fingerprints": Access to Metadata

Prior to the digital age, when paper documents were stored in filing cabinets, there would sometimes be an index to the files, generated by government employees, showing the "filing scheme" that might, in appropriate circumstances, reveal how the documents were characterized and classified by government officials (e.g., "enemies" or "personas non grata"). Such government-generated catalogs or file indexes were unquestionably "public records" that reflected the "mental processes" or "inner workings" of the government.

With the advent of the digital era, however, the filing systems are automated, and the data-processing systems—whether they be spreadsheet programs, word processing, e-mails, or text messaging—automatically record and track various information that previously required human labor (and that more often than not was simply not recorded). Examining the "metadata" on a typical document created and edited on Microsoft Word, for example, one can determine who first generated the document, on what date and at what time, and for how long it was open and being edited, and thereafter, by whom, on which dates, and at which times; indeed, depending on the document settings, it is sometimes possible to recreate earlier drafts of a document and to show which persons made which edits.[82]

Access to metadata, referred to as "information describing the history, tracking, or management of an electronic document,"[83] associated with public records is important for several reasons. Metadata can be used to reveal the authenticity of documents and, alternatively, to expose possible government misconduct.[84] Metadata also serves to make electronic records searchable and thus more useful.[85]

No federal court has yet definitively addressed whether metadata constitutes an "agency record" under the federal FOIA.[86] In 2011, Judge Shira A. Scheindlin of the Southern District of New York ruled that "metadata *maintained* by the agency *as a part of an electronic record* is *presumptively* producible under FOIA, unless the agency demonstrates that such metadata is not 'readily reproducible.'"[87] However, that opinion was short-lived. The parties subsequently settled and the opinion was withdrawn, so it holds no precedential value.[88]

State courts, on the other hand, have been fairly uniform in concluding that metadata encompasses an "agency record" that must be produced under state open records laws.[89] Based on the language of FOIA itself, state courts' interpretations of similarly worded state open records laws, and executive guidance, there is a strong argument that metadata should be considered part of an agency record subject to the federal FOIA, as Judge Scheindlin had once concluded.

As Communications Technology Evolves, So Will the Legal Battles over Access to Public Records

Progress toward the "paperless office" continues in the halls of government as it does in the private sector. As ever more government records that shed light on the conduct of the public's business are comprised of digital zeros and ones, and are stored "off premises" in the cloud and/or on portable electronic devices, the issues discussed in this article will increasingly be litigated.[90] Thus far, courts have generally (and appropriately) recognized that is it the *content* of the record, *not* its physical form or location, that should determine whether the public is entitled to inspect and copy such data. It is hoped that government leaders' lofty proclamations extolling the virtues of "transparency" and committing to "proactive access" will someday translate into concrete steps—that the government will systematically post and/or distribute public records without requiring that individual requests be submitted. Until that Elysian day arrives, however, advocates for access will continue to battle to inspect public records, wherever they reside, and

in whatever format. After all, such records are often the only way reliably to determine what our government is up to.

Endnotes

1. Theodoric Meyer, *Why Is the Cuomo Administration Automatically Deleting State Employees' Emails?*, ProPublica (Aug. 11, 2014), http://www.propublica.org/article/why-is-cuomo-administration-automatically-deleting-state-employees-emails?utm_source=et&utm_medium=email&utm_campaign=dailynewsletter#.

2. Mary Ellen Klas, *Lawsuit Seeks Disclosure of Private Email Accounts of Gov. Rick Scott, His Staff*, Tampa Bay Times, Aug. 13, 2014, http://www.tampabay.com/news/politics/stateroundup/lawsuit-seeks-disclosure-of-private-email-accounts-of-gov-rick-scott-his/2192738.

3. Mary Wilson, *Emails a Blind Spot in PA Transparency Laws*, WITF (Aug. 15, 2014), http://www.witf.org/state-house-sound-bites/2014/08/e-mails-a-blind-spot-in-pa-transparency-laws.php.

4. Mary Niederberger & Bill Schackner, *Corbett Defends Education Adviser Who Resigned amid Questions about Duties*, Pittsburgh Post-Gazette, Aug. 15, 2014, http://www.post-gazette.com/news/education/2014/08/14/Corbett-defends-education-adviser-who-resigned-amid-questions-about-his-duties/stories/201408140291.

