

Ethical Lawyering in the "Wireless Handheld" Age

BY JEREMY R. FEINBERG

Admit it. You have one, and you love using it. Wireless handheld devices, from the Blackberry to the Treo, have become an everyday part of an urban professional's life. For many lawyers, these gadgets are indispensable tools in their legal practice. They also present additional dangers for the unwary. A lawyer who loses or misplaces her wireless handheld risks waiving attorney-client privilege or work product protection. She could even face professional discipline for failure to safeguard client property and the related breach of the duty of confidentiality. This article will analyze the resulting ethical issues presented by the increased use of this technology and recommend a set of simple precautions to prevent reliance on wireless handhelds from becoming a professional crisis, even if accidents do happen.

Advantages and Disadvantages of Wireless Handhelds

Wireless handhelds enable more productive and efficient client service through increased responsiveness and the ability to stay abreast of e-mails and their attachments while away from the office. The instant gratification of receiving and reviewing e-mails and their attachments from anywhere at any time has a surprisingly intoxicating effect on even the most powerful of minds, earning the devices the nickname "Crackberry." One man described his excessive wireless handheld use: "I would actually answer my e-mails at two o'clock in the morning," he said. "I'd be doing e-mails and brushing my teeth." (Dan Harris, 'Crackberry Addiction,' Gadget Users Compared to Drug Users for Excessive Behavior, ABCNews.com, August 23, 2006, available at <http://abcnews.go.com/WNT/Technology/story?id=2348779>.)

Experts say that the potential to develop an actual addiction to these communication devices exists, "because they can make people feel disconnected," comparing excessive wireless handheld use with alcohol, drug and gambling addictions. *Id.*

The dangers of overuse aside, failure to practice caution when handling the information contained in these devices risks disastrous consequences, and the dangers of accidentally disclosing confidential and sensitive information are all too real. An on-line news source speaks of a 2003 incident in which an officer at a major financial institution left his job and, without clearing his wireless handheld's memory, sold it in an online auction. The buyer quickly learned that along with the new handheld, he had also purchased a trove of confidential corporate data: 200 internal company e-mails and a "database of more than 1,000 names, job titles..., e-mail addresses and phone numbers." (Kim Zetter, *Blackberry Reveals Bank's Secrets*, WIRED, August 25, 2003, available at <http://www.wired.com/news/business/0,1367,60052,00.html>.)

It is not hard to envision mishaps, even if not as reckless as this reported one, in the context of legal practice. Consider the following all-too familiar stories: an attorney receives confidential documents from a client as e-mail attachments. After the attorney reviews the e-mail and attachments while on the road, the wireless handheld slips out of the attorney's pocket and is lost where a stranger retrieves it. Or suppose in crafting a confidential e-mail to a client, the attorney over-relies on the auto-complete feature on a wireless handheld and, not checking, allows it to misaddress an e-mail, intended for the client, to a third party.

Certainly, any client whose confidential information fell into the wrong hands through an attorney's carelessness would not be happy. But the consequences of losing or misusing a wireless handheld, for both the attorney and the client, could go far beyond mere embarrassment. First, the attorney might waive the attorney-client privilege or work product protection. In some instances, such a waiver could have far greater reach and implications than the documents actually viewed. Second, the attorney may violate her duty of confidentiality and may even be subject to professional discipline.

New technological innovations significantly raise the stakes. Wireless handheld software now makes it possible to access and input time-entries and read and edit documents on a document management system remotely, creating a virtual window into the lawyer's (and her offices) entire business.

See, e.g., <http://www.handango.com/blackberry/PlatformProductDetail.jsp?siteId=1181&osId=950&jid=3A77B546X9B8DEBAXDB4D5D6A79AE1D3§ionId=0&catalog=0&productType=2&platformId=5&productId=193283>.

No client would want to leak to the public the number of hours and the description of the work attorneys were doing for it on a confidential matter. Nor would the client want to face the prospect of exposing hundreds of thousands of files-an entire firm's work product, extending back for years-to an adversary or a member of the public.

