Wisconsin Lawyer

Vol. 72, No. 3, March 1999

Coping With the Legal Perils of Employee Email

Email communication between a company's employees, or with its clients and the public, is fast, easy - and potentially dangerous. Learn what steps companies are taking to protect themselves by regulating employee use of email and the Internet.

Editor's Note: *To view Wisconsin Statutes and Acts referenced in this article you must have and/or install Adobe Acrobat Reader 3.0 on your computer.*

By Michael McChrystal, William Gleisner & Michael Kuborn

Today, email can be created easily and transmitted with virtually no difficulty, either within a company or over the Internet. Email encourages an informality and directness of communication that is hard to achieve, even in person or over the telephone. It allows for the rapid dissemination of ideas, plans, documents, and images throughout a company or throughout the world literally at the touch of a (mouse) button. In short, this miracle of the information age appears to be just what business in our fast-paced world needs to compete and thrive.[1] Even lawyers are becoming convinced that email is the answer to communicating with counsel, the courts, and clients.[2]

However, consider for a moment the potential problems that email can create for a business or law firm,[3] and then ask yourself how does a business protect itself from those problems? For example, is a company liable when an employee sends harassing email, or downloads pornographic material from a Web site and distributes it to fellow employees? Can a company be held responsible if an employee sends

libelous email over the Internet? What if an employee is angry or malicious enough to send confidential information to competitors or anonymously post such information on the Internet? What if an employee decides to leave a job, but only after he or she emails confidential customer or client information or trade secrets outside the firm for improper postemployment use? In dealing with such problems, how does a business balance its needs against the privacy rights of its employees?

The difficulties of email communication are magnified a thousandfold because it is, in a very real sense, becoming ubiquitous. Email[4] is very rapidly becoming "the" way to communicate, within a business or over the Internet. According to an article by attorneys Mark S. Dichter and Michael S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications*,[5] published in early October 1996, 90 percent of all large companies, 64 percent of mid-size companies, and 42 percent of small businesses used internal email, and more than 40 million workers were corresponding via email. Within the span of two years, email use has increased dramatically. It's estimated that Internet users sent more than 6 billion email messages last year,[6] and it is estimated that worldwide there has been an explosion of business users on the Internet.[7] Internet email will grow exponentially as the worldwide use of email increases.[8] Moreover, the distinction between internal company email and Internet email is blurring, especially as more companies make Internet access available from desktop systems or via an Internet server using routers or similar technology.

Ease of use or abuse

The problems posed by email are very real and have resulted in very real liability for several companies. The very ease with which email can be created and disseminated appears to reduce a user's inhibitions.

An employer can be held liable for sexual or racial harassment perpetrated or furthered by email.[9] There is some suggestion that prompt action to remedy a hostile atmosphere thus created may exculpate the employer.[10] It would be dangerous for an employer to hope that it will escape liability merely because it does not know such harassment is ongoing, especially if the probability of such harassment is foreseeable.[11] Of course, email is just one of many vehicles by which offensive conduct may be communicated in the workplace. However, unlike other forms of misconduct, the average employer may have more difficulty detecting or preventing email harassment. Nevertheless, "a company will be liable if management-level employees knew, or in the exercise of reasonable care should have known, about a barrage of offensive conduct."[12]

Some courts have held employers subject to liability if an employee with apparent authority libels a third party or inflicts trade disparagement in the furtherance of his or her employer's business.[13] The problem for an employer who permits a large number of employees to send out email over the Internet from a company Internet server or from a company computer, lies not just in the fact that employees may be viewed as clothed with apparent authority. Especially if an employer also maintains a Web page, Internet email that travels across state and international boundaries may potentially subject an employer to the jurisdiction of foreign courts, with all of the difficulties and costs that inevitably attend the defense of an action far from the employer's

home jurisdiction.[14]

If an angry employee publishes confidential information anonymously over the Internet, or sends it to a competitor, the information loses its confidential protection and becomes part of the public domain.[15] Obviously, given the sophistication of today's Internet email systems, confidential information and trade secrets can be easily shared with unauthorized third parties.

Protecting against the misuse of email

Certainly, email abuse can and will occur. Unfortunately, guarding against such abuse is not easy. There will be a growing interrelationship between internal, or "intranet," email systems and Internet email systems in the years ahead, especially if companies such as Microsoft have their way.[16] The potential will soon exist for an uncomfortable transparency between an office environment and the Internet. Therefore, regardless of how companies police the email activities of employees, they must exercise considerable caution in implementing new technological solutions that permit employees extensive access to the Internet.

