



# Communications Lawyer

Publication of the Forum  
on Communications Law  
American Bar Association  
Volume 27, Number 2, July 2010

THE JOURNAL OF MEDIA, INFORMATION, AND COMMUNICATIONS LAW



## In this issue

### COVER STORY

#### Getting the Complete Story

Most states have yet to address directly whether existing definitions of *public records* encompass metadata, potentially leading to attempts to subterfuge open government laws.

#### Sex, Violence, and Videogames..2

The U.S. Supreme Court recently granted certiorari to a Ninth Circuit decision that struck down a California law prohibiting the sale of “violent video games” to minors. Previously declining to act *in loco parentis*, the Court is going to take another look at sex, violence, and minors.

#### Keeping Your Text Messages

#### Out of Court .....4

The upsurge in text messaging by traditional media organizations and others has triggered a wave of class action suits, alleging violations of everything from the Telephone Consumer Protection Act to state consumer protection laws.

#### Courts in the Former

#### Soviet Union.....16

The author reports on the similarities (and differences) of the Ukrainian judicial system twenty years after the country declared its independence from the USSR and six years after the Orange Revolution.

#### Blogging at the Big Game..... 18

The author looks at the First Amendment implications of attempts by sports organizations to restrict reporters and fans who want to send blogs, Tweets, and text messages during The Game of the Century.

#### Courtside.....22

In one of its most controversial decisions this Term, the Court struck down a federal law that makes it a crime to sell videos or photos of animals being illegally killed or tortured.

## Access to Metadata in Public Records: Ensuring Open Government in the Information Age

PETER S. KOZINETS

If the Declaration of Independence were written today, it likely would be composed on a computer, with the drafters’ words stored in an electronic file as a series of ones and zeros. That file likely would contain a host of data about the document, including information about its author and editors; dates created, accessed, edited, e-mailed, or printed; file name, size, and type; file storage or location; and possibly revisions or comments, especially if the drafters used “track changes.” If the drafters included a chart describing, for instance, the growth rate of Colonial taxes from 1746–1776, tables of data and formulae also might be stored in the document’s file. These categories of information are examples of metadata, i.e., data about data, that generally are not visible when a document is printed or converted to a static image, like a PDF or TIFF file.<sup>1</sup> Rather, most metadata can only be seen when viewing an electronic record in its “native format,” i.e., by opening it in the software application in which it was created (its native application).

While the original Declaration of Independence had its own types of metadata (accessible through the study of ink, paper, handwriting, and other sources), nearly all information generated by government and nongovernment sources alike is now created electronically. As a result, access to digital documents, the modern paper trail, has become essential to furthering the search for truth in both the courtroom and the newsroom.<sup>2</sup> Nevertheless, public agencies are often reluctant to provide public access to government records in

electronic format. One consequence is that requestors are frequently denied access to metadata.

Yet protecting public access to electronic records, including metadata, is essential to safeguarding the public’s ability to open government conduct to public scrutiny. Metadata can verify the authenticity and integrity of a public record, reveal what officials knew about critical actions or decisions and when they knew it, and render intelligible vast storehouses of government data that would otherwise be useless when separated from their metadata. Although few courts have addressed whether metadata is part of a public record, the Arizona Supreme Court (the highest state appellate court to have considered the issue thus far) held last year in *Lake v. City of Phoenix* that when a public entity maintains a public record in electronic format, that electronic record, including its embedded metadata, qualifies as a public record and is subject to a strong presumption of access and disclosure under Arizona’s public records law.<sup>3</sup>

Other courts and legislatures are now considering whether metadata falls within the scope of state open records laws. This article reviews the legal landscape

*Peter S. Kozinets (pkozinets@steptoe.com) practices media and constitutional law, and commercial and intellectual property litigation, in the Phoenix office of Steptoe & Johnson LLP. He thanks Jamaar Williams, a student at the Arizona State University Sandra Day O’Connor College of Law, for his research assistance.*

regarding public access to metadata, and proposes a model for resolving disputes about access that strikes the proper balance between the public's right to know and countervailing concerns. The article first explains metadata's significance in furthering the interests of open government and an informed citizenry. It then discusses federal and state cases that have grappled with issues relating to public access to metadata. Finally, it proposes a model for addressing requests for such access.

Under the proposed model, the native version of an electronic public record, including metadata, should be furnished by public entities upon request, absent a showing that is supported by specific facts, that release of the electronic record will cause substantial harm to recognized interests of privacy, confidentiality, or other compelling government interests. Objections relating to the burden or scope of such requests should be handled largely as they would in civil discovery practice, through good faith discussions aimed at tailoring the request to specific documents or categories of documents and, if necessary, through application to the courts. Simply put, metadata is vital to ensuring continued and meaningful public access to records of government conduct, and it should be presumptively available to the public when requested.

