

[New York State Bar Association Letterhead]

COMMITTEE ON PROFESSIONAL ETHICS

Topic: Using employer's computer system; preserving client confidentiality

Digest: Unless all relevant clients first give informed consent, a lawyer employed by a government agency to represent individual clients may not use the agency's computer system for work that discloses clients' confidential information if the agency may obtain access to the client's confidential information.

Rules: 1.1, 1.6 & 8.5.

FACTS

1. The inquirer is a lawyer licensed in New York (and in no other jurisdiction) who is employed as a defense counsel in the Department of Defense ("DoD"), Office of Military Commissions - Office of the Chief Defense Counsel. The inquirer is inquiring on his own behalf as well as on behalf of other New York-admitted lawyers in that office. The responsibilities of the Office of the Chief Defense Counsel extend to defending, before a military commission, those detainees currently held at Guantanamo Bay who have been criminally charged. Under the governing statute, the office is within the Department of Defense, but its professional responsibilities are toward the detainees, who are their clients. The lawyers owe these clients the same fiduciary duties that criminal defense lawyers ordinarily owe to their clients.

2. As part of the inquirer's employment, he and the other lawyers in his office use government-owned information systems, including computers, Internet, email and telephone, for communicating with clients and others, storing files, and creating work product. The inquirer works in a secure facility (meaning that only those with a security clearance may enter); e-mail is the principal means of communication with those outside the facility; and filings in cases are made electronically.

3. DoD has asked the lawyers in the inquirer's office to sign a form (a "Systems User Agreement") that would give the government consent to intercept and monitor electronic files and communications, including data and communications covered by the attorney-client privilege and attorney-client confidentiality. Among other things, the form provides that the signer "consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence

investigation)” (all caps in original), but the signer does not consent to the use of “privileged communications or data” for any purpose.

4. It is unclear from the fact presented to us whether DoD would permit the lawyers in the Office of the Chief Defense Counsel to conduct work from the office electronically without employing the DoD computer system (or, if not, whether a court could or would order DoD to permit the lawyers to engage in non-intercepted electronic communications, research, word processing and other work). It is also uncertain whether currently, even before receiving consent, DoD is intercepting and reviewing the office’s electronic files and data, or reserves the right to do so.

QUESTION

5. Under these circumstances, may the inquirer provide the requested consent, and subsequently use the DoD computer system for client-related work, knowing that DoD may intercept and monitor his work?

OPINION

A. Choice of Law Questions.

6. At the outset, we note, but do not resolve, the question of whether, and to what extent, the inquiring lawyer’s relevant conduct is governed by the New York Rules of Professional Conduct (the “New York Rules”), which were adopted effective April 1, 2009. Under Rule 8.5 of the New York Rules, lawyers admitted to practice in New York are subject to discipline in this state no matter where their conduct occurs. However, the New York Rules are not invariably the ones that determine the propriety of their conduct. For example, Rule 109(b)(1) of the Manual for Military Commissions (2010 ed.) requires lawyers practicing before military commissions to comply with three different sets of rules: (i) State Rules of Professional Conduct, (ii) rules specific to military service, and (iii) rules specific to military commissions. Rule 109(b)(3)(A) addresses issues of choice of law and conflicts that may arise among the different rules to which lawyers are subject.

7. Because this Committee’s jurisdiction is limited to interpreting the New York Rules, we have not considered whether Rule 109(b) (or any other provision) of the Manual for Military Commissions requires compliance with the New York Rules. Nor have we considered whether any other relevant sets of rules or regulations may govern defense counsel in the Office of Military Commissions (though we are aware of none). Nor have we considered whether the New York Rules conflict with service-specific or commission-specific rules with regard to the conduct in question, or how any conflict would be resolved. We assume for purposes of this opinion that the New York Rules may be relevant, but we also observe that other rules may apply in addition or instead. Thus, it is not clear that the New York Rules, standing alone, would apply in a New York disciplinary proceeding on the questions addressed in this opinion.¹

¹ Under Rule 8.5(b) of the New York Rules, if the military commissions have professional conduct rules that govern the scope of lawyers’ duty to preserve the confidentiality of information relating to representations before the

B. The Scope of Confidential Information.

8. Insofar as the New York Rules apply, the inquiry would be governed by Rule 1.6. Rule 1.6(a) provides, in pertinent part:

A lawyer shall not knowingly reveal confidential information, as defined in this Rule, . . . unless: (1) the client gives informed consent, as defined in Rule 1.0(j); (2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or (3) the disclosure is permitted by paragraph (b).