SideBar

- Sample Internet Use Policy

Federal Laws

- Electronic Communications Privacy Act of 1986 (ECPA)
- Telecommunications Act of 1996

Articles

- Electronic Interaction in the Workplace
- Security on the Internet
- Document Destruction and Confidentiality
- Invasions of Computer Privacy

While the need for employer policing or monitoring of employee email activity will become more important in the years ahead, such activity will have to be undertaken with extreme care. Although the Fourth Amendment and other constitutional proscriptions do not as a rule apply to private businesses,[17] there are both state[18] and federal[19] statutes that could be construed as prohibiting such monitoring on the grounds that it invades the privacy or protected labor law rights of employees.[20] There always have been limitations on the extent to which an employer can search or otherwise monitor employee activities at work,[21] and these cases often have been resolved on the grounds that an employer unreasonably invaded the employee's privacy.[22]

Courts have carved out exceptions to the monitoring of employee activity where a legitimate business purpose can be demonstrated,[23] and that includes the monitoring of email communications.[24] However, Congress has evinced a serious concern with the privacy of email,[25] including email generated in the workplace. The Electronic Communications Privacy Act of 1986 (ECPA) defines electronic communication in such a way that it can be construed as applying to email. According to the Act, electronic communication:

> "[includes] any transfer or signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate commerce."[26]

The ECPA makes it illegal to intentionally intercept, use, or disclose oral, wire, or electronic communications,[27] and it provides for criminal, civil, and injunctive relief, as well as attorney fees and other equitable relief.[28] It could be argued that the ECPA's definition does not apply to internal email systems, but the growing interrelationship between intranet and Internet email systems undoubtedly will render such a distinction virtually meaningless in the years ahead. There are several relevant exceptions to the application of the ECPA proscriptions. The most important exceptions are predicated on business necessity and consent.

The business exception to the ECPA

To the extent employees are using email at work via company computers, an employer may be justified in monitoring that email. While unlimited and indiscriminate monitoring is very hard to justify,[29] the courts will tolerate some monitoring. However, to the extent that "monitoring" involves the surreptitious interception or surveillance of employee email, monitoring activities will very probably find disfavor in the courts. By analogy to telephone wiretap cases, while occasionally permitted,[30] surreptitious interception or surveillance of employee telephone calls has not been received well by the courts.[31]The authors submit that any email monitoring should be done only after notifying employees that their email will be monitored.[32] While there may be a justifiable business reason for undisclosed monitoring, a business that does so runs a considerable risk.[33]

Next Page

Wisconsin Lawyer

Coping With the Legal Perils of Employee Email

The consent exception to the ECPA

If employees have received full notice that email monitoring may take place and have clearly and unambiguously consented to that monitoring, the employer's hand is strengthened considerably, providing the employer limits its monitoring to business-related email (in terms of email, an interesting problem in and of itself).[34] At minimum, this consent should be either explicit or very clearly inferable from the conduct of the parties.[35] While Congress intended that the ECPA consent requirement be construed broadly,[36] courts examine a claim of consent very carefully. According to the U.S. Court of Appeals for the First Circuit:

> "[Under the ECPA] consent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights. Of course, implied consent is not constructive consent. Rather, implied consent is 'consent in fact' which is inferred 'from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance.' Thus, implied consent - or the absence of it - may be deduced from 'the circumstances prevailing' in a given situation. The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts that tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of [the ECPA] - a purpose that suggests that consent should not casually be inferred."[37]

Incidentally, some commentators have suggested that an employer could argue it has the right to monitor email on the grounds that the employer is the provider of email service to its employees. While there is such an exception under both state[38]

and federal law,[39] it seems clear that this exception is intended to permit the technical administration of an email system and not the monitoring of the content of the email transmitted over that system.

Implementing a monitoring policy

The best, and perhaps the only, solution lies in establishing a monitoring plan based upon a carefully conceived email policy that is disseminated to all employees and agreed to by all employees. Several commentators have attempted to delineate the contents of such a policy.[40] Attorneys Dichter and Burkhardt have constructed a thoughtful outline of what such a policy should contain, and how it should be worded.[41] Whatever policy is decided upon, a physical copy should be given to all employees (not emailed to them[42]), and posted with other official legal notices to employees. Further, employees should be required to acknowledge, by their signature, receipt of and agreement with that policy.[43]

Several suggested policies directed toward employee use of email and the Internet are posted on the Web and on Westlaw.[44] However, the most complete and well-developed policy model the authors have found is the one crafted by attorneys Dichter and Burkhardt, which appears near the end of their online article entitled *Electronic Interaction in the Workplace: Monitoring, Retrieving, and Storing Employee Communications*.[45] A small portion of their suggested policy on email and Internet procedure appears as a sidebar to this article.