Consequences of Losing (or Misusing) A Wireless Handheld

Would a court hold that sloppy use and care of a wireless handheld could waive attorney-client privilege or work product protection? It just might. In order to determine whether privilege has been waived by inadvertent disclosure, such as the kind that might happen through errors in the use of wireless handhelds, New York federal and state courts apply multi-factor tests that focus heavily on whether and how the attorney took steps to (a) prevent inadvertent disclosure, and (b) rectify disclosure after the matter has been discovered. Thus, inadvertent disclosure waives privilege in the Second Circuit when the party's conduct was so careless as to suggest that it was not concerned with the protection of the...privilege.

In determining whether the production was inadvertent, courts consider (1) the reasonableness of the precautions taken to prevent inadvertent disclosure, (2) the time taken to rectify the error, (3) the scope of the discovery and extent of the disclosure and (4) overarching issues of fairness.

In re Natural Gas Commodity Litigation, 229 F.R.D. 82 (S.D.N.Y.2005), citing *Lois Sportswear, USA, Inc. v. Levi Strauss & Co.*,104 F.R.D. 103, 105 (S.D.N.Y. 1985) (first establishing the standard test for analyzing issues of waiver). The rule is similar under New York state law. See, *Campbell Aerospace Products Intern*, 37 A.D.3d 1156 (4th Dep't 2007); *Baliva v. State Farm Mut. Auto. Ins. Co.*, 275 A.D.2d 1030 (4th Dep't 2000). Thus, a careful attorney may avoid waiver even in the event of inadvertent disclosure, but a sloppy one may not. The following cases illustrate the courts' application of this test.

In *United States v. Rigas*, 281 F. Supp. 2d 733 (S.D.N.Y. 2003), the court upheld assertions of work product privilege as to documents revealed to the adversary through a failure to safeguard a computer. The Government turned over a hard drive which inadvertently made a paralegal's entire electronic database available to the defendant for copying. The database contained memoranda of law, "grand jury material, confidential law enforcement information and [the paralegal's] own work product relating not only to the

[instant] matter but to a number of other cases...." *Id.* at 736.

The court upheld work product privilege as to these documents because the Government had taken reasonable precautions to prevent disclosure, including the storage of the files on a password-protected account and a secure server, and asserting work product protection on the same day it discovered that the documents had fallen into the wrong hands. *See, also, Campbell Aerospace*, 37 A.D.3d, *supra*, at 1157. (Because plaintiffs' attorneys took reasonable precautions to prevent the disclosure and asserted privilege within one day of the discovery of inadvertent disclosure, plaintiff did not waive the attorney-client privilege.)

By contrast, in *S.E.C. v. Cassano*, 189 F.R.D. 83, 85 (S.D.N.Y.1999), the court held that the S.E.C. waived its work product protection as to inadvertently disclosed documents. *Id.* at 86. In that case, although an attorney had ostensibly screened the 50 boxes of materials made available to defendants in order to remove any privileged documents, defense counsel discovered a memorandum exhaustively describing the SEC's assessment of the case. *Id.* at 83-84. When defense counsel requested a copy of this single document, SEC's counsel complied without first examining the document, and did not examine the document or discover the disclosure until 12 days later. *Id.* at 84-85. The court held that in view of counsel's failure to take the reasonable precaution to examine the document before copying it, and in view of the long delay between disclosure and discovery of the error, any protection as to the document was waived. *Id.* at 85-86.

A court could, if presented with the issue, apply the test illustrated above and hold that a waiver occurred if a lawyer does not appropriately protect the data on her wireless hand-held. But that's not the only risk. Lawyers who use wireless handhelds without reasonable precautions risk violating their duty of confidentiality to clients, and thereby exposing themselves to "pain of professional discipline including loss of their license to practice law." *Madden v. Creative Services, Inc.*, 84 N.Y.2d 731 (1995), citing DR 4-101 and EC 4-4.

In DR 4-101(B), the New York Code of Professional Responsibility prohibits lawyers from "knowingly" revealing their clients' confidences and secrets. The importance of the duty of confidentiality between a lawyer and her client is a bedrock principle to the proper functioning of the legal system. *See*, EC 4-1. Because of the precedence placed on this ethical obligation, Courts and ethics opinions have, despite the word "knowingly," interpreted DR 4-101(B) broadly and in concert with other rules, to include even inadvertent disclosures.

