

# Access to the E-Mail Records of Public Officials: Safeguarding the Public's Right to Know

PETER S. KOZINETS

If the principle of open government means anything, it is that records of the conduct of government officials in office should be presumptively open to public scrutiny. Although this proposition is seemingly uncontroversial and well accepted, recent court decisions involving access to electronic mail messages on government computer systems have created a distinction between public and personal e-mails that threatens to erode the strong historic presumption of public access to governmental records. Specifically, several courts have held that the presence of an e-mail on a government computer system does not per se make the e-mail a public record. Rather, these courts have held that the contents of the e-mails must first be examined in camera to decide whether the e-mails relate to government duties or are personal and therefore beyond the reach of public records statutes. By so doing, these decisions have created a "personal" exemption to public records laws that, by and large, did not previously exist and that is based on an ill-defined standard of relevance to official duties.

Questions about the relevance of government e-mail records to official duties often defy easy resolution. For instance, amorous e-mails exchanged by two government employees may seemingly relate to a personal relationship rather than public business. But such a relationship could evidence corruption or favoritism, violate personnel rules, expose the agency to Title VII liability, exhibit dereliction of duty and misuse of public resources, or breach e-mail use and other policies that could trigger discipline or termination. Similarly,

---

*Peter S. Kozinets (pkozinets@steptoe.com) practices media and constitutional law in the Phoenix office of Steptoe & Johnson LLP. He thanks Lindsay Taylor, a student at the University of Arizona James E. Rogers College of Law, for her research assistance.*

although some e-mails between a public official and private individuals might not directly evidence possible misconduct in office, e-mails about a public official's dispensation of favors to people having business before the official's agency undoubtedly fall within the public's right of access. Indeed, e-mails that appear to concern an official's plans for private vacation travel might seem purely personal, only to be imbued with public significance when it turns out that the vacation was underwritten by developers or others having business before the official's agency.

Further complicating matters, there is no ready legal definition of the term *personal*. Although privacy is a legal concept that has been refined by more than a century of common law and legislative developments, the term *personal* is often undefined and seemingly amorphous. Nevertheless, some courts have indicated a willingness to extend that term beyond the narrow confines of privacy law. Although public employees might not have any reasonable expectation of privacy in their workplace e-mails (by virtue of employer policies that permit agencies to monitor and inspect e-mails), some courts have held that personal e-mails may still be withheld from disclosure.

In short, the distinction between public and personal e-mail threatens to shield from disclosure e-mails that do not necessarily memorialize the performance of required government functions but that could nevertheless reveal official malfeasance, misfeasance, or nonfeasance. Moreover, separating the public from the personal may require in camera review as a prerequisite to public access without first requiring the party opposing access to demonstrate why the records should not be released. The requirement of in camera review in cases where such review might not otherwise be necessary will increase the costs of public records requests and

impede the public right of prompt access to government documents.<sup>1</sup> Indeed, as one court noted in a related context, "[t]o delay or postpone disclosure undermines the benefit of public scrutiny and may have the same result as complete suppression."<sup>2</sup>

This article briefly discusses the policies underlying public access laws and highlights the critical importance of access to government e-mail. Next, the article reviews and critiques the differing standards that courts have formulated to resolve disputes about public access to the e-mail records of public officials. The article then advocates a "presumption of public access" standard that would render all government e-mails presumptively subject to freedom of information laws and would require in camera review only if the party opposing access shows that specific information in the e-mails would, if released, cause harm to legally cognizable interests of privacy or confidentiality or to a substantial state interest.

## Public Policy Behind Public Access Laws

The policies underlying open records statutes provide a useful guidepost for evaluating the merits of different standards that might apply to access requests for government e-mail records. There are at least three strong public policy justifications for such statutes. First, access to agency records allows members of the public to monitor the conduct of their officials and provides a check on government abuses. Such access promotes accountability of government officials and employees to the public.<sup>3</sup> Second, public access fosters public trust and confidence in the legitimacy and integrity of government decisions by opening government conduct to public view.<sup>4</sup> Third, and more generally, public access promotes democratic self-government and public participation. An informed citizenry is a necessary prerequisite to

any meaningful democracy, and access to public records provides a critical source of information to citizens about the conduct of government.<sup>5</sup>

### Importance of E-Mail Access

These policies militate strongly in favor of standards that permit broad public access to agency e-mail records. Access to e-mail offers an unparalleled window into the activities of public officials. According to one study, 93 percent of all new information created in the United States in 1999 was generated in electronic form.<sup>6</sup> “Electronic data are the modern-day equivalent of the paper trail,” and the recent e-discovery amendments to the Federal Rules of Civil Procedure recognize the critical importance of access to electronic records, including e-mails, in furthering the search for truth.<sup>7</sup>

Public officials use e-mail to conduct public business and communicate with constituents. According to a 2002 Pew national survey, 88 percent of local elected officials use e-mail in their public activities. One-third of public officials who had a public e-mail account said that they used it exclusively for public affairs; another third said that they used it for both public and private matters; and the final third said that they used their personal e-mail accounts to conduct public business.<sup>8</sup>

Public employee e-mails have shed important light on government activity in several recent controversies and have also illuminated official attempts to avoid public scrutiny. For instance, in June 2007, the House Oversight and Government Reform Committee reported that White House officials had evidently circumvented the Presidential Records Act by using e-mail accounts maintained by the Bush-Cheney 2004 campaign and the Republican National Committee (RNC), rather than their White House e-mail accounts, for official purposes, “such as communicating with federal agencies about federal appointments and policies.”<sup>9</sup> The Presidential Records Act requires the president to “take all such steps as may be necessary to assure that the activities, deliberations, decisions and policies that reflect the performance of his constitutional, statutory, or other official or

ceremonial duties are adequately documented . . . and maintained as Presidential records.”<sup>10</sup>

Nevertheless, the House Oversight Committee reported extensive destruction of the e-mails of senior White House officials by RNC, finding that RNC failed to preserve any e-mails for fifty-one of the eighty-eight officials who had RNC accounts and reporting “major gaps” in the e-mail records of the remaining thirty-seven officials, including Karl Rove.<sup>11</sup> Senate Judiciary Committee Chairman Patrick J. Leahy excoriated White House officials for using non-White House e-mail accounts to conduct official government business, stating

