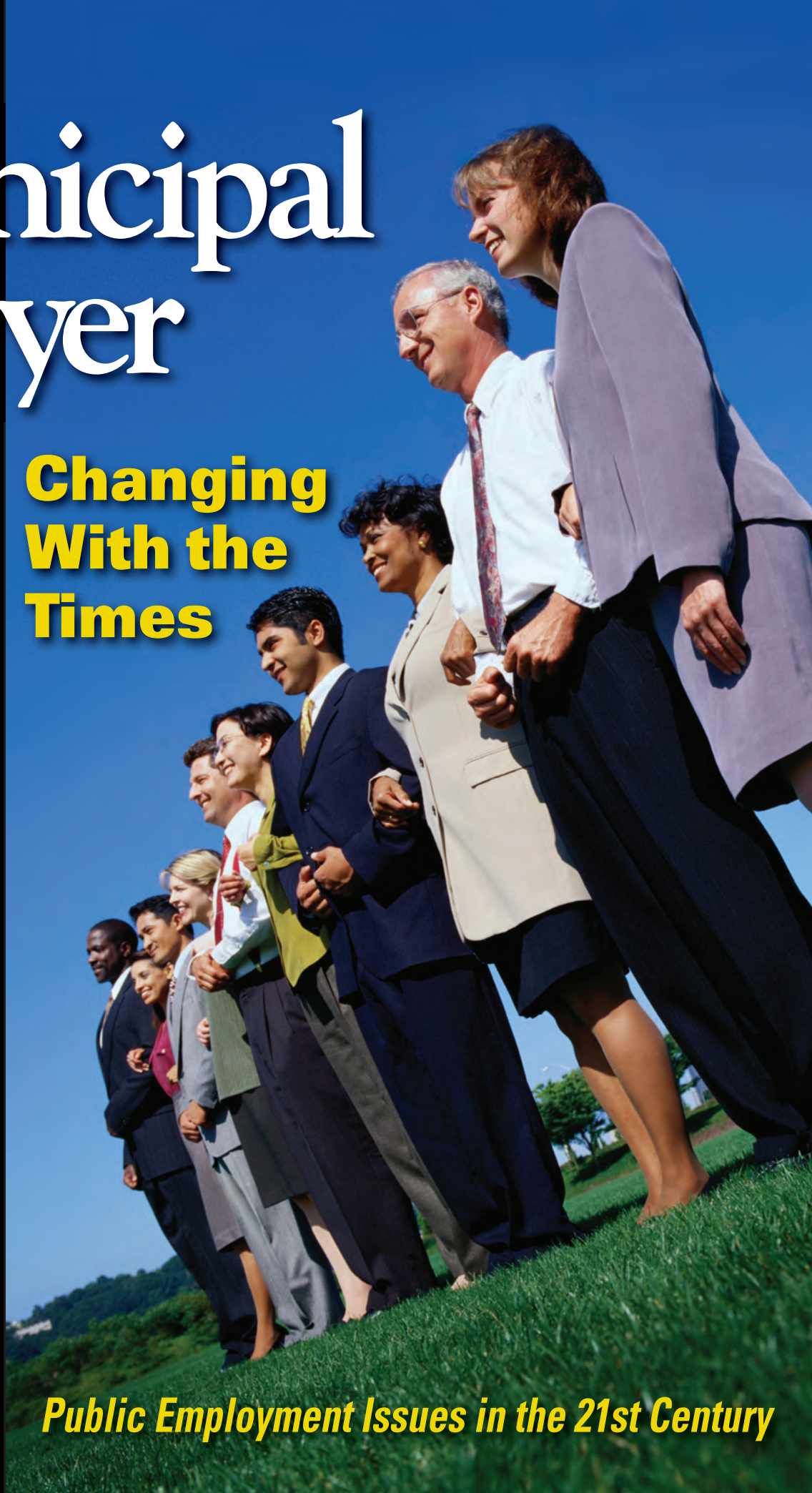
January/February 2009

Municipal Lawyer

INTERNATIONAL
MUNICIPAL
LAWYERS
ASSOCIATION

Changing With the Times



In this issue:

Public Employment Issues in the 21st Century

Municipalities and Employee Electronic Communications

— by Joshua K. Leader and Caroline C. Marino —

Consider this scenario: your department purchases and distributes BlackBerries to its employees. The devices operate on the municipality's service plan with a third-party provider. A few months later, a female employee complains that a male employee has been sending her and other female employees harassing, offensive messages from his BlackBerry. You review the content of the messages and confirm that the male employee has been using the device to send inappropriate material to his coworkers. Accordingly, you initiate disciplinary proceedings and inform him that his misconduct will result in a negative review in his file. A few weeks later, you are served with a complaint alleging that your review of "his" BlackBerry—owned by the municipality and issued on the municipality's service plan—constitutes an improper invasion of his privacy and violated his Fourth Amendment rights.