In one such instance, the First Department affirmed public censure of an attorney who negligently delivered confidential documents to the media. Although the attorney did not know that the documents were under seal, he had failed to inquire as to their status. The Court found that the attorney violated his duty to his client by failing to take "ordinary precautions," reasoning that "whether [respondent] acted recklessly or negligently does not matter since, either way, respondent's failure to take adequate precautions to safeguard confidential materials of a client, even if considered unintentional, was careless conduct that reflects adversely on his fitness to practice law." *In re Holley*, 285 A.D.2d 216 (1st Dep't 2001). As the *Holley* case noted, the purpose of the sanction was "not to punish but to protect the public through notice to the profession" that certain precautions and safeguards are expected in regards to an attorney's duty to his or her client. *Id.* at 218.

Similarly, the Committee on Professional Ethics of the New York State Bar Association has recognized that "an attorney must use reasonable care to protect client confidences and secrets." N.Y. State Eth. Op. 709 (1998) [*citing* DR 4-101(B), DR 4-101(D) (requiring reasonable care to prevent employees and others from disclosing client confidences and secrets), and EC 4-4 (attorneys "should... act in a manner which preserves the evidentiary privilege")]. That Committee has even specifically expressed that "a lawyer who uses technology to communicate with clients must use reasonable care with respect to such communication." This "may, in some circumstances, call for the lawyer to stay abreast of technological advances." N.Y. State Eth. Op. 782 (2004). Indeed, another ethics opinion has recognized the dangers to confidentiality that current technology can cause and has outlined steps that lawyers can take to avoid inadvertent disclosure. See, ABA Formal Opinion 06-442 (August 5, 2006).

If a lawyer like the one in *In re Holley* could be censured for negligently handling paper documents by failing to observe "ordinary precautions," it is not a stretch to see how a disciplinary committee could target a lawyer who did not use, or who did not know how to use, a wireless handheld properly.

What's a Handheld-Toting Lawyer to Do?

There is thus a dual incentive for lawyers to be careful with their wireless handhelds: for their clients' sake and their own. The good news is that lawyers who take reasonable precautions can guard against both sets of potential consequences simultaneously. The following best-practice recommendations, all of which should be intuitive and simple to implement with the help of a law office's IT department and/or the handheld's instruction manual, may go a long way toward managing the risks.

Activate the wireless handheld's password feature, so that only intended users can access the device.

Consistent with document retention policies and any "litigation holds," regularly delete or transfer old e-mails stored on the device, so that fewer e-mails and attachments are vulnerable to disclosure in the event of loss or theft.

Do not compose or read e-mails if others nearby can look over your shoulder. Attorneys would never allow complete strangers to watch them type an e-mail from their office's desktop computer, and they should similarly guard against this possibility when using their wireless handheld in public.

Similarly, remember a wireless handheld is not a "toy." Do not let children or others without the right to see privileged material use the device to play games or access the Internet.

Affix a physical notice to the wireless handheld, stating that the information therein is confidential, and providing contact information for return in the event of loss. Add a similar electronic notice to the device's "home" screen. Nothing would be worse than for a well-intentioned Good Samaritan to accidentally deliver the wireless handheld to the lawyer's adversary, thinking that he was the rightful owner.

Ensure that the same confidentiality notice appended to e-mails sent from the attorney's desktop computer is used for e-mails sent from the attorney's wireless handheld.

Turn off the auto-complete feature on the wireless handheld, which can be particularly dangerous with smaller keyboards. At a minimum, be extra careful and double-check any e-mail composed using this

feature to ensure it is directed to the right recipients.

Know what you need to do to quickly stop the stream of data to lost devices, as you would cancel a lost credit card. Such a procedure should also promptly terminate access to the wireless device's ability to access time-entry and document management software.

Make sure that your office has a protocol to erase sensitive data on departing attorneys' wireless handhelds, particularly if the attorneys are permitted to keep the devices when they switch jobs, or leave.

Conclusion

Mistakes are going to happen. (Readers may or may not be surprised to learn that the author of this article has already had more than one near-miss on losing his wireless handheld.) But by taking the simple precautions outlined above, attorneys can prevent innocent mistakes from mushrooming into waivers of privilege, breaches of confidentiality, and exposure to professional discipline.

Jeremy R. Feinberg is the Statewide Special Counsel for Ethics for the New York Unified Court System. He would like to thank Rebecca Adams of the Office of Court Administration, and his former colleague, Isaac Nesser for their superb assistance with the preparation of this article. The views expressed in this article are those of the author only and are not those of the Office of Court Administration or Unified Court System.