If an employer decides to implement such a monitoring policy, several other factors become important. First, as a practical matter, how does one actually monitor email or Internet use by employees? In the information age, it should come as no surprise that several companies are actively involved in developing software that will facilitate such employer monitoring of employee email usage.[46] The Equitrac Corporation, for example, introduced a new type of software at the beginning of 1997 that may assist an employer in monitoring employee email traffic and Internet usage. According to Equitrac:

> "Companies looking for a way to track Internet usage for billing and project management purposes should evaluate Equitrac Corporation's E.P.I.C. - Equitrac's Professional Internet Client - Internet client/server software tool. E.P.I.C. is a tracking, monitoring, and blocking Internet access tool enabling lawyers and other service professionals to track time spent online, monitor online research, and track email sent and received."[47]

Email is rapidly becoming a vehicle for intra-office communication that is as important, if not more important, than "snail" mail and hardcopy memoranda. Companies should begin to think seriously about retention and

Michael McChrystal, top, Marquette 1975, is a professor of law at the Marquette University Law School.

William Gleisner, middle, Marquette 1974, both a practicing attorney and computer consultant, maintains a law firm-based litigation support service bureau in Milwaukee.

Michael Kuborn, bottom, Marquette 1998, is with Olsen, Kloet, Gundersen & Conway, and is trained in computer recovery and computer search and seizure techniques. Products and services mentioned in this article should not be construed as an endorsement.

destruction policies regarding email, because email increasingly will become the subject of discovery. Indeed, there already have been cases involving discovery requests to inspect a company's computer hard drives for email,[48] and one only need consider the Microsoft antitrust litigation to recognize how devastating email can be even to a computer literate litigant.[49] In developing those email policies, however, remember that simply deleting office email from a hard drive may not result in its actual destruction.[50]

Conclusion

Nowhere are the legal challenges of the information age more clearly apparent than in the area of email communication. Inevitably, both lawyers and clients need to consider carefully how they are going to deal with both the benefits and the unavoidable risks presented by the growing use of email.

Wisconsin Lawyer Main

WisBar Main

Problems? Suggestions? Feedback? Email Wisconsin Lawyer

Wisconsin Lawyer

Vol. 72, No. 3, March 1999

Coping With the Legal Perils of Employee Email

Endnotes

[1]An article in *USA Today* reports:

> "Email has become so popular that many managers are using it more than the telephone for business communication. More than 35% of 400 managers polled say they use email the most of any communications tool, based on an April survey by the American Management Association and Ernst & Young. That beats the 26% who use the phone most frequently and 15% who rely on face-to-face meetings."

[2] R. Timothy Muth, Security on the Internet, 70 Wis. Law. 17 (Oct. 1997).

[3]This article is not concerned with possible viruses, spam email, or other similar potential dangers commonly associated with Internet browsing and email communication.

[4] Senate Report No. 99-541, which is the chief legislative source of the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510, et seq., defines email, or "electronic mail," in terms that could apply to both internal company or Internet email:

> "Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer 'mail box' until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system. Electronic

> mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence."

From Westlaw Online version of S. Rep. 99-541, p. 16-17.

[5]This article is located online. Attorneys Dichter and Burkhardt are with the Philadelphia office of Morgan, Lewis & Bockius LLP. Their scholarly article is recommended to anyone interested in the topic of this article.

[6] PBS Online

[7] International Communications Headcount.com

[8] "Unleash E-Commerce Now", an article from *Wired Magazine*. *See also* ZD-Net E-Business Homepage.

[9]*Harley v. McCoach*, 928 F. Supp. 533 (E.D. Pa. 1996); *Strauss v. Microsoft Corp.*, 814 F. Supp. 1186, 1193-94 (S.D. N.Y. 1993).

[10] *Harley*, 928 F. Supp. at 540.

[11] It appears that negligence and not strict liability continues to be the standard for determining whether an employer is liable for creating a hostile work environment, at least in the Seventh Circuit. According to an en banc determination of the court in *Jansen v. Packaging Corp. of America*, 123 F.3d 490 (7th Cir. 1997), "All the judges with the exception of Judges Easterbrook, Rovner, and Wood believe that negligence is the only proper standard of employer liability in cases of hostile-environment sexual harassment even if as here the harasser was a supervisor rather than a coworker of the plaintiff." *Id.* at 494.