5. Tessa Cheek, *Colorado's Analog Records Laws Lag Behind Digital Practice*, Colo. Indep. (Jan. 24, 2014), http://www.coloradoindependent.com/145719/colorados-analog-records-laws-lag-behind-digital-practice.

6. In 2012, the chief of staff to New Mexico Governor Susana Martinez was caught on tape stating that he never used his government-provided e-mail account to discuss public business, so that his communications would not be subject to that state's open records law. *See* Steve Terrell, *Martinez Administration Dodges Requests for Out-of-State Travel Costs*, Santa Fe New Mexican, Mar. 20, 2014.

7. *See* Aaron Mackey, *Governments Continue to Come Up with New Ways to Prevent Access to Records*, News Media & L. (Reporters Comm. for Freedom of the Press, Arlington, Va.), Winter 2013, at 10, *available at* http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-winter-2013/governments-continue-come-n; Sarah Laskow, *Use of Private Emails for Public Work Sparks FOIA Battle*, Colum. Journalism Rev. (Feb. 13, 2013), http://www.cjr.org/cloud_control/new_mexico_public_records_thin.php?page=all#sthash.LuNeB9HY.dpuf.

8. A 2003 study found that the amount of information available, worldwide, had roughly doubled in the previous three-year period, and 93 percent of that information was in digital form. Peter Lyman & Hal R. Varian, Sch. of Info. Mgmt. & Sys., Univ. of Cal.-Berkeley, How Much Information? (2003), *available at* http://www.sims.berkeley.edu/research/projects/how-much-info-2003/, *cited in* Nat'l Elec. Commerce Coordinating Council, Challenges in Managing Records in the 21st Century 14–15 (2004), *available at* https://library.osu.edu/assets/Uploads/RecordsManagement/Challenges-in-21st-e-recs-neccc.pdf.

9. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 772–73 (1989).

10. *See, e.g.*, Kristen Berg, *Federal Government Enters the Era of the "Cloud,"* News Media & L. (Reporters Comm. for Freedom of the Press, Arlington, Va.), Fall 2011, at 16, *available at* http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-fall-2011/federal-government-enters-era; John Breeden II, *Forever Accessible Archives? Michigan Moves Its Records to the Cloud*, GCN (Mar. 5, 2014), http://gcn.com/articles/2014/03/05/michigan-archives.aspx; Winifred Shum, *State of Oregon Embraces HP TRIM for Statewide Cloud-Based Records Management*, HP Autonomy (Jan. 8, 2013), http://www.autonomy.com/work/news/details/hkfgxbqi.

11. A very helpful guide to all 50 states' laws on this subject was produced in 2009 by the Reporters Committee for Freedom of the Press (RCFP). *See* Cristina Abello, RCFP, Access to Electronic Communications (2009), *available at* http://www.rcfp.org/rcfp/orders/docs/ELECCOMM.pdf. Other useful secondary sources include Andrea G. Nadel, Annotation, *What Are "Records" of Agency Which Must Be Made Available under State Freedom of Information Act*, 27 A.L.R.4th 680 (Supp. 2014); Marjorie A. Shields, Annotation, *Disclosure of Electronic Data under State Public Records and Freedom of Information Acts*, 54 A.L.R.6th 653 (Supp. 2014); and Holly Piehler Rockwell, Annotation, *State Freedom of Information Act Requests: Right to Receive Information in a Particular Medium or Format*, 86 A.L.R.4th 786 (Supp. 2014).

12. *See* Larry Walsh, *Google Drops Lawsuit for Government Cloud*, Channelnomics (Sept. 27, 2011), http://www.channelnomics.com/channelnomics-us/news/2365402/google-drops-lawsuit-for-government-cloud (reporting that "Google has won several federal, state and municipal government contracts, including the [federal] General Services Administration, the State of Wyoming and the city of Los Angeles").

13. An excellent summary of this body of case law can be found in Peter S. Kozinets, *Access to the E-Mail Records of Public Officials: Safeguarding the Public's Right to Know*, Comm. Law., Summer 2007, at 17. *See, e.g.*, Denver Publ'g Co. v. Bd. of Cnty. Comm'rs of Arapahoe Cnty., Colo., 121 P.3d 190 (Colo. 2005) (holding that sexually explicit text messages exchanged between two government employees on county-provided devices, while on duty, were not "public records" because the content of those messages did not bear "a demonstrable connection" to the discharge of public functions).