### Why Metadata Matters

For several reasons, the metadata associated with electronic public records provides an indispensable mechanism for monitoring government conduct in the information age. First, metadata can be vital to demonstrating the authenticity, integrity, and admissibility of electronic documents and to revealing possible official misconduct. The Arizona Supreme Court's decision in *Lake v. City of Phoenix* arose from just such a challenge to the authenticity of a public record, and the court found that public access to the metadata of a police supervisor's notes could be highly relevant to assessing claims of government malfeasance, misfeasance, or nonfeasance involving alleged backdating of the notes.<sup>4</sup>

For paper documents, a variety of forensic tests can be used to assess the authenticity of a paper record, including study of the ink, paper, handwriting, or fonts.<sup>5</sup> In the electronic world, and

in lieu of paper-based indicators of authenticity, metadata contains dates created and modified, author and location information, and similar "distinctive characteristic[s] . . . that can be used to authenticate" electronic evidence under Federal Rule of Evidence 901(b)(4).<sup>6</sup> Moreover, metadata is widely recognized as discoverable under Federal Rule of Civil Procedure 34(a).<sup>7</sup>

Metadata also can reveal the influence of special interests on official conduct. Illustratively, in 2004, California's then attorney general, Bill Lockyer, circulated a letter castigating peer-to-peer file-sharing software as "a dangerous product." Examination of the properties section of the document showed that one "stevensonv" had written it. Vans Stevenson, a senior vice president of the Motion Picture Association of America, which vigorously opposed peer file sharing, later said that he had provided some input regarding the letter but had not written it.<sup>8</sup>

Second, metadata is essential to making electronic spreadsheets and databases intelligible and useful. As one federal court has recognized, "the more interactive the application, the more important metadata is to understanding the application's output."<sup>9</sup> For many word processing documents, metadata may not be needed to understand the document's contents. "At the other end of the spectrum," however, "is a database application where the database is a completely undifferentiated mass of data," and "metadata is the key to showing the relationships between the data."<sup>10</sup> Indeed, native format versions of Microsoft Excel spreadsheets often display far more columns of data than printed versions, include additional spreadsheets located under different tabs, and display formulas, comments, and other information that are otherwise invisible when viewing an Excel printout. More sophisticated relational databases contain file layouts, tables, data dictionaries, and other metadata that organize the data and are essential to making the database functional and intelligible. For such documents, allowing a public entity to curtail access to the metadata effectively blocks public access to the record itself.<sup>11</sup>

News organizations and journalists have used such metadata to shed important light on government activity. For example, *The Miami Herald* published

a Pulitzer Prize award-winning analysis of data relating to the damage caused by Hurricane Andrew in 1992. The authors obtained public record data involving 60,000 official damage inspection reports and merged them by address with other county data, including property tax rolls and building and zoning databases. Using this analysis, *The Herald* then produced a map showing how 420 subdivisions had weathered the storm. It revealed that the hardest-hit neighborhoods contained a disproportionate number of homes built after 1980, when officials began allowing poorer construction techniques.<sup>12</sup> Similarly, in 2004, *The New York Times* conducted a computer analysis of tens of thousands of federal accident reports, leading to a seven-part series about lax oversight of railroad crossing safety.<sup>13</sup>

Third, metadata is essential to opening government conduct to public review because future public record archives might not function without it. The U.S. Library of Congress's National Digital Information and Infrastructure Preservation Program is funding the Persistent Digital Archives and Library System (PeDALS), a multistate effort, led by the Arizona State Library, Archives and Public Records, to design a digital archiving system for electronic public records.<sup>14</sup> The PeDALS system relies on the use of metadata to ensure the ongoing preservation of and future access to electronic public documents.<sup>15</sup>

### Federal Approach: "Regardless of Physical Form or Characteristics"

Federal law has long recognized the critical importance of electronic agency records. Indeed, two key federal definitions of *records* have strongly influenced state statutes and court decisions involving public access to electronic documents. First, the Federal Records Act (FRA), which governs the preservation of federal agency records, defines a *record* as

all books, papers, maps, photographs, machine readable materials, or other documentary materials, *regardless of physical form or characteristics*, made or received by any agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency . . . as

evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.<sup>16</sup>

The FRA requires an agency to obtain approval from the National Archivist before disposing of any record.<sup>17</sup>

Second, the federal Freedom of Information Act (FOIA) contains a

## Federal law has long recognized the critical importance of electronic agency records.

similar definition of record. In addressing the increasing governmental use of technology to keep and maintain records, Congress passed the Electronic Freedom of Information Act Amendments of 1996, which define a *record* 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.”<sup>18</sup> The amendments also require federal agencies to produce records in any requested format, if readily reproducible in that format.<sup>19</sup> Upon signing the amendments into law, President Clinton stated that the legislation “brings FOIA into the information and electronic age by clarifying that it applies to records maintained in electronic format.”<sup>20</sup>

The majority of states have followed the federal government’s lead and have defined public records broadly to include electronic records and data regardless of their form. Thirty-three states have specific references in their public records statutes to “electronic or computer-based information”<sup>21</sup> or have descriptions similar to the FRA’s “regardless of physical form or characteristics” language.<sup>22</sup> The Reporters Committee for Freedom of the Press has found that “[a] growing number of states now include electronic data in their definitions of what constitutes a public record,” and that all fifty states and the District of Columbia “include

[ ] computerized records in their definition of public records, either specifically in the statutory language or through judicial interpretation.”<sup>23</sup>

### Roots of Public Access to Metadata

Construing language of the FRA that has been mirrored in many state statutes, the D.C. Circuit in *Armstrong v. Executive Office of the President*<sup>24</sup> laid the foundation for many of today’s decisions recognizing the public’s right of access to metadata in public records. *Armstrong* was filed in the aftermath of the Iran-Contra scandal of the mid-1980s, in which two White House National Security Council officials, Oliver North and John Poindexter, famously corresponded with each other via PROFS, one of the first e-mail systems in government service. Shortly before public disclosure of their activities, North and Poindexter deleted thousands of e-mails that they had exchanged regarding a scheme to sell arms to Iran to obtain the release of hostages and to use the profits to fund a civil war in Nicaragua.<sup>25</sup>