9. Rule 1.0(j) defines “informed consent” to denote “the agreement by a person to a proposed course of conduct after the lawyer has communicated information adequate for the person to make an informed decision, and after the lawyer has adequately explained to the person the material risks of the proposed course of conduct and reasonably available alternatives.”

10. Rule 1.6(a) goes on to define “confidential information” to consist of: “information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential.”

11. Rule 1.6(b) sets forth exceptions to the confidentiality duty, none of which appear to be applicable in these circumstances.²

commissions, the rules of the military commissions may be the applicable ones. *See* Rule 8.5(b)(1) (“For conduct in connection with a proceeding in a court before which a lawyer has been admitted to practice (either generally or for purposes of that proceeding), the rules to be applied shall be the rules of the jurisdiction in which the court sits, unless the rules of the court provide otherwise.”). If not, but if the state in which the lawyer maintains his office has authorized him to practice law regularly in that state subject to that state’s professional conduct rules, the applicable rules may be those of the state in which he regularly practices. *See* Rule 8.5(b)(2)(ii); *cf.* N.Y. State 815 (2007) (a New York lawyer who can lawfully engage in conduct in a foreign jurisdiction that would be the practice of law in New York -- even though the lawyer is not formally “admitted to practice” in the foreign jurisdiction -- and who is generally subject to the ethics rules in the foreign jurisdiction, is not subject to all provisions of the New York Code, provided the lawyer principally practices in the foreign jurisdiction and the primary effect of the lawyer’s conduct is not in New York); N.Y. State 750 (2001) (if conduct of a lawyer licensed in New York clearly has its “predominant effect” in another jurisdiction in which the lawyer is licensed to practice, the ethics rules of that jurisdiction apply to the conduct).

² The Committee is unaware of any laws or regulations that affect the conclusions reached in this opinion regarding Rule 1.6. Although Rule 1.6(b)(6) authorizes a lawyer to reveal confidential information “to comply with other law or court order,” our attention has not been directed to any law or court order that requires defense lawyers such as the inquirer to disclose detainee-clients’ confidential information to the Department of Defense without client consent. Even assuming *arguendo* that lawyers were required to consent to the interception and monitoring of electronic files and communications as a condition of using a government-owned computer (an assumption for which we have no factual basis), it does not follow that the lawyers would be required by law to use a government-owned computer for client matters. Further, to the extent that any law or court order might arguably require the disclosure of client confidential information without client consent, lawyers would be required to make any

C. The Duty to Protect Confidential Information.

12. Finally, Rule 1.6(c) provides in pertinent part: “A lawyer shall exercise reasonable care to prevent the lawyer’s employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client.”

13. As Rule 1.6(c) reflects, a lawyer must take steps to avoid unintentional disclosures of confidential information. Comment 17 to the rule elaborates this requirement, as follows:

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

14. A lawyer may thus be subject to discipline not only for disclosing confidential information knowingly but also for doing so recklessly or negligently. *See Matter of Holley*, 285 A.D.2d 216, 220, 729 N.Y.S.2d 128, 132 (1st Dep’t 2001) (“whether he acted recklessly or [merely] 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”).

15. This Committee has consistently recognized the obligation of lawyers to take precautions to avoid disclosing confidential information to third parties (other than those such as agents or professional colleagues of the lawyer who are committed to keeping the information confidential).³ For example, N.Y. State 820 (2008) recognized that a lawyer could not properly communicate about client matters on an e-mail provider “if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the

available, non-frivolous challenges to the law before complying. *See, e.g.*, N.Y. City 2005-3 (if a lawyer testifying about a former client is asked a question that the former client has not given consent to the lawyer to answer, the lawyer should assert any applicable objection, including privilege, that would enable the lawyer to avoid answering the question).