[12]*Noble v. Monsanto Corp.*, 973 F. Supp. 849, 858 (S.D. Iowa 1997). *See* *Faragher v. City of Boca Raton*, 118 S. Ct. 2275, 2292-93 (1998), wherein the U.S. Supreme Court stated:

> "In order to accommodate the principle of vicarious liability for harm caused by misuse of supervisory authority, as well as Title VII's equally basic policies of encouraging forethought by employers and saving action by objecting employees, we adopt the following holding in this case and in *Burlington Industries Inc. v. Ellerth*, ante, ___ U.S. at ___, 118 S. Ct. at ___, also decided today. An employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor with immediate (or successively higher) authority over the employee. When no tangible employment action is taken, a defending employer may raise an affirmative defense to liability or damages, subject to proof by a preponderance of the evidence. *See* Fed. Rule Civ. Proc. 8(c). The defense comprises two necessary elements: (a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise. While proof that an employer had promulgated an antiharassment policy with complaint procedure is not necessary in every instance as a matter of law, the need for a stated policy suitable to the employment circumstances may appropriately be addressed in any case when litigating the first element of the defense."

[13]*Paine Webber Jackson and Curtis Inc. v. Winters*, 579 A.2d 545, 548 (Conn. App. 1990).

[14] While the law is unsettled and still in a state of flux, the existence of a Web page can be sufficient to subject a company to the jurisdiction of a foreign tribunal. *Heroes Inc. v. Heroes Found*, 958 F. Supp. 1, *4 (D.D.C 1996); *cf. Inset Sys. Inc. v. Instruction Set Inc.*, 937 F. Supp. 161, 164 (D. Conn. 1996). Where a company responded to "hits" from out-of-state visitors to its Web page by sending out email across state lines, at least one court found that the Web page and email responses were sufficient to confer jurisdiction over that foreign company. *Maritz v. CyberGold Inc.*, 947 F. Supp. 1328, 1333 (E.D. Mo. 1996) ("CyberGold automatically and indiscriminately responds to each and every Internet user who accesses its Web site. Through its Web site, CyberGold has consciously decided to transmit advertising information to all Internet users, knowing that such information will be transmitted globally.").

[15] *Castano v. American Tobacco Co.*, 896 F. Supp. 590 (E.D. La. 1995).

[16] Consider the following description of the new Microsoft Office 2000:

> "With Office 2000, you can save Office documents in HTML file format and retain the fidelity of your native Office file format. By saving as HTML, you ensure that anyone with a Web browser can view your documents. Office 2000 also simplifies publishing your Office documents to your intranet or to an Internet site. New File Open and File Save dialog boxes make saving documents to a Web server as easy as saving them to your hard disk or to a file server."

Quoted from Microsoft Office 2000 WWW site.

[17] *See, e.g., Jackson v. Metropolitan Edison Co.*, 419 U.S. 345, 453 (1974); *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

[18]*See, e.g.*, Wis. Stat. § 895.50.

[19] Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, *et seq.*

[20] There are other reasons why an employer needs to be cautious about how it treats employee email. For example, the NLRB recently ruled that employee email could be found to be a protected activity. 14 Comp. Law. 22 (September 1997).

[21] *K-Mart Corp v. Trotti*, 677 S.W.2d 632, 634-35, 640-41 (Tex. Ct. App. 1984) (where an employer was found liable for $100,000 for conducting a search of an employee's locker on a suspicion of wrongdoing); *cf. Doe v. Kohn, Nast & Graf*, 862 F. Supp. 1310, 1326 (E.D. Pa. 1994) (involving the searching of an attorney's desk by his partner).

[22] *K-Mart*, at 638.

[23]*Saldana v. Kelsey-Hayes Co.*, 443 N.W.2d 382, 384 (Mich. App. 1989); *Simmons v. Southwestern Bell Tel.*, 452 F. Supp. 392, 394 (W.D. Okla. 1978). Even public employers can monitor employees or search their workspaces if there is a legitimate business reason for such searches, although the Fourth Amendment obviously increases the extent of an employee's right to privacy. *See, e.g., O'Connor v. Ortega*, 480 U.S. 709, 719-20 (1987).

[24] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (Despite the fact that an employer assured employees that email communication would be private [*Id.* at 98], the employer escaped

liability because the employee who was terminated after the company searched for and found offensive email was an at will employee.). *Id.* at 101.

[25] Regardless of privacy issues, it would seem that an employer will be protected if the employer attempts to block employee access to pornographic, violent, harassing, or otherwise objectionable Web sites or third-party email sent into a company, under the Good Samaritan exception to the Telecommunications Act of 1996, 47 U.S.C. § 230, which provides in pertinent part:

> "No provider or user of an interactive computer service shall be held liable on account of -
> "(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> "(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)."