14. The Colorado Supreme Court has held that when a public employee makes only passing reference to his or her professional conduct in the entries of a private diary, that diary is "made, maintained, [and] kept" purely in that employee's private capacity. Wick Commc'ns Co. v. Montrose Cnty. Bd. of Cnty. Comm'rs, 81 P.3d 360 (Colo. 2003).

15. *See, e.g.*, *Denver Publ'g Co.*, 121 P.3d 190; State v. City of Clearwater, 863 So. 2d 149 (Fla. 2003); Howell Educ. Ass'n, MEA/NEA v. Howell Bd. of Educ., 789 N.W.2d 495 (Mich. Ct. App. 2010); State *ex rel.* Wilson-Simmons v. Lake Cty. Sheriff's Dep't, 693 N.E.2d 789 (Ohio 1998); Forbes v. City of Gold Bar, 288 P.3d 384 (Wash. Ct. App. 2012); Associated Press v. Canterbury, 688 S.E.2d 317 (W. Va. 2009); Schill v. Wis. Rapids Sch. Dist., 786 N.W.2d 177 (Wis. 2010); *see also* Kozinets, *supra* note 13.

16. *See, e.g.*, *City of Clearwater*, 863 So.2d at 154 (concluding that "the determining factor [in deciding whether e-mails are public records] is the nature of the record, not its physical location," and noting that "an agency cannot circumvent the Public Records Act by allowing a private entity to maintain physical custody of documents that fall within the definition of 'public records'").

17. 252 F.R.D. 346 (E.D. Mich. 2008).

18. *Id.* at 356 (citing MacKenzie v. Wales Twp., 635 N.W.2d 335, 339 (Mich. Ct. App. 2001); Easley v. Univ. of Mich., 444 N.W.2d 820, 822 (Mich. Ct. App. 1989)).

19. *Id.* at 357.

20. U.S. Dep't of Justice v. Tax Analysts, 492 U.S. 136, 142 (1989). Two requirements must be met before materials will be considered to be "agency records." First, the agency must "either create or obtain" the documents. *Id.* at 144 (quoting Forsham v. Harris, 445 U.S. 169, 182 (1980)). Second, the agency "must be in control of the requested materials at the time the FOIA request is made." *Id.* at 145.

21. *See, e.g.*, Burka v. U.S. Dep't of Health & Human Servs., 87 F.3d 508, 515 (D.C. Cir. 1996) (finding that HHS had "constructive control" of data tapes in the possession of a private research firm); Ryan v. Dep't of Justice, 617 F.2d 781, 785 (D.C. Cir. 1980) ("A simple possession standard would permit agencies to insulate their activities from FOIA disclosure by farming out operations to outside contractors."); Democratic Nat'l Comm. v. U.S. Dep't of Justice, 539 F. Supp. 2d 363, 367 (D.D.C. 2008) (concluding that e-mails maintained on a political party's server are subject to FOIA, and that "because the form of the document does not factor into the analysis under FOIA, the court cannot adopt a *per se* rule that any e-mails sent on the RNC servers are not covered by FOIA").

22. Competitive Enter. Inst. v. NASA, 989 F. Supp. 2d 74, 86–87 (D.D.C. 2013); *see also* Houghton v. U.S. Dep't of State, 875 F. Supp. 2d 22, 30 (D.D.C. 2012).

23. *Ryan*, 617 F.2d at 787.

24. As the D.C. Circuit has held, "the purpose for which the document was created, the actual use of the document, and the extent to which the creator of the document and other employees acting within the scope of their employment relied upon the document to carry out the business of the agency" are "important considerations" for distinguishing between "agency records" and personal materials. Bureau of Nat'l Affairs v. U.S. Dep't of Justice, 742 F.2d 1484, 1493 (D.C. Cir. 1984).

25. Judicial Watch, Inc. v. U.S. Dep't of Energy, 310 F. Supp. 2d 271, 297 (D.D.C. 2004) ("[T]he actual physical location of the documents is not dispositive; the issue is actual or constructive 'control.'"), *aff'd in part, rev'd in part*, 412 F.3d 125, 133 (D.C. Cir. 2005) (recognizing that "[a]s the district court correctly observed, . . . possession is not the proper test of whether a record is within an agency's control," and holding that records generated by and in possession of a Department of Interior (DOI) employee "in the legitimate conduct of his official duties" were agency records of DOI); *see also* Landmark Legal Found. v. EPA, 959 F. Supp. 2d 175, 184 (D.D.C. 2013) (authorizing discovery into the adequacy of the EPA's search for responsive records, including the personal e-mail accounts of individual employees, because "[t]he possibility that unsearched personal email accounts may have been used for official business raises the possibility that leaders in the EPA may have purposefully attempted to skirt disclosure under the FOIA").