³ Although the opinions cited here were issued before April 1, 2009, when the New York Rules of Professional Conduct went into effect, they are as applicable to Rule 1.6 as they were to DR 4-101 of the New York Code of Professional Responsibility.

communications to third parties without the sender's permission (or a lawful judicial order). . . . A lawyer must exercise due care in selecting an e-mail service provider to ensure its policies and stated practices protect client confidentiality." Ten years earlier, in N.Y. State 709 (1998), this Committee found that communicating about client matters via the Internet is generally permissible because the law protects against the interception of communications, but we noted that "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, . . . the lawyer must select a more secure means of communication than unencrypted Internet e-mail."

16. Additional relevant opinions on the subject of protecting clients' confidential information include N.Y. State 827 (2008) (lawyer may send legal bills to an outside auditor hired by the client only after "tak[ing] steps to ensure that the client understands any risks for the client that follow from disclosure of billing information to the auditor. These risks include the possibility of further disclosure by the auditor to others, the possibility that the disclosure will waive the attorney-client privilege, and the possibility that the information disclosed to the auditor might somehow be used adversely to the client."); N.Y. State 718 (1999) (without client consent, a legal aid office may provide information for use in a bar association study only if the information could not possibly be identified with a particular client); N.Y. State 490 (1978) (staff attorneys of legal services office may not report on specific cases to the office's board of directors without client consent to the disclosure of confidences and secrets; in seeking client consent, lawyers "should be particularly sensitive to any element of submissiveness on the part of their indigent clients; and, such requests should be made only under circumstances where the staff is satisfied that their clients could refuse to consent without any sense of guilt or embarrassment"); and N.Y. State 485 (1978) (legal aid lawyers may not divulge client confidences to a not-for-profit research organization). *See also* N.Y. State 800 n.5 (2006) ("Consent can only be sought where the prospective client would be empowered to withhold consent freely. . . . [I]t would be difficult to obtain voluntary consent from an assigned client."); N.Y. City 1997-2 (when a client who is a minor child gives consent to disclose confidential information, "the client's consent must be voluntary. Among other things, the lawyer must consider whether the minor perceives, accurately or not, that in the absence of consent, he will not be able to secure legal assistance. If that is the case, it is unlikely that the consent can be deemed voluntary.").

17. Under Rule 1.6, without client consent, the office's lawyers may not use the DoD computer system for work relating to client matters pursuant to the Systems User Agreement if the work would directly or indirectly disclose confidential information to DoD. This would be true even if DoD promised not to use the information adversely to the detainee-clients (which it has not),⁴ and it would be true even if DoD were not in an adversary relationship with the detainee-clients (which it is). The mere disclosure of clients' confidential information to third parties (such as DoD) without the clients' informed and voluntary consent violates Rule 1.6, regardless of whether the client is thereby prejudiced.

⁴ As noted above, DoD's form would not authorize DoD to use clients' "privileged communications or data" – but confidential information includes not only communications protected by the attorney-client privilege but also any other information relating to a representation that is "likely to be embarrassing or detrimental to the client if disclosed" or that "the client has requested be kept confidential." DoD has not agreed to refrain from using confidential information in these non-privileged categories.

18. Because the inquirer has already used his computer for client matters, and it therefore currently contains e-mails and client files containing confidential information covered by the rule, he may not now sign the Systems User Agreement without first obtaining all relevant clients' informed and voluntary consent. Whether it would be possible to obtain the relevant clients' informed consent, and whether their consent can be voluntarily given, are questions that this Committee lacks sufficient facts to resolve.

19. Even if the lawyer does not sign the Systems User Agreement or otherwise authorize DoD monitoring and interception of communications, Rule 1.6(a) prohibits him from performing work on DoD computers if there is a reasonable possibility that individuals in DoD (other than defense lawyers in the office who are duty-bound to maintain the confidentiality of detainee-clients' information) will have access to that work. This means that the lawyer may not conduct work on the DoD computer system that would reveal confidential information until he first obtains adequate assurance that DoD will not engage in the "interception/capture and seizure" (to quote the DoD consent form) of the lawyer's files and other electronic data.⁵

CONCLUSION

20. Unless all relevant clients first give informed consent, a lawyer employed by a government agency to represent individual clients may not use the agency's computer system for work on client matters that discloses clients' confidential information if the agency may obtain access to the client's confidential information.

⁵ We have not been provided sufficient information to address whether the inquiring lawyer could provide competent representation, as required by Rule 1.1, without using a DoD computer.