It is troubling that so many senior White House officials . . . were engaging in an effort to avoid oversight and accountability by ignoring the laws meant to ensure a public record of official government business. . . . This extensive end run around the laws leads one to wonder what these officials wanted to hide from the public and Congress.<sup>12</sup>

In another controversy involving the release of government e-mails, the Department of Justice (DOJ) earlier this year disclosed e-mails from 2005 between Kyle Sampson, then counselor to Attorney General John Ashcroft, and White House counsel’s office personnel. In one e-mail, Sampson wrote, “[W]e would like to replace 15–20 percent of the current U.S. Attorneys. . . . The vast majority . . . are doing a great job, are loyal Bushies, etc., etc.”<sup>13</sup> The e-mails, disclosed to Congress as part of its investigation into the firings, contributed to the public debate over the propriety of DOJ’s termination of several top prosecutors.

Also this year, NASA became embroiled in a scandal involving three astronauts. Several e-mail exchanges between space shuttle pilot Bill Oefelein and Air Force Captain Colleen Shipman were found in the possession of astronaut Lisa Nowak when she was arrested after her drive from Houston to Orlando to confront her perceived romantic rival. The first e-mail, from Shipman to Oefelein, was even sent to the shuttle while Oefelein was on a mission in space.<sup>14</sup>

There is a substantial public interest in the disclosure of all of these e-mails. The public has a strong right to know whether administration officials circumvented the Presidential Records Act, whether the White House and DOJ instigated an unprecedented purge of politically “disloyal” U.S. attorneys, and whether astronauts in the nation’s space program are using public resources properly. However, several of these e-mails might not be eligible for release under the standards that have been adopted by some of the courts discussed below, or might be released only after a trial court conducted a lengthy document-by-document review triggered by nothing more than the unsupported assertions of litigants opposing access.

### A Troubling Trend

The decisions summarized below reflect the most recent attempts by state appellate courts to reconcile the public’s right of access to government employee e-mails with assertions that some of the e-mails contain personal information. Despite statutory language that would seem to indicate a contrary result, several courts have held that the presence of e-mails on a publicly funded computer system does not automatically render the e-mails subject to public records laws. Rather, these courts have held that the e-mails may be deemed to fall within the scope of public records laws only if they relate to public business and only after a trial judge reviews them in camera.

### Idaho and Legitimate Public Interest

The Idaho public records law provides one of the broadest definitions of *public records* in the country. It defines *public records* as including “any writing containing information relating to the conduct or administration of the public’s business.”<sup>15</sup> Despite this expansive definition, the Idaho Supreme Court held in May 2007 that the presence of an e-mail on a public computer system does not, standing alone, render the e-mail a public record. However, if the e-mail involves a matter of “legitimate public interest,” it will qualify as a public record.

In *Cowles Publishing Co. v. Kootenai County Board of County Commissioners*,<sup>16</sup> the Idaho Supreme Court affirmed the release of e-mail communications between county prosecutor William Douglas, an elected official, and the manager of the county's Juvenile and Education Training (JET) court, Marina Kalani, a public employee whom Douglas had hired and supervised.<sup>17</sup> After the JET court failed to produce regular quarterly reports of its finances, its federal funds were suspended. Douglas defended Kalani and allowed the program to continue, using county monies instead of federal funds.<sup>18</sup> Meanwhile, the local press began reporting about an alleged improper relationship between the two. A reporter for the Spokane, Washington, *Spokesman Review* submitted a public records request to the Kootenai County Board of Commissioners for all e-mail correspondence between the two officials. The county released approximately 400 e-mails in whole or in part and withheld 597 e-mails. *Cowles Publishing Co.*, publisher of the *Spokesman Review*, filed a petition for access to public records to obtain the remaining e-mails, and the trial court ordered their release.<sup>19</sup>

Kalani argued on appeal that the e-mails fell outside the scope of Idaho's public records law because they did not constitute records of official government business but rather were personal communications that involved the couple's romantic relationship.<sup>20</sup> The Idaho Supreme Court rejected this argument, finding that the e-mails clearly contained "information relating to the conduct and administration of the public's business."<sup>21</sup> Specifically, "[t]he public has a legitimate interest in these communications between an elected official and the employee who[m] he hired and supervised" because when the JET court's problems became public, Douglas vigorously defended Kalani's management to both the county board and the public, and whether he did so as her supervisor "or . . . because of an alleged inappropriate relationship is a public concern."<sup>22</sup>

The court wrote that it was "not simply the fact that the e-mails were sent and received while the employees were at work or the fact that they were

'in' the employee's office that makes them a public record."<sup>23</sup> Instead, it was their "relation to legitimate public interest that makes them a public record."<sup>24</sup> Douglas's public defense of Kalani's work "put these e-mails within the purview of the public's business," as did the county's review and use of the e-mails when investigating the financial problems and demise of the JET court.<sup>25</sup>

Although the Idaho decision vindicated the public's right of access to the records at issue, it did so based on the existence of a legitimate public interest in the e-mails that has not usually been required in public records cases. Historically, members of the public have been entitled to a presumption of access without having to demonstrate any specific interest in the documents other than the fact that they are public records.<sup>26</sup> Consistent with that tradition, public records requesters should be presumptively entitled to inspect and copy the e-mail records of public officials without having to make a predicate showing of a specific interest in a preexisting controversy (such as a disciplinary action against a public employee or allegations of misconduct that are already under official investigation). Requiring such a showing would unnecessarily restrict access to otherwise public records and would hinder the ability of members of the public, including the press, to monitor the conduct of government officials. Placing a burden on the public to demonstrate a particularized public interest in accessing public records reverses the presumption that all writings by government officials made, maintained, or kept in the course of conducting public business are open to public inspection in the absence of some countervailing interest.