26. Michael D. Pepson & Daniel Z. Epstein, *Gmail.gov: When Politics Gets Personal, Does the Public Have a Right to Know?*, Engage: J. Federalist Soc'y Prac. Groups, July 2012, at 4, 7.

27. McLeod v. Parnell, 286 P.3d 509, 515 (Alaska 2012) ("[U]sing private email accounts is no more an obstruction of access to public records than communicating through paper letters."); Griffis v. Pina Cnty., 156 P.3d 418, 421 (Ariz. 2007); Bradford v. Dir., Emp't Sec. Dep't, 128 S.W.3d 20, 27–28 (Ark. Ct. App. 2003) ("Emails transmitted between Bradford and the governor that involved the public's business are subject to public access under the Freedom of Information Act, whether transmitted to private email addresses through private internet providers or whether sent to official government email addresses over means under the control of the State's Division of Information Services."); City of Champaign v. Madigan, 992 N.E.2d 629 (Ill. App. Ct. 2013) (applying state's open meetings law); Matter of Smith v. N.Y. State Office of the Attorney Gen., No. 3670-08, NYLJ 1202555064972, at *1 (N.Y. Sup. Ct. Apr. 30, 2012) ("[T]he OAG has both the responsibility and the obligation to gain access to the private e-mail account of former Attorney General Spitzer to determine whether the documents contained therein should be disclosed to petitioner in accordance with its FOIL request."); State *ex rel.* Glasgow v. Jones, 894 N.E.2d 686, 691 (Ohio 2008) ("[Representative] Jones concedes that e-mail messages created or received by her in her capacity as state representative . . . constitute records subject to disclosure . . . regardless of whether it was her public or her private e-mail account that received or sent the e-mail messages."); Mollick v. Twp. of Worcester, 32 A.3d 859, 872–873 (Pa. Commw. Ct. 2011) ("[A]ny emails that meet the definition of 'record' under the RTKL, even if they are stored on the Supervisors' personal computers or in their personal email accounts, would be records of the Township."); Burton v. Mann, 74 Va. Cir. 471 (2008) ("[T]he e-mail correspondence sought in this case indicates the use of both public and private databases, the status of which is not determinative of the issue of disclosure."); O'Neill v. City of Shoreline, 240 P.3d 1149, 1155 (Wash. 2010) (ordering city to search deputy mayor's home computer for e-mail records after concluding that "[i]f government employees could circumvent the [Public Records Act] by using their home computers for government business, the PRA could be drastically undermined").

28. D.C. Code §§ 2-531 *et seq.*

29. Vining v. Dist. of Columbia, No. 2013CA8189B (D.C. Super. Ct. July 9, 2014).

30. Pers. Use of Elec. Equip., AGO File No. 661-08-0388 (Alaska Att'y Gen. Aug. 21, 2008); Pub. Access Op. No. 11-006 (Ill. Att'y Gen. Nov. 15, 2011); Open Meetings Act—Pub. Info. Act—Status of Elec. Mail, 81 Md. Op. Att'y Gen. 140, 144–45 (May. 22, 1996) ("[E]-mail messages among members of the Commission pertaining to Commission business would be public records, albeit housed only in the home computers of the members"); N.M. Att'y Gen. Letter (Feb. 7, 2013) ("If email is used to conduct public business, the email is a public record, without regard to whether the email is created or maintained on a public or private email account."); N.D. Op. Att'y Gen. No. 2008-O-15 (July 1, 2008); N.D. Op. Att'y Gen. No. 2008-O-07 (Mar. 2008); N.D. Op. Att'y Gen. No. 98-O-05 (Mar. 3, 1998); Okla. Op. Att'y Gen. No. 09-12 (May 13, 2009); Tex. Op. Att'y Gen. No. ORD-1790 (2001); Letter Op. (Wis. Att'y Gen. Sept. 25, 2006).