*Armstrong* involved a legal challenge to the record preservation practices of the Executive Office of the President, the National Security Council, and the U.S. Archivist under the Federal Records Act. The defendants had instructed employees to print and save a paper version of any electronic communication that fell within the statute’s definition of a *record*, rather than saving the original electronic versions. The court held that this instruction violated the FRA, observing that the hardcopy printouts “may omit fundamental pieces of information which are an integral part of the original electronic records, such as the identity of the sender and/or recipient and the time of receipt,”<sup>26</sup> and “[d]irectories, distribution lists, acknowledgements of receipts and similar materials.”<sup>27</sup> “Without this ‘non-screen’ information,” the court wrote, a later reader would be deprived of “such basic facts as who sent or received a particular message or when it was received,”<sup>28</sup> and “essential transmittal information relevant to a fuller understanding of the context and import of the electronic communication [would] simply vanish.”<sup>29</sup>

Rejecting the government’s approach of keeping paper printouts but discarding electronic versions, the court

found that the paper and electronic documents are different records under the FRA “unless the paper versions include all significant material contained in the electronic records.” Otherwise, “the two documents cannot accurately be termed ‘copies’—identical twins—but are, at most, ‘kissing cousins.’”<sup>30</sup>

The court wrote that its view “amounts to far more than judicial nitpicking”:

Texts alone may be of quite limited utility to researchers and investigators studying the formulation and dissemination of significant policy initiatives at the highest reaches of our government. . . . [T]he practice of retaining only the amputated paper print-outs is flatly inconsistent with Congress’ evident concern with preserving a complete record of government activity for historical and other uses.<sup>31</sup>

*Armstrong*’s rejection of the notion that an electronic record can be preserved merely by printing part of its contents presaged the reasoning of *Lake* and other decisions and continues to inform judicial analysis of how metadata can shed light on the conduct of government.

### Arizona: The Public’s Right to the “Real Record”

In *Lake v. City of Phoenix*,<sup>32</sup> the Arizona Supreme Court rejected a lower court decision that would have categorically excluded metadata from the scope of the Arizona public records act, and ruled that electronic records, including their metadata, fall within Arizona’s definition of a public record. The court held that “if a public entity maintains a public record in an electronic format, then the electronic version, including any embedded metadata, is subject to disclosure” under Arizona Revised Statutes § 39-121 *et seq.*<sup>33</sup> The court applied the reasoning of *Armstrong* to statutory language similar to that considered by the D.C. Circuit and endorsed a broad right of public access to electronic records in their native format.

Lake, a Phoenix police officer, had filed a lawsuit alleging employment discrimination by the City of Phoenix. He claimed that his supervisor, Lt. Robert Conrad, retaliated against him

after he had reported serious police misconduct, ultimately causing his demotion. After receiving hardcopies of Lt. Conrad's notes pursuant to a public records request, Lake suspected that the notes had been backdated to a date that preceded his demotion. He then requested "'metadata' or specific file information contained inside . . . [the notes] file," including "the TRUE creation date, the access date, the access dates for each time it was accessed, including who accessed the file as well as print dates etc."<sup>34</sup>

The city asserted that the requested metadata was not part of the definition of a *public record* and denied Lake's request. Lake challenged the city's decision by filing a special action (an expedited civil action, similar to a mandamus proceeding) in Arizona Superior Court. He alleged that the city was "intentionally and purposely delaying the production of certain public records" until they could be destroyed under records retention laws.<sup>35</sup> He also argued that "[w]ithout the metadata, the public has no way of authenticating Lt. Conrad's notes to monitor the machinations of government," and that the metadata is necessary to determine if the government was "acting in a lawful and honest manner."<sup>36</sup>

Lake lost in the trial court and the Arizona Court of Appeals, which ruled two-to-one that metadata is not covered by the state's Public Records Law.<sup>37</sup> The majority reasoned that the terms *record* and *public record* are not coextensive under Arizona law, and that the vast quantity of electronic records created on a daily basis, many with little or no volitional act of public employees, do not necessarily fall within the scope of the Arizona Public Records Law:

[W]e must also recognize the practical reality that each time a government employee logs on or off of a computer, clicks a computer mouse, pushes the characters on a keyboard, sends an e-mail, prints a document, uses the internet, talks on a phone, or enters a building with keycard access, a "record" has arguably been generated.<sup>38</sup>

The majority preferred to leave it to the legislature to determine whether such records are subject to public disclosure.<sup>39</sup>

The dissenting judge, Judge Norris, strongly objected to the majority's focus on whether metadata, viewed in isolation, constitutes a public record. She wrote that metadata is not an "electronic orphan," but rather is an integral part of an electronic document.<sup>40</sup> Because the city never asserted that the requested notes were not public records, she concluded that "[w]hen . . . [an] electronically created document is a public record, then so too is its metadata."<sup>41</sup>

Following *Armstrong*, Judge Norris observed that part of an electronic document, i.e., its metadata, is lost when the document is printed on paper, and that the metadata "is as valuable as the text itself because this information can, as the majority correctly notes, 'identify and certify the scope, authenticity, and integrity of active or archival electronic information or records.'"<sup>42</sup> She wrote: "[A] person asking to inspect a public record is entitled to inspect the real record," and if the record was created in an electronic format, then the real record will consist of that document in its electronic form.<sup>43</sup>