#### **Arizona and Substantial Nexus**

In April 2007, the Arizona Supreme Court held that purely private or personal e-mails that do not reflect a substantial nexus with government activities are beyond the reach of the Arizona Public Records Law. However, the court put the burden on the opponent of access to demonstrate that the requested e-mails are not public records.

In December 2005, Stanley Griffis, the highest unelected official of

Arizona's fastest growing county, was suspended from his position as Pinal County manager after the county launched an investigation into his unauthorized purchase of sniper rifles with county funds. Phoenix Newspapers, Inc. (PNI), the publisher of the *Arizona Republic*, filed a public records request with Pinal County seeking release of all e-mails sent to or received by Griffis on the county's e-mail system in the eight weeks leading to his suspension. The county released 706 e-mails but withheld 120 that might have contained personal information. Griffis filed suit against the county and sought an injunction prohibiting the county from releasing the e-mails, claiming that they were purely personal and that their release would cause irreparable harm. PNI intervened and moved to vacate the injunction. The trial court granted PNI's motion, finding that all of the e-mails should be released unless Griffis could demonstrate with specific facts that discrete information in the e-mails would cause harm if released. The Arizona Court of Appeals reversed, taking Griffis at his word (without conducting its own review of the e-mails' contents) that the e-mails were purely personal. The Arizona Supreme Court vacated that decision and remanded to the trial court for in camera review to determine whether the records fall within the scope of the public records statute.<sup>27</sup> The trial court has since conducted the review and ordered the release of 57 e-mails, including several that "identified a personal/business relationship between [Griffis] and El Dorado Holdings," a development company having business before the county.<sup>28</sup>

Days after the state supreme court heard argument, Griffis pleaded guilty to six felonies for embezzling hundreds of thousands of dollars in county fees for personal use, defrauding the state retirement system, failing to pay taxes, and using his county credit card for personal purchases. Investigators called the case the largest instance of public graft in Arizona history.<sup>29</sup>

In ordering remand, the Arizona Supreme Court recognized that Arizona's public records law does not contain precise definitions of *public records* or *other matters* covered by the statute.<sup>30</sup> However, the statutory

framework supported a broad reading of the scope of the public records law. For example, § 39-121.01.B of the Arizona Revised Statutes requires 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 monies from the state or any political subdivision of the state.” Prior case law provided three definitions of *public record* and a broader definition of *other matters* but largely avoided technical distinctions between such categories and focused instead on balancing the public policy in favor of open government against countervailing interests in privacy, confidentiality, or the best interests of the state.<sup>31</sup>

**The e-mail must “have a demonstrable connection to the performance of public functions or involve the receipt or expenditure of public funds.”**

Notwithstanding the broad statutory language and the strong presumption of public access embodied in Arizona law, the court found that e-mails “do not necessarily qualify as public records” merely because they are generated or maintained on a government e-mail system.<sup>32</sup> However, the court held that if e-mails are withheld because of an assertion that they are “purely personal,” the requester has a right to in camera review of the records by a trial court judge to determine whether the records fall within the scope of the public records statute.<sup>33</sup> Once in camera review is triggered, the opponent of access has the burden of establishing that the e-mails are not public records.<sup>34</sup>

The court wrote that the statute “does not encompass documents of a purely private or personal nature.”<sup>35</sup> Instead, the e-mails must have a “‘substantial nexus’ with a government agency’s activities [to] qualify as public records.”<sup>36</sup> The “nature and

purpose” of the records will determine their status, requiring a “content-driven inquiry.”<sup>37</sup>

The court strove to avoid a result where e-mails about plans for the family dinner would become subject to public disclosure.<sup>38</sup> “The contents of [such] purely private documents,” the court wrote, “shed no light on how the government is conducting its business or spending taxpayer money.”<sup>39</sup> However, in attempting to avoid disclosure of such personal documents, the court emphasized a substantial nexus standard that it failed to define and that seems at odds with Arizona’s strong presumption of public access to government records. Presumably, e-mails that shed light on the performance (or nonperformance) of a public official in office, or on the use or expenditure of taxpayer funds, possess the requisite substantial nexus to qualify as public records. It remains to be seen, however, whether lower courts will attempt to use the substantial nexus standard to constrict the scope of the public records law in ways that hinder the public’s ability to monitor the conduct of its officials.

**Colorado and the “Demonstrable Connection”**

In 2005, the Colorado Supreme Court held that “the simple possession, creation, or receipt of an e-mail record by a public official” is not enough to render the e-mail a public record.<sup>40</sup> Rather, the e-mail must “have a demonstrable connection to the performance of public functions or involve the receipt or expenditure of public funds.”<sup>41</sup>

In *Denver Publishing Co. v. Board of County Commissioners of County of Arapahoe*, the court found that sexually explicit e-mails between the county clerk and the assistant chief deputy clerk (with whom the county clerk was having an affair) were not public records even though the records were made part of an investigative report regarding sexual harassment in the workplace.<sup>42</sup> The court held that to qualify as a public record, “an e-mail message must be for use in the performance of public functions or involve the receipt and expenditure of

public funds.”<sup>43</sup> If the requester can show that the e-mails were made or are maintained or kept by a government agency, the burden shifts to the agency to show that the e-mails are public or nonpublic.<sup>44</sup> To meet that burden, “the agency must look to the content of the records to resolve whether they relate to the performance of public functions or involve the receipt or expenditure of public funds.”<sup>45</sup>

After considering the contents of the requested e-mails, the court found that most of them involved sexually explicit exchanges between the two employees that were sent “in furtherance of their personal relationship” and not in the performance of official duties.<sup>46</sup> Disclosing these e-mails would merely satisfy “prurient interests.”<sup>47</sup> However, to the extent that the e-mails contained both public and private communications, the court remanded for redaction of nonpublic information and release of the remainder.<sup>48</sup>

*Denver Publishing* permits exclusion from the scope of the state’s public records statute e-mails gathered in the course of a government investigation into workplace harassment and deemed too “sexually explicit” by the court. It contrasts with the Idaho Supreme Court decision discussed above, in which the review and use of e-mails in an internal agency investigation, among other factors, supported the court’s holding that the documents qualified as public records. Moreover, it relies on the arbitrary judgment of courts regarding when e-mails involving public officials are too explicit to be disclosed to the public, raising concerns about censorship and editorial judgment that should have no place in a discussion of whether government employee e-mails are public records. The decision also imbues public employee e-mails with an aura of privacy that is unjustified as a matter of settled law, as discussed below.