31. Tex. Gov't Code Ann. §§ 552.001–.353.

32. No. 13-12-00535-CV, 2014 WL 2708424 (Tex. App. June 13, 2014).

33. *Id.* at *6

34. *Id.* at *6 n.4.

35. *Id.* at *8.

36. *Id.* at *9 (emphasis added).

37. *Id.* at *12.

38. Tex. Op. Att'y Gen. No. OR2012-19216 (Nov. 29, 2012). Although not applicable to the *Allala* case, in 2013 Texas amended its records law to declare that "public information" includes any documents created by a governmental officer or employee acting in an official capacity as long as the "information pertains to official business of the governmental body." Tex. Gov't Code Ann. § 552.002.

39. Tex. Gov't Code Ann. § 552.002(a) (emphasis added).

40. Complaint for Declaratory and Injunctive Relief at 4, Smith v. City of San Jose, No. 109CV150427 (Cal. Super. Ct. Aug. 21, 2009).

41. *Id.* at 5.

42. *See* Cal. Gov't Code § 6252(a).

43. City of San Jose v. Superior Court, 169 Cal. Rptr. 3d 840, 850 (Ct. App. 2014).

44. Cal. Const. art. 1, § 3(b)(1) (emphasis added).

45. City of San Jose v. Superior Court, 173 Cal. Rptr. 3d 46 (2014).

46. *See, e.g.*, Rinsley v. Brandt, 446 F. Supp. 850, 857–58 (D. Kan. 1977) ("A public official has no right of privacy as to the manner in which he conducts himself in office."); Rawlins v. Hutchinson Publ'g Co., 543 P.2d 988, 993 (Kan. 1975) (same); Citizens to Recall Mayor James Whitlock v. Whitlock, 844 P.2d 74, 77–78 (Mont. 1992) (rejecting as "unreasonable as a matter of law" a public officer holder's expectation of privacy "in performance of his public duties").

47. *See, e.g.*, Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977) (holding that public official enjoys a right of privacy only with respect to government-held information concerning "matters of personal life *unrelated to any acts done by them in their public capacity*" (emphasis added)); Denver Publ'g Co. v. Bd. of Cnty. Comm'rs of Arapahoe Cnty., Colo., 121 P.3d 190 (Colo. 2005) (holding that any portions of text messages exchanged between two government employees that discussed governmental business were public records and were required to be disclosed; the portions of such messages that contained only graphic, sexually explicit statements did not reflect official conduct and were redacted as "private").

48. *See* Kevin Duggan, *Public Access to Council Email Gets Easier*, Coloradoan, Jul. 26, 2014 (reporting that the City of Fort Collins, Colorado, has posted all nonprivileged e-mails of city councilors online, where they remain available for 90 days and then are deleted, consistent with city policy); Mary Ellen Klas, *Judge Orders Fla. Gov. Rick Scott to Stop Fighting Request for Records*, Miami Herald, Sept. 9, 2014 (reporting that Florida Governor Rick Scott's '"code of conduct' states that employees should not use personal email accounts 'unless such use is necessary upon a reasonable evaluation of the circumstances at hand' and then must forward the public record to his or her state account").

49. *See, e.g.*, Steve Terrell, *Governor Orders Staff to End Use of Private Email for Work Matters*, New Mexican, June 18, 2012 ("After a week of taking heat following the disclosure that Gov. Susana Martinez and top officials in her administration used personal emails to conduct state business, on Monday she ordered all state employees in agencies under her authority to use official state email for state business.").

50. *See, e.g.*, Freedom of Info. Act Complaint against Wilmington Hous. Auth., Del. Op. Att'y Gen. No. 06-ID23, 2006 WL 3663142 (Nov. 27, 2006) (concluding that "the Authority did not violate the . . . FOIA because any of [the executive director's] e-mails that might have been responsive to your request no longer exist").

51. *See, e.g.*, Edenburn v. N.M. Dep't of Health, 299 P.3d 424, 427 (N.M. Ct. App. 2012) (noting that the state's records preservation statute and its right to inspect public records act are distinct, and serve different purposes, so the former does not affect decisions under the latter).

52. The Council of State Archivists' website includes a compilation of all 50 states' public records preservation statutes: http://www.statearchivists.org/arc/states/res_stat.htm.

53. *See, e.g.*, Pam Zubeck, *Ain't No Sunshine*, Colo. Springs Indep., July 2, 2014, http://www.csindy.com/coloradosprings/despite-laws-that-require-transparency-city-government-keeps-us-in-the-dark/Content?oid=2900323.