The dissent concluded by tying access to metadata to the underlying purpose of the public records law, "to open government activity to public scrutiny."<sup>44</sup> Because metadata "contains information about who authored a document, when it was edited, and who would have accessed it," metadata "can be crucial to ensuring government transparency."<sup>45</sup> The electronic version of Lt. Conrad's notes identified "how and when the government acted" and could reveal whether a government official backdated a public record, possibly to cover up retaliation.<sup>46</sup> Because the electronic version "sheds light on how the government is conducting its business," the dissenting judge would have held that the document fell within the scope of the Arizona Public Records Law.<sup>47</sup>

The Arizona Supreme Court agreed with Judge Norris and vacated the court of appeals' metadata ruling. In a unanimous opinion, Arizona's highest court explained that although Arizona statutes do not define the term *public record*, in the wake of Watergate the state legislature amended the Public Records Law to require that

[a]ll officers and public bodies shall maintain all records reasonably necessary or appropriate to

maintain an accurate knowledge of their official activities and of any of their activities which are supported by funds from the state or any political subdivision thereof.

In 2000, the legislature further broadened the statute by inserting the phrase "including records as defined in [A.R.S.] § 41-1350" into the foregoing provision. Arizona Revised Statutes § 41-1350, in turn, mirrors the definition of record found in the FRA, and specifically refers to all government records "*regardless of physical form or characteristics . . . made or received by any governmental agency in pursuance of law or in connection with the transaction of public business. . . .*"<sup>48</sup>

The court recognized that these amendments "define[d] those matters to which the public right of inspection applies more broadly," and that all records required to be made, maintained, and preserved pursuant to these statutes are covered by the public's right of access and disclosure under the Arizona Public Records Law, "subject to the official's discretion to deny or restrict access where recognition of the interests of privacy, confidentiality, or the best interest of the state in carrying out its legitimate activities outweigh the general policy of open access."<sup>49</sup>

Applying these principles to metadata, the court found that the key issue "is not whether metadata considered alone is a public record," but "whether a 'public record' maintained in an electronic format includes not only the information normally visible upon printing the document but also any embedded metadata."<sup>50</sup> It concluded that "[t]he metadata in an electronic document is part of the underlying document; it does not stand on its own," and that "Arizona's public records law requires that the requestor be allowed to review a copy of the 'real record,'" which includes the metadata of a public record maintained in an electronic format.<sup>51</sup> Indeed, "[i]t would be illogical, and contrary to the policy of openness underlying the public records laws, to conclude that public entities can withhold information embedded in an electronic document, such as the date of creation, while they would be required to produce the same information if it were written manually on a paper public record."<sup>52</sup>

The city asserted that this result would create an “administrative nightmare” requiring officials to spend “countless hours” identifying metadata for release, but the court found the City’s fears overstated for several reasons.<sup>53</sup> First, electronic copying is generally easier and less costly than producing in paper format. Dragging and dropping files onto a portable electronic storage medium can be done in a matter of seconds, but photocopying the same information (or even printing it) can take hours or longer.<sup>54</sup>

Second, not every public records request will require disclosure of native files, and “[p]ublic entities may provide paper copies if the nature of the request precludes any need for the electronic version.”<sup>55</sup> Third, if a public entity finds a request unduly burdensome, it can ask the requestor to narrow the request, or object, deny access, and ultimately

have a court decide questions of burden. If the native files contain confidential, private, or other protected or privileged metadata, the agency can withhold information that is otherwise exempt from disclosure under the state’s public records law.<sup>56</sup>

In short, and like *Armstrong, Lake* recognized a broad presumptive right of access to the native format versions of public records, including metadata. In so doing, the court guaranteed that the public would not lose a vital source of information about the conduct of government that is contained within the government’s electronic files.

#### **Washington: Separating Metadata and Record**

In *O’Neill v. City of Shoreline*, the Washington Court of Appeals construed similar “regardless of physical form or characteristics” statutory

language and held that Washington’s broad definition of *public records* included an e-mail and its attached metadata.<sup>57</sup> At a public meeting of the Shoreline City Council, the deputy mayor stated that she had received an e-mail from “a Ms. Hettrick and a Ms. O’Neill” that contained serious allegations of improper influence by city council members over a zoning matter. O’Neill, who attended the meeting, immediately asked “to see that e-mail,” and the deputy mayor responded that she would be “happy to share” it. However, the deputy mayor had received the e-mail at home, and she deleted the e-mail’s top four lines before forwarding it to her work computer for disclosure to O’Neill.<sup>58</sup>

The header information consisted of the following:

**From:** Lisa Thwing



## WORK YOUR MEMBERSHIP

### WITH ABA MEMBER ADVANTAGE

To get the most from your ABA membership, put your ABA Member Advantage savings to good use. The ABA Member Advantage Program offers discounts on hundreds of products and services from more than a dozen companies. If you don’t use them, you won’t lose them—but you will lose out.

Visit the ABA Member Advantage website at [www.abanet.org/advantage](http://www.abanet.org/advantage) for a complete list of participating companies and the discounts they offer ABA members. The number continues to grow, so check back often for updates and additional opportunities.