**E-Mails in Arkansas**

The trend in e-mail cases of requiring a substantial nexus or demonstrable connection to official activities may have reached its zenith with the majority opinion of the Arkansas Supreme Court in *Pulaski County v. Arkansas Democrat-Gazette*.<sup>49</sup> In a four-to-three decision, handed down in July 2007,

the Arkansas court required in camera review of e-mail communications between the former Pulaski County comptroller and director of administrative services, Ronald Quillin, and employees of Government e-Management Solutions, Inc., a county contractor. Quillin had been arrested for allegedly embezzling \$42,000 from the county, and the requested e-mails were reviewed by the government as part of its investigation of his activities in office. Moreover, Quillin and the representative of the contractor who negotiated with the county (identified only as Jane Doe) were apparently involved in an affair that was possibly linked to Quillin's alleged misuse of public funds.

Despite broad statutory language suggesting that all government e-mail records are subject to the state's freedom of information law and are presumptively public, the court held that "in this particular case, it is necessary to conduct an in camera review of the e-mails to discern whether the e-mails relate solely to personal matters or whether they reflect a substantial nexus with Pulaski County's activities, thereby classifying them as public records."<sup>50</sup> Without having a "neutral court" review the e-mails, the court held that there was not enough evidence in the record to sustain the trial judge's ruling that "all aspects of the personal relationship between Mr. Quillin and Jane Doe are intertwined and enmeshed in the business relationship between Pulaski County and Government e-Management Solutions, Inc."<sup>51</sup> Moreover, absent such a review, the record could not support the trial court's conclusion that "the e-mails at issue are public records because they involve a business relationship of the County and are a record of the performance or lack of performance of official functions by Ron Quillin during the times when he was an employee of Pulaski County."<sup>52</sup>

The decision drew two sharp dissents. Justice Tom Glaze, joined by two other justices, wrote that the majority's decision "will seriously weaken the [state's] FOIA and its legislative intent."<sup>53</sup> The plain language of the Arkansas statute, unlike those of Arizona, Florida, or other states, specifically recognizes that "[a]ll

records maintained in public offices or by public employees within the scope of their employment shall be presumed to be public records."<sup>54</sup> Moreover, the statute defines *public records* as including

writings . . . electronic or computer-based information, or data compilations in any medium required by law to be kept or otherwise kept that constitute a record of the performance or lack of performance of official functions that are or should be carried out by a public official or employee.<sup>55</sup>

Based on the statute's plain language, Justice Glaze argued that Quillin's e-mails, which were maintained by the county, were presumptively public. Moreover, the factual context demonstrated that the e-mails constituted a record of Quillin's performance or lack of performance of his duties because "the personal and professional relationship between Quillin and Doe may have affected or influenced Quillin's performance and his expenditures of county funds. . . ."<sup>56</sup>

In these circumstances, the law required disclosure unless an opponent could establish the applicability of a statutory exemption. Because no one had rebutted the statutory presumption of access, Justice Glaze wrote that remanding the matter for in camera review "unnecessarily prolongs the process and increases the expense of a FOIA request, and in so doing needlessly infringes upon a citizen's right to obtain public records."<sup>57</sup>

Justice Annabelle Clinton Imber, who joined Justice Glaze's dissent, wrote separately to emphasize that although the majority's decision would make sense "under a narrow interpretation of the [FOIA] statute, . . . that is not our law with respect to FOIA."<sup>58</sup> Rather, Arkansas courts traditionally apply a broad, liberal construction to that state's FOIA statute, and such a construction would preclude the majority's decision. Moreover, Justice Imber highlighted the context in which the e-mails were exchanged: "Where, as here, an alleged misuse of funds intersects with an extramarital affair, the timing and nature of the e-mail exchanges are material to the media's investigation into whether a county

employee conducted county business in an open and public manner."<sup>59</sup>

The dissents of Justices Glaze and Imber underscore the fundamental flaws of the decisions discussed above. Those decisions threaten to roll back the strong presumptive right of public access to public records, and to increase substantially the delay and expense of public records requests and any follow-on litigation by requiring in camera reviews of potentially voluminous documents based merely on unsupported assertions of harm. Moreover, those decisions are fundamentally at odds with the historic presumption in favor of public access to government records, and with the tradition of liberally construing open government laws to maximize public access to records of the conduct of government officials.

On remand, the trial court took a broad view of the Arkansas Supreme Court's requirement that the e-mails reflect the performance of official functions and ruled that virtually all of the e-mails be released.<sup>60</sup>

### Florida and Ohio

In *Florida v. City of Clearwater*, the Florida Supreme Court held that an e-mail is not a public record simply because it was created and stored on a publicly owned computer.<sup>61</sup> Rather, "[t]he determining factor is the nature of the record, not its physical location."<sup>62</sup> The court decision is grounded largely in the language of Florida law. The court noted that the Florida constitution affirmed the public's right to inspect and copy "any public record made or received in connection with the official business of any public body, officer, or employee of the state," and that the Florida public records statute defined *public records* as including documents "made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency."<sup>63</sup> Both definitions indicated that public records must be "in some way connected to 'official business.'"<sup>64</sup> The court held "without prejudice to *Times Publishing* seeking an *in camera* review of the disputed e-mails,"<sup>65</sup> that private or personal e-mails fall outside the scope of the state's public records laws.

In Ohio, a public record must be a document created or received by a public office, "which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office."<sup>66</sup> In *Ohio ex rel. Wilson-Simmons v. Lake County Sheriff's Department*, the Ohio Supreme Court held that allegedly racist e-mails sent between corrections officers were not public records.<sup>67</sup> The court noted that although the e-mails were written by public employees on a public office's e-mail system, the e-mails were "never used to conduct the business of the public office."<sup>68</sup>

Standards such as the one adopted by Ohio could be read to exclude e-mails that do not document official business but that could evidence malfeasance, misfeasance, or nonfeasance in office.

### **Privacy Interests in Washington State**

Washington's public records law states that a public record is a writing that contains "information relating to the conduct of government or the performance of any governmental or proprietary function."<sup>69</sup> Washington courts tend to interpret this provision broadly.

In *Tiberino v. Spokane County*, Cowles Publishing Co. and Spokane Television, Inc., made a public records request to Spokane County for all e-mails that the county had printed when it terminated a legal secretary for excessive personal use of the county e-mail system. The Washington Court of Appeals held that the e-mails related to the conduct of a governmental or proprietary function because the secretary's excessive personal use of e-mail was the reason for her discharge and because the county printed the e-mails to prepare for litigation relating to her termination, a "proprietary function."<sup>70</sup>

Nevertheless, the court then held that the e-mails were exempt from disclosure as personal information. Unlike many jurisdictions, Washington statutorily exempts from disclosure "[p]ersonal information . . . to the extent that disclosure would violate [the employee's] right to privacy."<sup>71</sup> The court found that the secretary's personal e-mails were sent only to a limited group of people and contained "intimate details about her

personal and private life and do not discuss specific instances of misconduct."<sup>72</sup> Moreover, the contents of her e-mails were "unrelated to government operations," and the employee's privacy interests outweighed the public interest in access.<sup>73</sup> Although the court recognized that the amount of time she spent on personal concerns at work was a matter of public interest, information about the number and frequency of her personal e-mail communications satisfied the public interest. "What she said in those e-mails," however, "is of no public significance."<sup>74</sup>

The court recognized that where the employee's misuse of e-mail became a reason for discipline or termination, her e-mails fell within the scope of Washington's public records statute. The court then applied a statutory exemption for "personal information" that was expressly tied to the legal concept of the right of privacy and that provided a readily employable definition for determining the circumstances in which the e-mails should be released or withheld.

Like the Idaho case, the Washington decision suggests that an employee disciplinary action or some other controversy must exist before underlying e-mails are deemed subject to the public records law. This notion is inconsistent with the presumption in favor of public access to government records and limits the ability of the public to monitor official conduct.

### **Broader Right of Access Elsewhere**

Other states recognize a broader right of access to e-mails stored on government e-mail systems.<sup>75</sup> In Massachusetts, for example, the state archives department, a division of the Secretary of the Commonwealth's Office, has instructed all public records custodians in the state that "[a]ll e-mail created or received by an employee of a government unit is a public record" and that "[a]ll e-mail messages are subject to public access and disclosure through the provisions of the [Massachusetts] Public Records Law."<sup>76</sup> Government agencies in Kentucky, Maryland, Oregon, and other states have announced similar positions.<sup>77</sup>

In an October 2007 Texas trial court decision, Judge Gena Slaughter ordered the City of Dallas to release

e-mails from personal e-mail accounts and personally owned BlackBerries. The court held that the e-mails were subject to disclosure under the Texas Public Information Act because they were used by former Dallas Mayor Laura Miller and other officials to conduct public business.<sup>78</sup>

### **Federal Cases**

Although federal cases recognize that e-mails should be treated as public records, no recent decisions discuss whether and how ostensibly personal e-mails should be differentiated from other e-mails maintained on federal agency computers. In *Armstrong v. Executive Office of the President*, the D.C. Circuit held that e-mails should be treated like other presidential records and that official business contained in e-mails should be preserved and made accessible to the public.<sup>79</sup> More recently, in *Tax Analysts v. Internal Revenue Service*,<sup>80</sup> the court held that IRS e-mails containing legal advice that lawyers in the IRS Chief Counsel's Office sent to field personnel are public documents that must be disclosed under 26 U.S.C. § 6110. The court invalidated an IRS rule stating that, although e-mail is a "writing," if an e-mail "consumed less than two hours of research and preparation, such that [a lawyer] need not open a case file, then the e-mail is to be treated like informal telephone advice. . . ."<sup>81</sup> The court held that the rule was inconsistent with the pertinent statute, which requires that any "written advice or instruction" prepared by the IRS Office of Chief Counsel and issued to any field personnel that conveys any legal or policy advice "shall be open to public inspection. . . ."<sup>82</sup>

### **Public Employee Privacy**

Many of the decisions discussed above are premised in varying degrees on employee privacy rights in the contents of their workplace e-mails. Yet these decisions are strikingly inconsistent with settled law regarding the privacy rights of employees: when an employer adopts a policy stating that its employees' e-mails are the property of the employer and are subject to auditing and inspection, employees have little or no legally cognizable privacy right in their work e-mails. Indeed, the U.S.

Supreme Court has recognized that “[p]ublic employees’ expectations of privacy . . . may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.”<sup>83</sup> Several courts have held that employees have no reasonable expectation of privacy where they are aware of policies that grant ownership of data created on their employer’s computers to the employer or that allow the employer to review or disclose their e-mail messages.<sup>84</sup>

In fact, many public agencies adopt policies expressly stating that employees have no right of privacy nor any expectation of privacy in any information transmitted over the Internet and that the agency reserves the right to review, access, and disclose e-mail records. Public employees are typically required to acknowledge such policies in writing.<sup>85</sup>

In *Warshak v. United States*, the Sixth Circuit struck down as facially unconstitutional several provisions of the Stored Communications Act that allow a court to order the disclosure of the contents of stored e-mails without either a warrant based on probable cause or a subpoena with notice to the subscriber. The court found that the plaintiff had a reasonable expectation of privacy in the contents of e-mails sent through his Internet service provider (ISP) because “there is a societal expectation that the ISP . . . will not [access the contents of e-mails] as a matter of course.”<sup>86</sup> The court noted that if an ISP adopts a policy or user agreement explicitly providing “that e-mails and other files will be monitored or audited . . . , the user’s knowledge of this fact may well extinguish his reasonable expectation of privacy.”<sup>87</sup>

These decisions demonstrate that public employees’ privacy rights cannot justify the rollback of the presumption in favor of public access embodied by several of the state court cases summarized above. Although those cases purport to base their holdings on interpretations of public records laws that require a well-defined nexus to government activities, the decisions seem driven in large part by practical concerns about how to preserve employee privacy in workplace e-mails. As the foregoing privacy

cases show, however, these interpretations are legally insupportable as a matter of privacy law. And as the dissents of Justices Glaze and Imber illustrate in the Arkansas case, these interpretations are radically inconsistent with the strong tradition of construing public records statutes liberally.<sup>88</sup>

### **Restoring the Presumption of Public Access**

To safeguard the public’s ability to monitor the conduct of government officials, courts and legislatures should reject the narrow constructions of state public records laws recently adopted by several state courts and should instead restore a strong presumption of public access to the e-mail records of public officials.

Several recent decisions, as discussed above, require trial courts to conduct an in camera review of e-mails, without requiring the opponent to first provide any evidence or facts sufficient to substantiate the claim of harm, if the opponent of the public records request asserts that the records are personal or private. The resort to near-automatic in camera review may be unnecessary in many cases, and it will increase the costs of litigation, delay the disclosure of records, and potentially overburden trial courts with the review of voluminous e-mail records.

Although in camera review might be unavoidable in many cases, a different standard should be adopted to streamline the resolution of public records disputes and enforce the public’s right of access. That standard should (1) begin with a strong presumption of prompt public access to the e-mail records of public officials stored on government computer systems; and (2) require the party challenging disclosure to demonstrate, before in camera review is considered, why each ostensibly personal e-mail (or each item of personal information contained therein) should not be released.

Such a standard ensures that information of public interest will not be obscured by technical distinctions or threshold legal disputes about what qualifies as a public record. Moreover, it forces opponents of disclosure to

focus their objections on those specific e-mails that would allegedly cause substantial harm if released, and provides an early opportunity for opponents to identify e-mails that may be released without further delay. It also requires opponents to justify their position before compelling the court to undertake a potentially unnecessary in camera review. In short, this standard facilitates the opening of government activity to public scrutiny without requiring public records requesters to incur substantial costs and delays in securing access.

## **Courts and legislatures should restore a strong presumption of public access to the e-mail records of public officials.**

If an in camera review becomes necessary, courts should examine both the content and context of the requested e-mails, should be informed by the policies underlying open records laws, and should resolve all doubts in favor of public access and disclosure. Moreover, the opponent of access should be required to provide suggested redactions to the court, along with a complete set of the unredacted records, for the court’s review. Requesters should be encouraged to submit extrinsic evidence, supplemental briefing, checklists of facts or questions for the court to consider, and other materials that may assist the court with viewing the e-mails in context as it conducts the in camera review.

Applying a strong presumption of access to agency e-mail records also comports with the policies that numerous government agencies have adopted regarding employee e-mail usage. Those policies typically require employees to acknowledge that their e-mail records are subject to inspection, monitoring, and public disclosure; that they have no right of privacy or any reasonable expectation of privacy in workplace e-mails; that the e-mails are owned by the agency, not the employee; and that e-mails are presumptively considered to be public records.

The prevailing law of employee privacy in the private sector fully supports application of the presumption of public access to these records.

Moreover, the presumption recognizes that all e-mails generated or received on government e-mail systems reflect the public's business because they involve the expenditure of substantial taxpayer funds. Significant public resources are needed to establish and maintain such systems, including the e-mail servers on which such communications are stored.<sup>89</sup> The use of public e-mail systems for personal purposes burdens servers with unnecessary storage and traffic, increases the risk of infection by viruses and worms, and diverts public employees from their task of performing public business on the public's time.<sup>90</sup> Indeed, knowledge that the public has an actual enforceable right to inspect all public employee e-mails ought to deter and thus reduce the misuse of government resources by public employees.<sup>91</sup> These factors further support the adoption of a strong presumption in favor of public access and disclosure.

### Applying the Proposed Standard in Practice

A brief hypothetical demonstrates how the presumptive access standard would safeguard public access to e-mails of ostensibly personal conduct that relate to the performance or nonperformance of government officials. Assume that suspicions arise about whether the police chief of a midsize city has developed a gambling addiction. The chief is absent from work frequently and has been known to talk casually about taking trips to Las Vegas. A local newspaper submits a public records request for all of the chief's work place e-mails for the last four months, and the chief objects to disclosure of several e-mails that he claims are personal and unrelated to his official job duties. Among the withheld e-mails are several e-mail exchanges with his secretary and travel agent regarding arrangements for multiple trips to Las Vegas, as well as several exchanges with hotels on the Las Vegas Strip offering complimentary suites, meals, beverages, and more.

Under the demonstrable connection or substantial nexus standards adopted

by some courts, the newspaper might not secure access to the records. If the chief objects, the requester will have to file suit and obtain in camera review of the requested records. The court will have to determine whether the e-mails are demonstrably connected to the chief's performance of his official duties, or whether a substantial nexus exists between the e-mails and those duties. The chief might assert simply that he conducted no work during his trips and that they were not paid for with public funds. The court might accept this proposition at face value, especially if its content-driven analysis of the records does not uncover any specific connection between the e-mails and the chief's duties.

The result would likely be far different and far more consistent with the public's right of access if courts or legislators adopt the presumptive public access standard. Under that standard, the chief's workplace e-mails would be presumptively public, and he would bear the burden to specifically demonstrate what harms would occur if the e-mails were released. The newspaper would be able to argue that the public's interest in investigating the causes of the chief's absenteeism outweighs any interest in privacy that the chief might assert. If the court determines that it does not have enough of a record on which to issue a ruling, it could then require in camera review. However, it would have to conduct the review in a manner consistent with the strong public policy in favor of public access, resolving all doubts in favor of disclosure and placing the burden of proof on the chief.