54. Rachel Bade, *Archivist: IRS Did Not Follow Law on Lost Emails*, Politico (June 24, 2014), http://www.politico.com/story/2014/06/irs-lost-emails-archivist-108242.html. Under the Federal Records Act (44 U.S.C. §§ 2905(a), 3106) and its implementing regulations (36 C.F.R. pt. 1230), when an agency becomes aware of an incident of unauthorized destruction, it must report the incident to the Office of the Chief Records Officer for the U.S. government.

55. *See* 33 U.S.C. §§ 3101–07; 36 C.F.R. §§ 1224.10, 1236.20(b)(6).

56. Lisa Rein, *U.S. Chief Records Officer Details Federal Email Record-Keeping Programs*, Wash. Post, June 16, 2013, http://www.washingtonpost.com/politics/us-chief-records-officer-details-federal-e-mail-record-keeping-programs/2013/06/16/a6995e92-d470-11e2-a73e-826d299ff459_story.html.

57. *Id.* The Managing Government Records Directive is available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf.

58. *See* Nat'l Archives, NARA Bulletin 2013-02, Guidance on a New Approach to Managing Email Records (Aug. 29, 2013), *available at* http://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

59. *See* Nat'l Archives, NARA Bulletin 2014-06, Guidance on Managing Email (Sept. 15, 2014), *available at* http://www.archives.gov/records-mgmt/bulletins/2014/2014-06.html (stating that "[c]apstone officials will generally be the top-level senior officials of an agency, but may also be other key decision makers at lower levels of the agency").

60. *See, e.g.*, Valencia-Lucena v. U.S. Coast Guard, 180 F.3d 321, 328 (D.C. Cir. 1999) (finding agency's search inadequate where a particular responsive record was missing and agency failed to contact other personnel where "there is a close nexus . . . between the person and the particular record"); FLP Grp., Inc. v. IRS, 698 F. Supp. 2d 66, 78–80 (D.D.C. 2010) (applying FOIA and holding that if known responsive documents have been destroyed, the agency is obligated to search the electronic and paper files of other personnel who are "*likely to have copies of the destroyed materials*," including *former* employees (emphasis added)); State *ex rel.* Toledo Blade Co. v. Seneca Cnty. Bd. of Comm'rs, 899 N.E.2d 961, 970 (Ohio 2008) (ordering government entity to bear the cost of forensic data recovery to attempt to restore e-mails that had been deleted in violation of published records retention schedule).

61. *See* John Ferrugia & Sandra Barry, *Poudre School District Destroys Records to Deny Special Needs Family's Access*, KMGH-TV (Mar. 5, 2014), http://www.thedenverchannel.com/news/call7-investigators/poudre-school-district-destroys-records-to-deny-special-needs-familys-access.

62. David Damron, *Orange Leaders Settle "Textgate," Pay $90,000*, Orlando Sentinel, Jan. 13, 2014, http://articles.orlandosentinel.com/2014-01-13/news/os-textgate-civil-lawsuit-settlement-20140113_1_orange-leaders-former-commissioner-john-martinez-citizens-group.

63. *See* Jacob Parsley, *Florida Judge Grants $750,000 Award for Attorneys' Fees in Open Government Suit*, Silha Center Bull. (Jan. 5, 2010), http://www.silha.umn.edu/news/fall2009.php?entry=211905.

64. *See supra* note 52.

65. Abello, *supra* note 11, at 4.

66. Dismukes v. Dep't of the Interior, 603 F. Supp. 760 (D.D.C. 1984).

67. *Id.*

68. *See infra* note 86.

69. DeLorme Publ'g Co. v. NOAA, 907 F. Supp. 10, 11–13 (D. Me. 1995) ("An agency's FOIA duty is to disclose records, and records are formatted information. No one would argue that an agency could refuse to disclose a pie chart or graph, for example, merely because the same 'content' is available in statistical tables.").

70. 5 U.S.C. § 552(a)(3)(B).

71. Dep't of Justice, Office of Info. Policy, FOIA Update, Vol. XVII, No. 4 (1996), *available at* http://www.justice.gov/oip/blog/foia-update-congress-enacts-foia-amendments; *see also* 28 C.F.R. § 16.11(b)(3) ("Components shall honor a requester's specified preference of form or format of disclosure if the record is readily reproducible with reasonable efforts in the requested form or format by the office responding to the request.").

