New York State Bar Association

Committee on Professional Ethics

Opinion 749 – 12/14/01

Topic: Use of computer software to surreptitiously examine and trace e-mail and other electronic documents

Digest: Lawyers may not ethically use available technology to surreptitiously examine and trace e-mail and other electronic documents.

Code: DR 1-102(A)(4), DR 1-102(A)(5), DR 4-101, DR 7-102(A)(8), Canon 4, Canon 7, EC 4-1

BACKGROUND

Modern computer technology enables sophisticated users who receive documents by electronic transmission to "get behind" what is visible on the computer screen and determine, among other things, revisions made at various stages, and sometimes even the authors of the revisions. Use of this technology would enable a lawyer who receives e-mail and electronic documents from counsel for an opposing party to obtain various kinds of information that the sender has not intentionally made available to the lawyer. For example, a lawyer who has received the final draft of a contract from counsel for a party with whom the lawyer is negotiating would be able to see prior drafts of the contract and, perhaps, learn the identity of those who made the revisions, without the knowledge or consent of the sending lawyer. How to effectively "block" recipients from access to deletions and prior versions of the "visible" document appears to be unclear and a matter of debate among sophisticated computer users. *See, e.g.,* M. David Stone, "Deleting Your Deletions," P.C. Magazine November 20, 2000.

It is also possible for an e-mail sender to determine the subsequent route of the e-mail, including comments on the e-mail written by its ultimate recipients. Through use of this application a lawyer can place a "bug" in e-mail he or she sends to opposing counsel and learn the identity of those with whom the first recipient shares the message and comments that these persons may make about it. Even if a user can avoid applications that make it possible to place a bug in the user's e-mail, the recipient's forwarded messages can still be traced if the user forwards the message to someone who has not

taken these measures. Accordingly, it is virtually impossible to render one's e-mail system "bug-proof". *See* www.privacyfoundation.org/privacywatch, "E-Mail Wiretapping", posted February 5, 2001.

QUESTION

May a lawyer ethically may use available technology to surreptitiously examine and trace e-mail and other electronic documents in the manner described?

OPINION

This new technology permits a user to access confidential communications relating to another lawyer's representation of a client, including "confidences" and "secrets" within the scope of DR 4-101 of the Lawyer's Code of Professional Responsibility ("Code")[1] For this reason, we conclude that the use of computer technology in the manner described above constitutes an impermissible intrusion on the attorney-client relationship in violation of the Code. The protection of the confidences and secrets of a client are among the most significant obligations imposed on a lawyer. As explained in EC 4-1:

> Both the fiduciary relationship existing between lawyer and client and the proper function of the legal system require the preservation by the lawyer of confidences and secrets of one who has employed or sought to employ the lawyer. A client must feel free to discuss anything with his or her lawyer and a lawyer must be equally free to obtain information beyond that volunteered by the client. . . .The observance of the ethical obligation of a lawyer to hold inviolate the confidences and secrets of a client not only facilitates the full development of facts essential to proper representation of the client but also encourages non-lawyers to seek early legal assistance.

Although the precise question presented in this inquiry has not previously been answered by this Committee or, to our knowledge, by other ethics authorities, we believe the circumstances described are substantively analogous to less technologically sophisticated means of invading the attorney-client relationship that we and other authorities have addressed and rejected as inconsistent with the ethical norms of the profession. For example, the strong public policy in favor of protecting attorney-client confidentiality is expressed in the prohibition against lawyers (1) soliciting the disclosure of unauthorized communications, *see, e.g., Dubois v. Gradco Sys., Inc.,* 136 F.R.D. 341, 347 (D. Conn. 1991) (Cabranes, J.) (Although former employees of adverse corporate party are not within reach of the no-contact rule "it goes without saying that plaintiff's counsel must take care not to seek to induce or listen to disclosures by the former employees of any

[1] The Code defines "confidence" as "information protected by the attorney-client privilege under applicable law"; the term "secret" includes all "other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client." DR 4-101(A).

privileged attorney-client communications to which the employee was privy"); *see also* ABA Formal Op. 91-359; (2) exploiting the willingness of others to undermine the confidentiality principle, *see* N.Y. State 700 (1997); ABA Formal Op. 94-382; and (3) making use of inadvertent disclosures of confidential communications, *see* ABA Formal Op. 92-368.