**ABA** Member  
Advantage

tootrd@comcast.net

**Date:** Mon, 18 Sep 2006  
07:55:38-0700

**To:** Lisa Thwing  
tootrd@comcast.net

**Subject:** Current city council  
meeting being broadcast this week

**From:** Diane Hettrick  
dhettrick@earthlink.net

**Sent:** Thursday, September 14, 2006 11:40 PM

**Subject:** Current city council  
meeting being broadcast this week<sup>59</sup>

The e-mail stated, “Hi Folks, My dear friend, Beth O’Neill, has asked me to pass along information about our dysfunctional Shoreline City Council,” and then stated that city council members had been “playing favorites” in zoning decisions in favor of their political supporters.<sup>60</sup> The deputy mayor deleted the first four lines listing Thwing as the sender and recipient, ostensibly to protect Thwing “from potential public exposure.”<sup>61</sup>

The city denied several requests from O’Neill for the electronic version of the e-mail and other records, and O’Neill sued for access under the Washington Public Records Act (WPRa). After the trial court ruled against her, the appellate court reversed, remanded, and explicitly held that the electronic version of the e-mail, along with the requested metadata, is a public record under Washington law.

First, the court noted that in view of the WPRa’s purpose, “we liberally construe its disclosure provisions and narrowly construe its exemptions.”<sup>62</sup> Turning to the definition of *public record* under the Washington statute, the court then recognized that the WPRa specifies that a public record is “any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency *regardless of physical form or characteristics*.”<sup>63</sup> The court also recognized that the WPRa defines a *writing* as any “means of recording any form of communication . . . including, but not limited to, . . . magnetic or punched cards, discs, drums, diskettes, . . . and data compilations from which information may be obtained or translated.”<sup>64</sup> Based on these definitions,

the court concluded that the electronic version of the e-mail is a public record, i.e., a writing that relates to the conduct of government or the performance of a government function that the deputy mayor used by making it the subject of public comment at the city council meeting.<sup>65</sup>

The court then separately considered whether the metadata associated with the e-mail is also a public record and found that the metadata, “or some portion of it, falls within the broad definition of a writing.”<sup>66</sup> Specifically, the deleted metadata at issue, the first four lines of the e-mail header, “contains information that ‘relates to’ the conduct of government or the performance of a governmental function” because it showed “the e-mail addresses of persons who may have knowledge of alleged government improprieties in dealing with a zoning matter.”<sup>67</sup> The court directed the trial court to determine, on remand, whether other portions of the e-mail’s metadata fell within the scope of the WPRa.<sup>68</sup>

On April 28, 2009, the Washington Supreme Court granted the City of Shoreline’s petition for review,<sup>69</sup> and several briefs have been filed in the appeal, which remains pending as of June 2010.<sup>70</sup>

Although *O’Neill* ruled in favor of public access, the court’s reasoning drew an improbable distinction between the electronic version of the e-mail and its metadata. Once it held that the electronic version of the e-mail is a public record, the court could and should have found that metadata embedded in the e-mail is part and parcel of that public record.<sup>71</sup> Rather than take this view, however, the Washington court appears to have considered whether disclosure of specific portions of the metadata (e.g., the missing header information) would further the core purposes of the Washington Public Records Law.

While this approach appears more nuanced, it effectively shifts the burden of establishing the public’s right of access to the requestor, who presumably would have to articulate the public interest in access to each requested field of metadata without knowing what the fields actually contain. By requiring requestors to bear the burden of proving something that they might not know, this approach threatens to reverse the traditional presumption

in favor of public access to public records, and to foreclose public access to undisclosed metadata that could provide important insights into government conduct. A better approach would apply the traditional presumption in favor of public access to the entire electronic document, including metadata. Doing so would place the burden of proof on the proponent of closure, the public body or custodian who *has* the record, to demonstrate why the electronic document, or any part of it, should not be disclosed.

### New York: A Tentative Approach

One of New York’s intermediate appellate courts recently held that one category of metadata fell within the scope of a particular public records request, but declined to hold that metadata is subject to the New York Freedom of Information Law (FOIL)<sup>72</sup> in other contexts. In *Irwin v. Onondaga County Resource Recovery Agency*,<sup>73</sup> the petitioner filed suit under FOIL against the Onondaga County Resource Recovery Agency seeking access to all electronically stored photographs available for use in the agency’s publications and associated metadata. The agency provided numerous photographs, but Irwin claimed they were reduced in resolution and lacked metadata.

The state appellate court held that Irwin was entitled to the photographs and what it called “system metadata,” including “file names and extensions, sizes, creation dates and latest modifications dates.”<sup>74</sup> It recognized that “[r]ecords stored in an electronic format are subject to FOIL.”<sup>75</sup> FOIL defines a *record* as “any information kept, held, filed, produced or reproduced by, with or for an agency or the state legislature, *in any physical form whatsoever* including, but not limited to . . . computer tapes or discs. . . .”<sup>76</sup> The court then recognized that “‘system’ metadata, which is at its core the electronic equivalent of notes on a file folder indicating when the documents stored therein were created or filed, constitutes a ‘record’ subject to disclosure under FOIL.”<sup>77</sup> The court declined to address whether metadata “of any other nature,” such as metadata showing the history of proposed changes and revisions (“substantive metadata”) or spreadsheet formulas (“embedded metadata”), is subject to disclosure under FOIL.<sup>78</sup>

Although the *Irwin* court did not articulate any reasoning behind its differential treatment of system metadata and other forms of metadata, it may have been concerned that what it called substantive and embedded metadata would reveal more information than the type of system metadata (file name, size, creation date, etc.) it was prepared to disclose. Moreover, the facts of *Irwin*, which concerned a request for access to electronic files of digital photographs, did not lend themselves to analysis of those other categories of metadata. The *Irwin* court was “careful to note . . . that our decision is limited to the facts of this case in this evolving area of the law.”<sup>79</sup> Nevertheless, like *Lake* and *O’Neill*, *Irwin* held that the metadata sought by the requestor was covered by the state’s public records statute and

## Most states have defined public records broadly to include electronic records regardless of their form.

subject to public disclosure.