### Conclusion

Although the public records cases described above involve variations based on particular statutory language and other factors, several cases evince a trend toward creating a distinction between public and personal e-mail records that would exclude personal e-mails from the scope of state public records statutes. This trend threatens to undermine the strong presumption in favor of public access, increase delays and costs associated with requests to access for public records, and hinder public access to government e-mail records that may reveal official

misconduct. To safeguard the public's right of access to this essential body of records, and consistent with the core purposes of our public records statutes, courts and legislatures should adopt a standard that embodies a strong presumptive right of public access and that places the burden squarely on the opponent of disclosure to demonstrate why specific information should not be released. In camera review should be required only when (and if) the opponent makes that showing, rather than as a first step.

The state court cases discussed above likely reflect an early and unfinished response to the question of how to reconcile the public's right of access to public records with the privacy rights of public employees. As e-mail continues to grow in importance as an essential source of information about the conduct of government, courts and legislatures should adopt standards designed to protect the public's right of access to e-mails and other written government records. Promoting public access is consistent with the prevailing law of employee privacy, and it will further the strong public interests in monitoring official conduct, fostering the public's trust in government actions, and strengthening our commitment to democratic self-government. 

### Endnotes

1. *See, e.g.*, ARIZ. REV. STAT. § 39-121.01.D.1 (public officers "shall promptly furnish" public records upon request).

2. *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 127 (2d Cir. 2006) (quoting *Grove Fresh Distribs., Inc. v. Everfresh Juice Co.*, 24 F.3d 893, 897 (7th Cir. 1994) ("The public cannot properly monitor the work of the courts with long delays in adjudication based on secret documents.")).

3. *See, e.g.*, *Phoenix Newspapers, Inc. v. Keegan*, 35 P.3d 105, 112 (Ariz. Ct. App. 2001) ("The core purpose of the public records law is to allow the public access to official records and other governmental information so that the public may monitor the performance of government officials and their employees."); ARK. CODE ANN. § 25-19-102 ("It is vital in a democratic society that public business be performed in an open and public manner so that the electors shall be advised of the performance of public officials and of the decisions that are reached in public activity and in

making public policy.”) *cf.* *Globe Newspapers Co. v. Superior Ct.*, 457 U.S. 596, 605 (1982) (“Public scrutiny of a criminal trial enhances the quality and safeguards the integrity of the factfinding process, with benefits both to the defendant and society as a whole.”).

4. *Cf.* *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 572 (1980) (“People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing.”).

5. *Globe Newspapers*, 457 U.S. at 606.

6. MICHAEL R. ARKFELD, *ELECTRONIC DISCOVERY AND EVIDENCE* § 1.1, at 1–2 (2006–07 ed.) (quoting *In re Bristol-Myers Squibb Sec. Litig.*, 205 F.R.D. 437, 440 n.2 (D.N.J. 2002)).

7. *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, Case No. 502003CA005045XXOCAI, 2005 WL 4947328, at \*5 (Fla. Cir. Ct. Mar. 1, 2005).

8. Elena Larsen & Lee Rainie, *Digital Town Hall: How Local Officials Use the Internet and the Civic Benefits They Cite from Dealing with Constituents Online*, PEW INTERNET & AM. LIFE PROJECT (Oct. 12, 2002), at [www.pewinternet.org/reports/toc.asp?Report=74](http://www.pewinternet.org/reports/toc.asp?Report=74).

9. COMM. ON OVERSIGHT & GOV'T REFORM, *THE USE OF RNC E-MAIL ACCOUNTS BY WHITE HOUSE OFFICIALS* (June 18, 2007), at <http://oversight.house.gov/story.asp?ID=1362>.

10. 44 U.S.C. § 2203(a).

11. COMM. ON OVERSIGHT, *supra* note 9.

12. Michael Abramowitz, *Bush Aides' Misuse of E-Mail Detailed by House Committee*, WASH. POST, June 19, 2007, at A03.

13. Dan Eggen & Paul Kane, *Justice Dept. Would Have Kept "Loyal" Prosecutors: Aide Recommended Retaining "Bushies" and Top Performers*, WASH. POST, Mar. 16, 2007, at A02.

14. *See Explicit E-Mail Exchange May Have Provoked Astronaut Lisa Nowak's Breakdown: E-Mails Were Written in Weeks Before Astronaut's Pursuit of Perceived Rival*, ABC NEWS, Mar. 6, 2007, at <http://abcnews.go.com/Technology/story?id=2928533>.

15. IDAHO CODE ANN. § 9-337(13) (2006). Other states with similarly broad definitions include Connecticut and Oregon. *See* CONN. GEN. STAT. ANN. § 14-1-200(5) (“Public records or files” means any recorded data or information relating to the conduct of the public’s business prepared, owned, used, received or retained by a public agency.”); OR. REV. STAT. § 192.410(4)(a) (*public record* “includes any writing that contains information relating

to the conduct of the public’s business”).

16. 159 P.3d 896 (Idaho 2007).

17. *Id.* at 898.

18. *Id.*

19. *Id.* at 899.

20. *Id.*

21. *Id.* at 900.

22. *Id.*

23. *Id.*

24. *Id.* at 901.

25. *Id.*

26. *See, e.g., Anderson v. Home Ins. Co.*, 924 P.2d 1123, 1126 (Colo. Ct. App. 1996) (“There is no requirement that the party seeking access demonstrate a special interest in the records requested.”) (citing *Denver Publ’g Co. v. Dreyfus*, 520 P.2d 104 (Colo. 1974)).

27. *Griffis v. Pinal County & Phoenix Newspapers, Inc.*, 156 P.3d 418 (Ariz. 2007). David J. Bodney, Chris Moeser, and the author represented Phoenix Newspapers, Inc., in this matter.

28. Order re In-Camera Review, *Griffis v. Pinal County*, CV 2006-00147 (Ariz. Super. Ct., Pinal County, July 5, 2007).

29. Lynh Bui, *Judge Sentences Griffis to 3½ Years: Former Pinal Manager Stole \$600,000-plus from County*, ARIZ. REPUBLIC, May 11, 2007, at B1; J. Craig Anderson, *Pinal Craft Called Ariz. Worst: Ex-County Boss Pilfered \$426,800, Investigators Say*, E. VALLEY TRIB., Feb. 21, 2007, at A1.

30. *See* ARIZ. REV. STAT. § 39-121 (“Public records and other matters in the custody of any officer shall be open to inspection by any person at all times during office hours.”).