[26] 18 U.S.C. § 2510 (5). While it could be argued that the quoted definition does not reach email, it is clear from the legislative history underlying this Act that it was intended to reach email. *See, e.g.*, the quoted language from Senate Report No. 99-541, reproduced *supra* at footnote 4.

[27]18 U.S.C. §§ 2510-2522; 2701-2711, 3121-3127.

[28]18 U.S.C. §§ 2511, 2520.

[29]*Cf. Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 741 (4th Cir. 1994).

[30]*Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983) ("[T]he general rule seems to be that if the intercepted call was a business call, then Berry Co.'s monitoring of it was in the ordinary course of business." *Id.* at 582).

[31] *Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992).

[32] *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979).

[33] In addition to the ECPA, consider the terms of Wis. Stat. section 968.31, which proscribes the interception of wire and electronic communication, that contains exceptions similar to those found in the ECPA. According to section 968.31 (2):

> "(2) It is not unlawful under §§ 968.28 to 968.37:
> "(a) For an operator of a switchboard, or an officer, employee or agent of any provider of a wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication to intercept, disclose or use that communication in the normal course of his or her employment while engaged in any activity which is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the provider of that service, except that a provider of a wire or electronic communication service shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

> "(b) For a person acting under color of law to intercept a wire, electronic or oral communication, where the person is a party to the communication or one of the parties to the communication has given prior consent to the interception."

[34] *Cf. Watkins v. L.M. Berry & Co.*, 704 F.2d at 583.

[35]*Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992) ("[c]onsent under [the ECPA] is not to be cavalierly implied.... [K]nowledge of the capability of monitoring alone cannot be considered implied consent.").

[36]*Griggs-Ryan v. Connelly*, 904 F.2d 112, 116 (1st Cir. 1990); *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987).

[37]*Griggs-Ryan v. Connelly*, 904 F.2d at 116-17.

[38] *See* Wis. Stat.§ 968.31 (2), *supra.*

[39] *Cf. United States v. Mullins*, 992 F.2d 1472, 1478.

[40]*See, e.g.*, Brown, *Developing Internet, Intranet and Email Policies*, 520 PLI/Pat 347 (July 1998); Ballon, *The Emerging Law of the Internet*, 507 PLI/Pat 1163, 1270-73 (Feb. 1998); Ciapciak and Matuszak, "Employer Rights in Monitoring Employee Email," *For the Defense* (Nov. 1998).

According to Ballon, *Alternate Corporate Responses to Internet Data Theft*, 471 PLI/Pat 737, 750-751:

> "Companies should adopt and enforce email and Internet use policies. Companies should adopt Internet policies [in order] (i) To negate any expectation of privacy employees might otherwise have. (ii) To limit liability under the Telecommunications Act of 1996. By taking affirmative action to monitor email transmissions for offensive conduct, a company may be able to avoid indirect liability for third party violations of state law (such as sexual harassment and defamation) under the Good Samaritan exemption created by the Telecommunications Act of 1996. [A]n Email Policy [should specify that] (i) The company owns the computer system and all data stored on or transmitted over company networks. (ii) The employee has no right to privacy in any information stored on the system. The employer reserves the right (but does not assume the obligation) to monitor employee email. (iii) Define categories of email that should be retained in the ordinary course of business and specific procedures for retaining such communications. (iv) Purge all other email messages at regular intervals."

[41] This article is located online. *Supra.*

[42]*See In re Prudential Ins. Co. Sales Practices Litigation*, 169 FRD 598 (D. N.J. 1997), where the court found that distribution by email was an ineffective method of distributing a company policy. *Id.* at 603-04.

[43] *Id.*

[44] *See supra* note 40.

[45] This article is located online.

[46] Companies such as Equitrac and Sequel Technology. *See*

[47] From the Equitrac Web page

[48] *See, e.g.*, *Fennel v. First Step Designs Ltd.*, 83 F.3d 526 (1st Cir. 1996), involving a request to examine an employer's hard drive for the purposes of learning whether a particular email memorandum had been predated to avoid liability. *Id.* at 532-33.

[49] *See Law Journal Extra: United States v. Microsoft,* specifically a Nov. 3, 1998, story, wherein it is reported, "Gates seemed most argumentative on the [video] tape [of his deposition by Government lawyers] when questioned about a June 23, 1996, [email] memo he wrote to Paul Maritz and Brad Silverberg, two top Microsoft executives. The email describes a meeting Gates had two days prior with Apple executives."

[50] *See* McChrystal, Gleisner, and Kuborn, *Document Destruction and Confidentiality,* 71 Wis. Law. 25 (Aug. 1998).

Wisconsin Lawyer Main

WisBar Main

Problems? Suggestions? Feedback? Email Wisconsin Lawyer