### Proprietary Information or Public Record?

Prior to *Irwin*, another New York court confronted metadata issues in *Hearst Corp. v. State of New York (Office of State Comptroller)*.<sup>80</sup> In that case, Hearst Corp., publisher of the *Albany Times Union*, and J. Robert Port, a *Times Union* investigative reporter, sued the state for access to certain data from New York state’s public employee payroll tables, including fourteen tables of information concerning positions and compensation, along with “related metadata, record layouts, and documentation.”<sup>81</sup> The state provided the names, office addresses, titles, and salaries for all public employees but refused to disclose the other requested categories of information, asserting that they constituted trade secrets or proprietary material of the state’s vendor, Oracle.<sup>82</sup> After examining an affidavit from Oracle, the Albany trial court found that

the metadata and record layouts met the definition of *trade secrets* and would cause competitive harm to Oracle if released.<sup>83</sup> Nevertheless, the court held that providing the requestors with data from the fourteen specified payroll tables would not breach Oracle’s rights, if the tables could be exported to an electronic spreadsheet that did not reveal Oracle’s proprietary layouts and electronic fields.<sup>84</sup> By so ruling, the court apparently attempted to provide the maximum amount of access possible, without comprising the asserted trade secrets of the state’s vendor. Nevertheless, the state’s objections to disclosure show that public entities might attempt to deny access to government databases that are created or maintained with the assistance of private vendors.

### Resolving Disputes: A Proposed Model

Any model for resolving disputes for access to metadata under state public records law should start with a broad presumption in favor of public access to public records, a presumption that states have applied historically to requests for access to public records kept in paper form. Such a presumption embodies and furthers the following core purposes of open records laws: (1) allowing members of the public to monitor the conduct of their officials and provide a check on government abuses, (2) fostering public trust and confidence in the legitimacy and integrity of government decisions by opening the conduct of government to public scrutiny, and (3) promoting democratic self-government and public participation.<sup>85</sup>

This starting presumption should apply to an electronic public record as a whole, including any embedded metadata, rather than to some parts of the record only. This properly places the burden of demonstrating why the record or any portion should not be released on the custodian, who has full access to the record and knows its contents. Reversing the presumption (even as to any part of a record) would require the requestor to explain why he or she needs the record, a difficult, if not impossible, task for someone who has not seen the withheld material and does not know what it contains. Reversing the presumption also would undermine the core purposes of public access described above, and would be fundamentally at odds with

the principle that members of the public have the right to inspect records of the government’s discharge of the public’s business without having to supply any special reason or explanation.

Moreover, the presumption should apply to the entire record because divorcing an electronic record from its metadata effectively cleaves one record into two. As recognized in *Armstrong* and *Lake*, without metadata, important governmental information about the history, origin, source, authenticity, and integrity of the record may vanish. Given (1) the history and purpose of state public records laws, (2) statutory language that refers to records kept in electronic format or subject to disclosure “regardless of physical form or characteristics,” and (3) the remedial purpose of and liberal construction afforded to open records laws, metadata *should* be considered part and parcel of the electronic record in which it is embedded.<sup>86</sup> Metadata might not be pertinent to every public records request, but it should be supplied when requested, absent a demonstrably good reason for closure.

In view of the strong presumption in favor of public access and disclosure, any objection to providing public access to any part of an electronic version of a requested record, including its metadata, should be substantiated with concrete facts, rather than vague, unsupported generalizations, showing how release would cause harm to a substantial countervailing interest. If objections are made, the parties should engage in a constructive dialogue regarding the scope of the request and the claimed burdens and harms of production. Such negotiations are often used to resolve requests for the production of metadata under the Federal Rules of Civil Procedure and can lead to more tailored requests for the metadata of specific documents or categories of documents.<sup>87</sup> If a requestor and a public body are unable to resolve their differences through negotiation, the matter could be submitted to a court under existing public records laws, which often call for *in camera* review.<sup>88</sup> Because this model safeguards access while allowing for orderly resolution of objections to disclosure, it should be adopted by courts and legislatures facing issues of public access to metadata.

### Conclusion

There is a surprising dearth of judicial opinions addressing the extent to which metadata falls within the definition of a *public record* under open records laws. With the exceptions of Arizona, Washington, and New York, most states have not yet explicitly addressed whether metadata is covered by existing definitions of public records. Nevertheless, public agencies should readily provide access to electronic versions of public records that include metadata. All or nearly all state statutory or common law definitions of *public records* encompass electronic documents. Promoting public access to these records in their entirety will further the strong public interests in monitoring official conduct, fostering the legitimacy and integrity of government actions, and protecting our form of democratic self-government in an age where government business is increasingly conducted and recorded electronically. ■

## Endnotes

1. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646–47 (D. Kan. 2005) (citation omitted).

2. Peter S. Kozinets, *Access to the E-Mail Records of Public Officials: Safeguarding the Public's Right to Know*, 25:2 COMM'NS LAW. 18 (2007) (citations omitted).

3. 218 P.3d 1004, 1008 (Ariz. 2009). David J. Bodney, Chris Moeser, and the author submitted an *amici curiae* brief for The Associated Press; Gannett Co., Inc.; The Reporters Comm. for Freedom of the Press; and The E.W. Scripps Co. in *Lake*.

4. *Lake v. City of Phoenix*, 207 P.3d 725, 730 (Ariz. Ct. App. 2009), *rev'd*, 218 P.3d 1004, 1005–08 (Ariz. 2009).

5. July 15, 2009, Declaration of Richard Pearce-Moses ¶ 7 [hereinafter Pearce-Moses Decl.], attached as Exhibit 1 to Brief for The Associated Press; Gannett Co., Inc.; The Reporters Comm. for Freedom of the Press; and The E.W. Scripps Co. as Amici Curiae, *Lake v. City of Phoenix*, No. CV-09-0036 PR (Ariz. S. Ct.), 2009 WL 2819793.

6. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 547–48 (D. Md. 2007) (quoted in Scott V. Cockerham, *Lake v. City of Phoenix: Is Metadata a Public Record?* 51:517 ARIZ. L. REV. 524 n.78 (2009)).

7. Cockerham, *supra* note 6, at 524.

8. Tom Zeller Jr., *Beware Your Trail of Digital Fingerprints*, N.Y. TIMES, Nov. 7, 2005.

9. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646–47 (D. Kan. 2005).

10. *Id.*

11. July 14, 2009, Declaration of Stephen K. Doig ¶¶ 5, 10 [hereinafter Doig Decl.], attached to Brief for First Amendment Coal. of Arizona, Inc.; Soc. of Prof'l Journalists; and Arizona Newspapers Ass'n as Amici Curiae, *Lake v. City of Phoenix*, No. CV-09-0036-PR (Ariz. S. Ct. 2009).

12. Jeff Leen, Stephen K. Doig & Lisa Getter, *What Went Wrong: Failure of Design and Discipline*, MIAMI HERALD, Special Sec., 1992 WLNR 2265633 (Dec. 20, 1992); Doig Decl., *supra* note 11, ¶ 13.

13. *E.g.*, Walt Bogdanich, *In Deaths at Rail Crossings, Missing Evidence and Silence*, N.Y. TIMES, July 11, 2004, <http://www.nytimes.com/2004/07/11/national/11RAILS.html> (last visited Apr. 5, 2010).

14. Pearce-Moses Decl., *supra* note 5, ¶¶ 1–3, 11.

15. *Id.* ¶ 11.

16. 44 U.S.C. § 3301 (emphasis added).

17. Armstrong v. Executive Office of the President, 1 F.3d 1274, 1279 (D.C. Cir. 1993).

18. 5 U.S.C. § 552(f)(2)(A).

19. *Id.* § 552(a)(3)(B).

20. [http://www.justice.gov/oip/foia\\_updates/Vol\\_XVII\\_4/page2.htm](http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm) (last visited Mar. 30, 2010).

21. ARK. CODE ANN. § 7-9-125; CONN. GEN. STAT. ANN. § 1-200(5); D.C. CODE § 2-502(18); GA. CODE ANN. § 50-18-70(a); LA. REV. STAT. ANN. § 44:1(A)(2) (a); NEB. REV. STAT. § 84-712.01(1); N.C. GEN. STAT. ANN. § 132-1(a); OKLA. STAT. ANN. tit. 51, § 24A.3(1); OR. REV. STAT. ANN. § 192.410(6); 65 PA. CONS. STAT. ANN. § 67.102; R.I. GEN. LAWS § 38-2-2.

22. CAL. GOV. CODE § 6252; DEL. CODE ANN. tit. 29, § 10002; D.C. CODE § 2-502(18); FLA. STAT. ANN. § 119.011(12); 5 ILL. COMP. STAT. ANN. 140/2(c); IND. CODE ANN. § 5-14-3-2(n); KAN. STAT. ANN. § 45-217(f)(1) [(g)(1)]; KY. REV. STAT. ANN. § 61.870(2); LA. REV. STAT. ANN. § 44:1(A)(2)(a); ME. REV. STAT. ANN. tit. 1, § 402(3); MISS. CODE ANN. § 25-61-3(b); NEB. REV. STAT. § 84-712.01(1); N.H. REV. STAT. ANN. § 91-A:1-a(III); N.M. STAT. ANN. § 14-2-6(E); N.Y. PUB. OFF. LAW § 86(4); N.C. GEN. STAT. ANN. § 132-1(a); N.D. CENT. CODE § 44-04-17.1(15); OKLA. STAT. ANN. tit. 51, § 24A.3(1); OR. REV. STAT. ANN. § 192.410(4) (a); 65 PA. CONS. STAT. ANN. § 67.102; S.D. CODIFIED LAWS § 1-27-1.1; TENN. CODE ANN. § 10-7-301(6); UTAH CODE ANN. § 63G-2-103(22)

(a); VT. STAT. ANN. tit. 1, § 317(b); VA. CODE ANN. § 2.2-3701; WASH. REV. CODE ANN. § 40.14.010; WIS. STAT. ANN. § 19.32(2); WYO. STAT. ANN. § 16-4-201(a)(v).

23. Access to Electronic Records: A State-by-State Guide to Obtaining Government Data, [http://www.rcfp.org/elecaccess/elec\\_access\\_main.htm](http://www.rcfp.org/elecaccess/elec_access_main.htm) (last visited Mar. 24, 2010) (quoting the National Association of Legislative Information Technology (NALIT)).

24. 1 F.3d 1274 (D.C. Cir. 1993).