72. 5 U.S.C. § 552(a)(3)(B).

73. 330 F.3d 1191, 1197 (9th Cir. 2003) ("In evaluating reproducibility, the agency should employ a standard of reasonableness that is benchmarked against the agency's 'normal business as usual approach' with respect to reproducing data in the ordinary course of the agency's business."); *see also* Reporters Comm. for Freedom of the Press, *Record Formats*, *in* Federal FOIA Appeals Guide (2012), *available at* http://www.rcfp.org/federal-foia-appeals-guide/record-format-issues/record-formats.

74. *See, e.g.*, Ark. Code Ann. § 25-19-105(d)(2)(B); Cal. Gov't Code § 6253.9(a); D.C. Code § 2-532(a-1); 5 Ill. Comp. Stat. 140/6(a); Ind. Code § 5-14-3-3(d); Minn. Stat. § 13.03(3)(e); Miss. Code Ann. § 25-61-10(2); N.J. Stat. Ann. § 47:1A-5(d); N.Y. Pub. Off. Law § 87; Ohio Rev. Code Ann. § 149.43(B)(6); Or. Rev. Stat. § 192.440(3); 65 Pa. Stat. Ann. § 67.701(a); Tex. Gov't Code Ann. § 552.228(b); Vt. Stat. Ann. tit. 1, § 316(i); W. Va. Code § 29B-1-3(3); Wis. Stat. § 19.36(4).

75. Miss. Code Ann. § 25-61-10(2); *see also* Ark. Code Ann. § 25-19-105(d)(2)(B) (providing that a citizen "may request a copy of a public record in any medium in which the record is readily available or *in any format to which it is readily convertible with the custodian's existing software*" (emphasis added)); 5 Ill. Comp. Stat. 140/6(a) ("When a person requests a copy of a record maintained in an electronic format, the public body shall furnish it in the electronic format specified by the requester, if feasible. If it is not feasible to furnish the public records in the specified electronic format, then the public body shall furnish it *in the format in which it is maintained by the public body . . . . " (emphasis added)).*

76. *See, e.g.*, Prall v. N.Y. City Dep't of Corrections, 971 N.Y.S.2d 821 (Sup. Ct. 2013) (holding that NYC DOC did not violate FOIL when it provided inmate arrest records in PDF format rather than in native format as requested because disclosing original format would also have required disclosure of metadata containing confidential information).

77. *See, e.g.*, Menge v. City of Manchester, 311 A.2d 116 (N.H. 1973) (holding that expense and labor involved in abstracting information from other sources far outweighed ease and minimal cost of tape production).

78. *See, e.g.*, Sample v. Bureau of Prisons, 466 F.3d 1086 (D.C. Cir. 2006) (holding that under FOIA, Bureau of Prisons was obligated to provide record in electronic form to inmate, as requested); Minn. Med. Ass'n v. State, 274 N.W.2d 84 (Minn. 1978) (holding that state data privacy act placed no restriction on the form in which records could be made available other than that they be easily accessible for convenient use); Brownstone Publishers, Inc. v. N.Y. City Dep't of Bldgs., 560 N.Y.S.2d 642, 643 (App. Div. 1990) ("[I]t is clear that both the statute and its underlying policy require that the DOB comply with Brownstone's reasonable request to have the information, presently maintained in computer language, transferred onto computer tapes."); *see also* Blaylock v. Staley, 732 S.W.2d 152 (Ark. 1987); Szikszay v. Buelow, 436 N.Y.S.2d 558 (Sup. Ct. 1981).

79. *See, e.g.*, Laroche v. SEC, No. C 05-4760 CW, 2006 WL 2868972, at *3 (N.D. Cal. Oct. 6, 2006) (finding that SEC could not readily reproduce in electronic format data not available electronically when "the only other way to create a searchable electronic file [besides scanning paper copies] would be for an SEC staff member to cut and paste each cell of data from the individual electronic records into another document for Plaintiff."), *aff'd*, 289 F. App'x 231 (9th Cir. 2008); Citizens for Responsibility & Ethics in Wash. v. U.S. Dep't of Educ., 905 F. Supp. 2d 161, 171 (D.D.C. 2012) (holding that agency had no responsibility to provide electronic format of responsive e-mails because "DoEd's email records are not 'readily reproducible' in electronic format, and the DoEd email retention system 'will not display or print' the BCC field 'for any retrieved email.'").