Does this sound far-fetched? A recent court ruling makes it clear that this is a real possibility, and far more likely to be an issue for municipal employers today given the prevalence of electronic communications in the workplace.

Recent Developments in the Law

In *Quon v. Arch Wireless Operating Co., Inc.*,[1] a city police department contracted for wireless text-messaging services for two-way pagers, which it then distributed to its employees. One employee, Jeff Quon, repeatedly exceeded the monthly text-message allotment on his pager, resulting in overage charges. The police department suspected that the overages resulted from the use of the pager to send personal messages. Although the police department had suggested that its official policy banning personal use of department-owned computers also applied to the pagers, there was no formal policy. Instead, the police department's informal policy was that employees who exceeded their monthly text-message allotment could avoid an audit of their messages if they paid the employer for any overages.

Although the department continued to allow Quon to pay for the overages in accordance with the informal policy for an extended period of time, it eventually obtained the transcripts of his text messages from the wireless provider to determine the cause of the constant overages. A review of the messages' content revealed that the overages were, in fact, attributable to personal messages. Quon filed a lawsuit against the police department alleging, *inter alia*, a violation of his Fourth Amendment right to privacy in the content of the messages.

The U.S. Court of Appeals for the Ninth Circuit determined that Quon had a reasonable expectation of privacy in his text messages, based on the police department's informal policy of foregoing an audit if the employee paid for any overages, despite the fact that the department owned the pager and paid for the wireless services. Additionally, the court held that the police department should not have been permitted to obtain transcripts of the messages from the service provider, since the federal Stored Communications Act[2] only permits the sender and addressee of the messages to view their content, regardless of who pays for the service.

Why is This Important?

Municipal employers need to stay abreast of developments in employees' privacy expectations and rights in electronic communications to avoid situations like that in *Quon*. A municipality may need to monitor or access its employees' electronic communications for many reasons, including:

- investigating employee misconduct, including sexual harassment and racial discrimination;
- responding to requests pursuant to freedom of information statutes, as discussed more fully below;
- discouraging employee use of municipal time and resources to conduct personal business; and
- protecting against illegal activities by employees, for which a municipal employer may be liable.

Many of these issues will also arise in the discovery context in litigation, and municipal employers should be aware of the scope of information that they may be required to access, review, and produce under the aegis of e-discovery obligations.

Constitutional Considerations

Municipal employers must be mindful of the potential constitutional implications when accessing their employees' electronic communications. Although the Fourth Amendment is more commonly associated with criminal matters, its protections extend to all unreasonable state-sponsored searches and seizures, including searches and seizures, by government employers or supervisors, of the private property of their employees.[3] As a result, a municipality's monitoring and review of its employees' electronic correspondence can potentially amount to an unlawful government search and seizure if those employees have a reasonable expectation of privacy in that

continued on page 14

Joshua K. Leader is a partner at Leader & Berkon LLP. He handles a wide range of litigation matters in areas such as complex commercial, securities, products liability, toxic torts, and intellectual property actions in state and federal courts. He has also been involved in defending municipal employees in § 1983 actions. He can be reached at 212-486-2400 or at jleader@leaderberkon.com.

Caroline C. Marino is an associate at Leader & Berkon LLP. She devotes the majority of her practice to commercial and products liability litigation. Her experience also includes defending claims for breach of non-compete agreements and misappropriation of trade secrets. She can be reached at 212-486-2400 or at cmarino@leaderberkon.com.

 cont. from page 13

correspondence. That determination is fact-driven and will turn on many of the issues discussed below.