31. *See, e.g., Carlson v. Pima County*, 687 P.2d 1242, 1245 (Ariz. 1984) (abandoning “technical distinctions” between public records and other matters because the language of the Arizona Public Records Law is so broad).

32. *Griffis*, 156 P.3d at 419.

33. *Id.* at 420.

34. *Id.* at 423.

35. *Id.* at 421.

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.* at 422.

40. *Denver Publ’g Co. v. Bd. of County Comm’rs of County of Arapahoe*, 121 P.3d 190, 199 (Colo. 2005).

41. *Id.* at 203 (citing Colo. Rev. Stat. Ann. § 24-72-202(6)(a)(II) (West 2007)).

42. *Id.* Notably, the Colorado Supreme Court’s order granting certiorari review accepted as uncontested the findings of the lower courts that the e-mails were “public records.”

43. *Id.* at 199.

44. *Id.*

45. *Id.*

46. *Id.* at 203.

47. *Id.*

48. *Id.* at 205.

49. No. 07-699 (Ark. July 20, 2007), at <http://courts.state.ar.us/opinions/2007a/20070720/07-669.pdf>.

50. *Id.* at 12 (citing *Griffis v. Pinal County & Phoenix Newspapers, Inc.*, 156 P.3d 418, 421–22 (Ariz. 2007)).

51. *Id.*

52. *Id.*

53. *Id.* at 13.

54. *Id.* at 15 (citing ARK. CODE ANN. § 25-19-103(5)(A)).

55. *Id.*

56. *Id.* at 16.

57. *Id.* at 17.

58. *Id.* at 20.

59. *Id.* at 21.

60. News Media Update, Reporters Comm. for Freedom of the Press, *Sex E-Mail Sheds Light on Official’s Performance* (Aug. 13, 2007), at [www.rcfp.org](http://www.rcfp.org).

61. 863 So. 2d 149, 154 (Fla. 2003).

62. *Id.*

63. *Id.* at 151–52 (quoting FLA. CONST., art. I, § 24, and FLA. STAT. § 119.011(1)).

64. *Id.* at 152.

65. 863 So.2d at 151.

66. OHIO REV. CODE ANN. § 149.011(G) (West 2007).

67. 693 N.E.2d 789, 793 (Ohio 1998).

68. *Id.*

69. WASH. REV. CODE ANN.

§ 42.17.020(41) (West 2006).

70. *Tiberino v. Spokane County*, 13 P.3d 1104, 1108 (Wash. Ct. App. 2000).

71. *Id.* (quoting WASH. REV. CODE § 42.17.310(1)(b)).

72. *Id.* at 1109.

73. *Id.* at 1110.

74. *Id.*

75. *See* Jean Maneke & Dan Curry, *Public Scrutiny of Missouri E-Mail Under the Sunshine Law*, 60 J. MO. B. 14 (Jan.-Feb. 2004).

76. SPR BULL. No. 1-99 (Feb. 16, 1999) (rev. & reissued May 21, 2003, Mass. Archives), [www.state.ma.us/sec/arc/arcmu/rmubul/bull99/htm](http://www.state.ma.us/sec/arc/arcmu/rmubul/bull99/htm).

77. *See* Maneke & Curry, *supra* note 75, at 17 nn.38, 42, 48.

78. *See* Jennifer LaFleur, *Ruling: Dallas officials’ e-mails must be turned over*, THE DALLAS MORNING NEWS (Oct. 30, 2007), at <http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/102907dnmetemails.317323a.html>.

79. 1 F.3d 1274, 1282–83 (D.C. Cir. 1993).

80. No. 06-5136, 2007 WL 2089708 (D.C. Cir. July 24, 2007).

81. *Id.* at \*2.

82. 26 U.S.C. §§ 6110(b)(1), 6110(i).

83. O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

84. *See, e.g.*, Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002) (employee had no reasonable expectation of privacy in data stored on laptop computer owned by employer where employer warned employee that it could inspect the laptop; noting that an employer-owned computer is not like a safe or file cabinet supplied by the employer for the employee to keep private papers); United States v. Angevine, 281 F.3d 1130, 1134–35 (10th Cir. 2002) (university professor had no reasonable expectation of privacy in data downloaded from the Internet onto university computers where policy stated that university reserved right to randomly audit employees' Internet use); Haynes v. Attorney Gen. of Kan., No. 03-4209-RDR, 2005 WL 2704956, at \*3–4 (D. Kan. Aug. 26, 2005) (no expectation of privacy where policy warned employee that he

had no expectation of privacy); United States v. Bailey, 272 F. Supp. 2d 822 (D. Neb. 2003) (employee had no expectation of privacy in information stored in work computer).

85. *See, e.g.*, AP, *AG: Former Chief's E-Mails Are Public Record*, FREE NEW MEX., Apr. 4, 2006, at [www.freewmexican.com/news/41799.html](http://www.freewmexican.com/news/41799.html) (New Mexico's policy on information technology states that anyone who uses the e-mail system "shall have no expectation of privacy."); REPORTERS COMM. FOR FREEDOM OF THE PRESS, ELECTRONIC ACCESS TO COURT RECORDS, at [www.rcfp.org/elecaccess/connecticut.htm](http://www.rcfp.org/elecaccess/connecticut.htm) (Connecticut state and municipal government employees' electronic and voice mail management and retention guide "states that e-mail [] and voice mail messages sent or received in the conduct of public business are public records.").

86. Warshak v. United States, 490 F.3d 455, 471 (6th Cir. 2007).

87. *Id.* (citing United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (government employee lacked a reasonable expectation of

privacy in electronic files on his office computer where employer's policy notified him of employer's intention to "audit, inspect, and monitor" his computer files)).

88. *See also* 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.

89. *See, e.g.*, Penelope Thurmon Bryan & Thomas E. Reynolds, *Agency E-Mail and the Public Records Laws—Is the Fox Now Guarding the Henhouse?*, 33 STETSON L. REV. 649, 662–63 (Winter 2004).

90. *See id.*

91. *Id.*