80. *See, e.g.*, AFSCME v. Cook Cnty., 555 N.E.2d 361 (Ill. 1990); Farrell v. City of Detroit, 530 N.W.2d 105, 108–09 (Mich. Ct. App. 1995) (observing that Michigan's statute "gives a person the right to 'inspect, copy, or receive copies of a *public record*,' not merely to obtain the 'information' contained in a public record in any form in which the public body sees fit to release it"); *Brownstone Publishers*, 550 N.Y.S.2d 564; *cf.* Higg-A-Rella, Inc. v. Cnty. of Essex, 660 A.2d 1163, 1170 (N.J. 1995) (requiring disclosure of tax list records in computerized form under common-law balancing test). *But see* Wells v. Wharton, No. W2005-00695-COA-R3-CV, 2005 WL 3309651, at *9 (Tenn. Ct. App. 2005) (rejecting these cases, and concluding that "[a]llowing a custodian of records to choose the manner in which he or she presents public records to citizens is not unreasonable so long as that manner does not distort the record or inhibit access to that record").

81. State *ex rel.* Margolius v. City of Cleveland, 584 N.E.2d 665, 669 (Ohio 1992) (emphasis added) (citation omitted).

82. A helpful description of various programs' available metadata, and how to access it, is available at http://canons.sog.unc.edu//wp-content/uploads/2010/03/document_metadata-2.pdf.

83. Reporters Comm. for Freedom of the Press, *Access to File "Metadata," in* Federal FOIA Appeals Guide, *supra* note 73. "Metadata is quite simply data about data, or hidden statistical information about a document that is generated by a software program." O'Neill v. City of Shoreline, 240 P.3d 1149, 1152 (Wash. 2010) (quoting Jembaa Cole, *When*

Invisible Electronic Ink Leaves Red Faces: Tactical, Legal and Ethical Consequences of the Failure to Remove Metadata, 1 SHIDLER J.L. COM. & TECH. 8, ¶ 7 (Feb. 2, 2005)).

84. *See* Kozinets, *supra* note 13.

85. *Id.*

86. Under the Electronic FOIA Amendments of 1996, a record is defined as "any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format." 5 U.S.C. § 552(f)(2)(A).

87. Nat'l Day Laborer Org. Network v. U.S. Immigration & Customs Enforcement Agency, No. 10 Civ. 3488 (S.D.N.Y. Feb. 7, 2011).

88. Nat'l Day Laborer Org. Network v. U.S. Immigration & Customs Enforcement Agency, 811 F. Supp. 2d 713 (S.D.N.Y. 2011).

89. *See*, *e.g.*, Lake v. City of Phoenix, 218 P.3d 1004, 1007–08 (Ariz. 2009) ("The metadata in an electronic document is part of the underlying document; it does not stand on its own. When a public officer uses a computer to make a public record, the metadata forms part of the document as much as the words on the page. . . . We accordingly hold that when a public entity maintains a public record in an electronic format, the electronic version of the record, including any embedded metadata, is subject to disclosure under our public records law."); O'Neill v. City of Shoreline, 240 P.3d 1149, 1153–54 (Wash. 2010) ("Metadata may contain information that relates to the conduct of government and is important for the public to know. . . . [A] n electronic version of a record, including its embedded metadata, is a public record subject to disclosure."); *see also* Irwin v. Onondaga Cnty. Res. Recovery Agency, 895 N.Y.S.2d 262 (App. Div. 2010); Hearst Corp. v. State, 882 N.Y.S.2d 862 (Sup. Ct. 2009).

90. In September 2014, two citizen advocacy groups filed suit against Orlando, Florida, Mayor Teresa Jacobs seeking access to the inventory and contents of records stored in Dropbox by the mayor and her staff. *See* Martin E. Comas, *Group Sues Jacobs, Accuses Her of Violating Records Laws*, ORLANDO SENTINEL, Sept. 26, 2014, http://www.orlandosentinel.com/news/breaking-news/os-teresa-jacobs-dropbox-lawsuit-20140926-story.html. A copy of the lawsuit is available at http://wmfeimages.s3.amazonaws.com/wp-content/uploads/2014/09/Complaint.pdf.