Freedom of Information Obligations

Municipal employers also face the additional hurdle of satisfying their obligations under freedom of information laws without violating their employees' constitutional right to privacy. Many states have codified their own versions of the federal Freedom of Information Act,[4] thereby affording the public and the press the right to access state and local government records, including electronic correspondence, in order to remain informed about the process of governmental decision-making.[5] Although it is beyond the scope of this article, it is important to be aware of the breadth of the applicable freedom of information statute when evaluating expectation-of-privacy concerns in a particular jurisdiction. The definition of "public records" subject to inspection pursuant to freedom of information laws varies from state to state, and, in some instances, can be quite sweeping,[6] thereby increasing the likelihood that the electronic correspondence employees believe is private will, in fact, be subject to disclosure. Accordingly, municipal employers must strike the appropriate balance between freedom of information obligations and the privacy rights of their employees.

What Can Municipal Employers Do to Protect Themselves?

Although wireless devices and communications technology (such as text messaging and instant messages) are still relatively new areas for legal analysis and regulation, precedent developed in the more established areas of workplace computers and e-mail in both the public and private sectors is instructive. Courts have examined the following factors in determining whether an employee has a reasonable expectation of privacy in e-mail and other communications on employer-owned devices:

- whether the employer maintains a policy banning personal or other objectionable use;
- whether the employer monitors the use of the employee's computer or e-mail;
- whether third parties have a right of access to the computer or e-mails, including under the applicable freedom of information laws; and
- whether the employer notified the employee, or the employee was otherwise aware of, the applicability of a freedom of information statute and the employer's computer use and monitoring policies.[7]

Municipal employers must strike the appropriate balance between freedom of information obligations and the privacy rights of their employees.

These factors can translate into everyday workplace policies and procedures in a number of ways. Although all of these factors are instructive, no single one is dispositive: the courts have held that "given the great variety of work environments in the public sector, the question [of] whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[8]

Municipalities that wish to maintain access to their employees' electronic communications should adopt an explicit ban on the personal use of e-mail, computers, and other employer-issued devices, and specifically indicate that employer-issued devices are subject to monitoring, search, and review. Ways to accomplish this include articulating a policy in employee handbooks, requiring employees to periodically sign written acknowledgments of the municipality's policy, and even implementing an automatic prompt upon log-in on the device, that requires the employee to acknowledge that he or she has no expectation of privacy in the use of the system, and that the system is subject to inspection by the municipality at any time.

As seen in *Quon*, equally important as articulating and obtaining employees' acknowledgments of policies and procedures is ensuring that the municipality's departments act consistently with the articulated ban on personal use and the policy of regular monitoring, search, and review (including prohibiting any conflicting informal policies). This can be accomplished by implementing a regular back-up of electronic files, including e-mails, to a back-up drive accessible by supervisors, and informing employees of this. Municipalities that are particularly concerned with regulating electronic communications may even want to consider implementing routine searches of office computers and electronic files to further diminish employees' expectations of privacy.

Examples in Case Law

Case law further illustrates ways in which governmental entities have preserved their right to access employee e-mail. For instance, in *Hoff v. Spoelstra*,[9] a Michigan court determined that a city attorney did not have a reasonable expectation of privacy in her e-mails on the City's computer system. The City's information systems policy stated that such e-mails were considered City property and could be subject to public disclosure under the freedom of information statute, and specifically warned that personal messages could be accessed by City management without warning; therefore, employees were advised not to use e-mail to transmit any messages they would not want read by third parties.[10]

Similarly, in *Kelleher v. City of Reading*,[11] the Eastern District of Pennsyl-

vania found that the plaintiff city clerk did not have a reasonable expectation of privacy in her e-mail communications on the City's e-mail system. The City's guidelines expressly indicated that e-mails created, sent, or received using the City's system were City property; that the City reserved the right to access and disclose the content of all such messages, and that the e-mail system was strictly for official City messaging.[12] Further, the plaintiff had signed an acknowledgment indicating that she had received and read the guidelines, and the City had made a practice of monitoring and reviewing employee e-mails in the past.[13]

In *U.S. v. Angevine*,[14] the U.S. Court of Appeals for the Tenth Circuit found that a defendant college professor at a public university did not have a reasonable expectation of privacy in the files on his state-owned computer. The university advised its employees that it reserved and periodically exercised the right to view or scan any file or software stored on its computers or passing through its network, and caused a "splash screen" to appear at each start-up, warning its employees that all e-mails on the system were presumed to be public records, contained no right of privacy or confidentiality, and were subject to inspection by the university at any time, as deemed necessary to protect its business concerns.[15]

Some courts have held that even an informal acknowledgment that electronic correspondence may be subject to disclosure can constitute a waiver of an expectation of privacy in that correspondence. In *Pulaski County v. Ark. Democrat-Gazette, Inc.*,[16] a County comptroller, Quillin, was arrested for allegedly embezzling money from the County. He had been romantically involved with "Jane Doe," an outside contractor with the County. When a newspaper applied under a freedom of information law to have the County produce the comptroller's e-mail messages, including messages between him and Doe, Doe contested the disclosure of the e-mails, claiming it was a violation of her privacy. The trial court ruled that Doe had no expectation of privacy when conversing with Quillin on a County computer or using the contractor's business e-mail. The Supreme Court of Arkansas affirmed. Because the contractor had acknowledged in the correspondence—sent from her work e-mail account and accessed by Quillin on his County-issued computer—that she knew the e-mails could become public, she had effectively waived her expectation of privacy in the e-mails, despite the fact that some of the e-mails contained discussions of matters of a personal and private nature.[17]

Municipal employers who adhere to clear policies regarding their employees' lack of expectation of privacy in electronic communications can further protect their ability to access such communications by keeping any review as narrowly tailored and as minimally invasive as possible.

Appropriate Purpose and Scope

Municipal employers who adhere to clear policies regarding their employees' lack of expectation of privacy in electronic communications can further protect their ability to access such communications by keeping any review as narrowly tailored and as minimally invasive as possible. Courts have found that employers who properly informed their employees of their policies regarding electronic communications did not invade their employees' privacy when reviewing electronic materials, as shown by the following scenarios:

- Where the employer demonstrated that it had a legitimate business interest in reviewing the electronic communications, such as ensuring that the employee was not engaging in unauthorized activity that would harm the employer.[18]
- Where a review of the electronic communications and computer files was done remotely and was limited to materials accessible from, and available on, the employer's server, even in instances where the items on the server included e-mails saved from the employee's personal e-mail account, those saved in folders that the employee had designated "private," or those that were password-protected by the employee.[19]
- Where a review of computer files was conducted on a former employee's company-issued laptop, one that the employee believed he had the option to purchase upon termination, and where the review was conducted by a single person and did not include a search for, or audit of, the employee's personal e-mail account, information, or pictures.[20]

The Stored Communications Act

As use of wireless devices, text messaging, and other forms of electronic communication becomes more widespread in the workplace, it is important for municipal employers to keep themselves apprised of their rights in monitoring such communications. The Stored Communications Act (SCA) prevents a provider of communications services from divulging the content of correspondence sent and received through its servers to anyone except the sender and the addressee, without the lawful consent of the same. As a result, municipalities that purchase BlackBerry or cell phone service for their employees may not be entitled to request, from the service providers, transcripts of their employees' communications using those devices.[21]

Although the SCA provides that employers do not have an absolute right to review the content of text messages, employers can, nevertheless, discourage personal use of these services by implementing a clear, consistent policy prohibiting using the devices for personal, offensive, or other inappropriate purposes. A possible additional safeguard might be to require employees to sign written waivers of any expectation of privacy in their electronic communications on such devices, and even sign agreements permitting the employer to access the provider's records for those accounts.

Indeed, recent caselaw in the wake of *Quon* suggests that city employees who are advised that their text

continued on page 16

 cont. from page 15

messages on a city's communications system are public information are not able to use the SCA to shield their communications. In *Flagg v. City of Detroit*,[22] the City of Detroit entered into a contract for text-messaging services with a non-party service provider, SkyTel, Inc., which provided messag-ing devices and corresponding services to various City officials and employees. The plaintiff sought production of the text messages sent and received on these City-issued devices from SkyTel. However, the City officials and employees had previously been issued a directive that "they should 'assume as a rule of thumb that any electronic communication created, received, transmitted, or stored on the City's electronic communication system is public information, and may be read by anyone,'" that such communications "should not be 'considered, in whole or in part, as private in nature,'" and that the employees should "bear in mind that, whenever creating and sending an electronic communication, they are almost always creating a public record which is subject to disclosure" under the applicable state freedom of information statutes.[23] The court determined that, because the employees had been given this directive, they impliedly consented, for the purposes of the SCA, to the production of their text messages by the service provider.[24]

Conclusion

As more and more employees rely on mobile e-mail and text messaging in their daily business, municipal employers must remain current about the law and about how to preserve their ability to monitor employee electronic communications. Although such safeguards may, at first glance, seem unnecessary or excessive, the reality is that municipal employers have a compelling interest in preventing employee misconduct and the misuse of municipal time and resources. Taking a few simple steps to help employees understand that their communications on employer-provided equipment are not private and are subject to employer review will ensure that the electronic services provided to municipal employees will help your municipality, not harm it.

Notes

1. 529 F. 3d 892 (9th Cir. 2008). On Jan. 27, 2009, the Ninth Circuit denied en banc review.
2. 18 U.S.C. § 2701 *et seq.* (West 2008).
3. U.S.C.A. Const. Amend. IV (made applicable to state government by U.S.C.A. Const. Amend. XIV); *see also,* O'Connor v. Ortega, 480 U.S. 709 (1987) (searches and seizures by government employers or supervisors of private property of their employees are subject to restraints of the Fourth Amendment).
4. 5 U.S.C. § 551 *et seq.* (West 2008).
5. *See, e.g.,* New York Freedom of Information Law, N.Y. PUB. OFF. LAW § 84 *et seq.* (McKinney 2008); California Public Records Act, CAL. GOV'T CODE § 6250 *et seq.* (West 2008); Illinois Freedom of Information Act, 5 ILL. COMP. STAT. ANN. 140/1 *et seq.* (West 2008); Florida Public Records Act, FLA. STAT. ANN. § 119.*01 et seq. (West 2008).*
6. *See, e.g.,* Pennington v. Clark, 16 A.D.3d 1049, 791 N.Y.S.2d 774 (N.Y. App. Div. 2005) (New York's Freedom of Information Law defines "public records," for the purposes of disclosure, as any information kept by an agency, regardless of the function or purpose for which such information is held).
7. In re Asia Global Crossing, Ltd., 322 B.R. 247 (S.D.N.Y. 2005); Curto v. Medical World Communications, Inc., No. 03CV6327 (DRH)(MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006); Sprenger v. Rector and Bd. of Visitors of Virginia Tech., No. 7:07cv502, 2008 WL 2465236 (W.D.Va. June 17, 2008).
8. Quon v. Arch Wireless Operating Co., Inc., 529 F. 3d 892, 904 (9th Cir. 2008) (citing O'Connor *v. Ortega*).
9. Nos. 272898, 275979, 276054, 276257, 2008 WL 2668298 (Mich. Ct. App. July 8, 2008).
10. *Id.* at *9.
11. No. CIV.A.01-3386, 2002 WL 1067442 (E.D. Pa. May 29, 2002).
12. *Id.* at *8.
13. *Id.*
14. 281 F. 3d 1130 (10th Cir. 2002).
15. *Id.* at 1132-33. The case involved a prosecution for possession of child pornography, and the employer's policy also prohibited employees from using computers to "access obscene material as defined by Oklahoma or federal law." *Id.* at 1132.
16. 264 S.W.3d 465 (Ark. 2007).
17. *Id.* at 467-68. The court pointed to one particular e-mail exchange between Quillin and Doe as evidence that Doe lost any expectation of privacy and knew the risk that the e-mails could become public. The sexually explicit exchange included Doe's response: "Hey now. This is work email, goofball!", with Quillin responding: "Delete, delete, delete...."
118. Hilderman v. Enea TekSci, Inc., 551 F. Supp.2d 1183 (S.D. Cal. 2008).
19. *See* Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004); McClaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. Ct. App. May 28, 1999).
20. *Hilderman,* 551 F. Supp.2d at 1203-04 (no evidence that the employer used the laptop to access the employee's private e-mail account or to otherwise "pry" into his personal affairs).
21. This prohibition depends on the exact technology being used (e.g., does the municipality use a BlackBerry Enterprise Server?) and whether the communications at issue run through the municipality's servers in any way.
22. 252 F.R.D. 346 (E.D. Mich. 2008).
23. *Id.* at 364-5.
24. *Id.* ("In light of this directive, a strong case can be made that City employees have given their implied consent to SkyTel's production of text messages to the City, at least under the circumstances presented here." The court added that, "[w]hatever any given City of Detroit employee might be able to say about his or her awareness of the City's electronic communications policy or any lack of rigor or consistency in its enforcement, such arguments are singularly ineffective—and, indeed, give cause for concern—when raised by two of the City's highest-ranking officials, at least one of whom unquestionably has policymaking authority for the City and authorized the policy in question." *Id.* at 365). The case involved the City and several individual defendants, including Christine Beatty—chief of staff to the now former mayor, Kwame Kilpatrick—seeking to prevent the disclosure on the basis of the SCA. ML