25. See Armstrong v. Bush, 721 F. Supp. 343, 345 n.1 (D.D.C. 1989) (discussing the Iran-Contra affair, which some called “Iranamok”), *rev'd*, 924 F.2d 282 (D.C. Cir. 1991); David A. Wallace, *Electronic Records Management Defined by Court Case and Policy*, 35:1 INFO. MGMT. J. 2, 2001 WLNR 4449679 (Jan. 31, 2001). As it turned out, the White House Communications Agency had preserved backup tapes containing the e-mails, which, according to the Tower Commission, ultimately provided a comprehensive, “first-hand, contemporaneous, account of events.” *Id.* (quoted in Leanne Holcomb & James Isaac, *Wisconsin's Public-Records Law: Preserving the Presumption of Complete Public Access in the Age of Electronic Records*, 2008:3 WIS. L. REV. 517, 540–41 (2008)).

26. *Armstrong*, 1 F.3d at 1277.

27. *Id.* at 1280.

28. *Id.*

29. *Id.*

30. *Id.* at 1283.

31. *Id.* at 1285.

32. 218 P.3d 1004 (Ariz. 2009).

33. *Id.* at 1005.

34. *Id.*

35. *Id.*

36. *Lake v. City of Phoenix*, 207 P.3d 725, 733–74 (Ariz. Ct. App. 2009).

37. *Id.* at 734, 741.

38. *Id.* at 733–74.

39. *Id.*

40. *Id.* at 740.

41. *Id.*

42. *Id.* at 739.

43. *Id.*

44. *Id.* at 740–41.

45. *Id.* at 740.

46. *Id.* at 741.

47. *Id.* (quoting *Griffis v. Pinal County*, 156 P.3d 418, 422 (Ariz. 2007)).

48. ARIZ. REV. STAT. § 41-1350 (“[R]ecords’ means all books, papers, maps, photographs or other documentary materials, regardless of physical form or characteristics, including prints or copies of such items produced or reproduced on film or

electronic media . . . made or received by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government, or because of the informational and historical value of data contained therein. . . .”) (emphasis added).

49. *Lake v. City of Phoenix*, 218 P.3d 1004, 1007 (Ariz. 2009) (quoting *Carlson v. Pima County*, 687 P.2d 1242, 1246 (Ariz. 1984)).

50. *Id.* at 1007–08.

51. *Id.*

52. *Id.*

53. *Id.* at 1008.

54. *See id.*

55. *Id.*

56. *See also id.* (“Public records requests that are unduly burdensome or harassing can be addressed under existing law, which recognizes that disclosure may be refused based on concerns of privacy, confidentiality, or the best interests of the state.”).

57. 187 P.3d 822 (Wash. Ct. App. 2008).

58. *Id.* at 824–25.

59. *Id.* at 828.

60. *Id.*

61. *Id.*

62. *Id.* at 825.

63. *Id.* at 826 (quoting WASH. REV. CODE §§ 42.17.020(41), 42.56.010(2)) (emphasis added).

64. *Id.* (quoting WASH. REV. CODE § 42.17.020(48)).

65. *Id.*

66. *Id.* at 827.

67. *Id.*

68. *Id.*

69. *O’Neill v. City of Shoreline*, 208 P.3d 554 (Wash. 2009) (table).

70. *See, e.g.*, Brief for Washington Coalition for Open Government as Amicus Curiae, *O’Neill*, 208 P.3d 554 (Feb. 16, 2010) (No. 84266-3), 2010 WL 782692.

71. *See* Brief for Washington Newspaper Publishers Ass’n and Allied Daily Newspapers of Washington, Inc., as Amici Curiae at \*4, *O’Neill*, 208 P.3d 554 (Feb. 12, 2010) (No. 84266-3), 2010 WL 782693.

72. N.Y. PUB. OFF. LAW § 85 *et seq.*

73. 895 N.Y.S.2d 262 (N.Y. App. Div. 2010).

74. *Id.* at 264, 266–68.

75. *Id.* at 268.

76. N.Y. PUB. OFF. LAW, art. 6, § 86.4 (emphasis added).

77. *Irwin*, 895 N.Y.S.2d at 268.

78. *Id.* at 267–68.

79. *Id.* at 266.

80. 882 N.Y.S.2d 862 (Sup. Ct., Albany Cty. 2009).

81. *Id.* at 864.

82. *Id.* at 865.

83. *Id.* at 877.

84. *Id.* at 877–78.

85. *Kozinets*, *supra* note 2, at 17–18.

86. *See Houghton v. Franscell*, 870 P.2d 1050, 1052 (Wyo. 1994) (“Legislation requiring disclosure of information is considered remedial, and ‘[r]emedial statutes are liberally construed. . . .’)” (quoting NORMAN J. SINGER, 3 SUTHERLAND STATUTORY CONSTRUCTION § 60.01, at 147 (5th ed. 1992)). To the extent that the definition of public records is remotely ambiguous in any state statute, courts should construe the law liberally, “resolving all reasonable doubts in favor of applicability of the statute to the particular case.” SUTHERLAND STATUTORY CONSTRUCTION, *supra*, at 189; *Kozinets*, *supra* note 2, at 23 and n.88.

87. *Kentucky Speedway, LLC v. Nat’l Ass’n of Stock Car Auto Racing, Inc.*, 2006 WL 5097354, at \*8–9 (E.D. Ky. Dec. 18, 2006).

88. *Kozinets*, *supra* note 2, at 24.