The Code prohibits a lawyer from engaging in conduct "involving dishonesty, fraud, deceit or misrepresentation," DR 1-102(A)(4) and "conduct that is prejudicial to the administration of justice." DR 1-102(A)(5). We believe that in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine or that may otherwise constitute a "secret" of another lawyer's client would violate the letter and spirit of these Disciplinary Rules. *Accord MMR/Wallace Power & Indus. Inc. v. Thames Assocs.*, 764 F. Supp. 712, 718-19 (D. Conn. 1991) (spirit if not the letter of ethical rules precludes an attorney from acquiring, inadvertently or otherwise, confidential information about his adversary's litigation strategy); *In re Wisehart,* 721 N.Y.S. 2d 356*,* 281 A.D. 2d 23, (1st Dep't 2001) (respondent suspended for two years for using documents purloined by his client from opposing counsel); N.Y. City 1989-1 (client's interception of adversary's communications with counsel involved dishonesty and deceit; lawyer may not help client take advantage of such wrongdoing).

In the present inquiry, although counsel for the other party intends the lawyer to receive the "visible" document, absent an explicit direction to the contrary counsel plainly does not intend the lawyer to receive the "hidden" material or information about the authors of revisions to the document. To some extent, therefore, the "inadvertent" and "unauthorized" disclosure cases provide guidance in the present inquiry.

In N.Y. State 700 (1997), we concluded that a lawyer who receives an unsolicited and unauthorized communication from a former employee of an adversary's law firm may not seek information from that person if the communication would exploit the adversary's confidences or secrets. Despite the fact that the Code does not expressly require a lawyer to refrain from encouraging a breach of client confidentiality by opposing counsel's staff, we determined that because use of such information would undermine confidentiality and the attorney-client relationship, it was conduct "involving dishonesty, fraud, deceit or misrepresentation," DR 1-102(A)(4), and "conduct prejudicial to the administration of justice." DR 1-102(A)(5).

In N.Y. State 700 we cited ABA Formal Op. 92-368 in support of our conclusion that the strong public policy in favor of confidentiality outweighed what might be seen as the competing principles of zealous representation (Canon 7) and encouraging more careful conduct. ABA 92-368 concluded that a lawyer who receives confidential materials under circumstances where it is clear that they were not intended for the receiving lawyer (a) should not examine the materials once the inadvertence is discovered, (b) should notify the sending lawyer of their receipt, and (c) should abide by the sending lawyer's instructions as to their disposition.

The circumstances of the present inquiry present an even more compelling case against surreptitious acquisition and use of confidential or privileged information than that presented by the "inadvertent" or "unauthorized" disclosure decisions. First, to the extent that the other lawyer has "disclosed", it is an unknowing and unwilling, rather than inadvertent or careless, disclosure. In the "inadvertent" and "unauthorized" disclosure decisions, the public policy interest in encouraging more careful conduct had to be balanced against the public policy in favor of confidentiality. No such balance need be struck here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets.

Nor need we balance the protection of confidentiality against the principles of zealous representation expressed in Canon 7. Our Code carefully circumscribes factual and legal representations a lawyer can make, people a lawyer may contact, and actions a lawyer can take on behalf of a client. Prohibiting the intentional use of computer technology to surreptitiously obtain privileged or otherwise confidential information is entirely consistent with these ethical restraints on uncontrolled advocacy.

Although our jurisdiction does not extend to questions of law, we note that the misuse of some aspects of this technology, particularly the use of e-mail "bugs," may violate federal or state law prohibiting unauthorized interception of e-mail content. S*ee, e.g.,* The Electronic Communications Privacy Act, 18 U.S.C. §§2510 *et. seq*. In that event, such conduct would, of course, be unethical *per se*. DR 7-102(A)(8) ("In the representation of a client, a lawyer shall not . . .[k]nowingly engage in other illegal conduct or conduct contrary to a Disciplinary Rule").

Finally, the inquiry that has prompted this opinion underscores the need for all lawyers to exercise care in using Internet based e-mail. Accordingly, we reiterate the admonition we offered in N.Y. State 709 (1998) that "lawyers must always act reasonably in choosing e-mail for confidential communications, as with any other means of communication." [2]

CONCLUSION

A lawyer may not make use of computer software applications to surreptitiously "get behind" visible documents or to trace e-mail.

(25-01)

---

[2] As noted in N.Y. State 709 (1998), " in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely within the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail."