Washington Journal of Law, Technology & Arts

Volume 3 | Issue 2 Article 2

12-4-2006

Hiding Evidence from the Boss: Attorney-Client Privilege and Company Computers

Kelcey Nichols

TOPIC
Cite as: Kelcey Nichols, *Hiding Evidence from the Boss: Attorney-Client Privilege and Company Computers*, 3 Shidler J. L. Com. & Tech. 6 (Dec. 4, 2006), *at* <http://www.lctjournal.washington.edu/Vol3/a006Nichols.html>

HIDING EVIDENCE FROM THE BOSS: ATTORNEY-CLIENT PRIVILEGE AND COMPANY COMPUTERS

By Kelcey Nichols[1]

Abstract

Recent court decisions in *In re Asia Global Crossing, Ltd.*, *People v. Jiang*, and *Curto v. Medical World Communications* have held that attorney-client privilege can protect certain information located on an employer-issued computer from disclosure if the employee had a reasonable expectation of privacy. This Article provides a brief background on attorney-client privilege and explores the factors courts consider when determining whether an employee has this reasonable expectation. These factors include the scope of employer monitoring, the employer-employee agreement pertaining to the computer, the presence of password-protection, the location of the computer, and the relevancy of the evidence to a particular legal proceeding.

Table of Contents

INTRODUCTION

<1> Several recent cases illustrate how courts interpret the scope of attorney-client privilege as it relates to data stored on employer-issued computers.[2] In *In re Asia Global Crossing,*

Ltd., a New York bankruptcy court held that attorney-client privilege protected employees' emails sent through their employer's email system.[3] Former employees asserted the privilege against their former employer's bankruptcy trustee who sought the information in connection with a pending bankruptcy proceeding.[4] Similarly, in *People v. Jiang*, a sexual assault defendant claimed attorney-client privilege with respect to documents prepared for his attorney on his company computer.[5] A California appellate court upheld the privilege.[6] In *Curto v. Medical World Communications*, a New York district court protected memos an employee sent to her attorney using an outside mail program on an employer-issued laptop.[7] The employee asserted the privilege to protect documents related to her Equal Employment Opportunity Commission ("EEOC") complaint against the employer.[8] With the help of a forensics consultant, the employer recovered the documents from the hard drive of the employee's company laptop.[9] These cases demonstrate that courts are willing to uphold attorney-client privilege when two conditions are met: (1) the employee has properly asserted the privilege and (2) the employee has a reasonable expectation of privacy.

UNDERSTANDING ATTORNEY-CLIENT PRIVILEGE

<2> The attorney-client privilege allows a client to refuse to disclose confidential communications with his or her attorney.[10] The standard test for attorney-client privilege has two elements. First, the communication must involve legal advice sought by a client from an attorney acting in his or her capacity as a legal advisor.[11] Second, the communication from the client to the attorney must be made confidentially.[12] Disclosure to a third party generally constitutes a waiver of the privilege.[13] The burden of proof rests on the party asserting the attorney-client privilege.[14] Employees and their attorneys may seek to invoke attorney-client privilege as long as the above elements are met.

<3> Courts construe attorney-client privilege narrowly because the privilege results in withholding information from the fact-finder.[15] Federal Rule of Evidence 501 states that courts should determine whether attorney-client privilege exists based on common law principles. The issue of attorney-client privilege as it relates to employer-issued computers may arise in any civil or criminal case in which a party seeks to protect or disclose information on a company computer. Such information may range from an employee's email messages[16] to website history[17] to documents prepared in defense of criminal

charges.[18]

REASONABLE EXPECTATIONS OF PRIVACY

<4> An employer's policies regarding the workplace and computer use may diminish an employee's expectation of privacy. To date, courts have not developed bright line approaches for determining when attorney-client privilege protects data stored on an employer-issued computer. Courts, however, have considered factors such as: (1) the extent of networking within the workplace[19] and previous employer monitoring of employee computers,[20] (2) the scope of the employer-employee agreement pertaining to the use of the computer,[21] (3) the existence of password-protected documents,[22] (4) the location of the computer,[23] and (5) the relevancy of the evidence.[24] Each of these factors help courts determine whether the employee had a reasonable expectation of privacy and may assert attorney-client privilege.

<5> An employee's expectation of privacy plays a central role in determining if attorney-client privilege exists.[25] A company's office policies and procedures, with respect to emails sent through its computer system, may reduce an employee's reasonable expectation of privacy according to the *Asia Global Crossing* court.[26] There, five employees communicated with their personal attorney using company computers and email.[27] The employees left the company shortly thereafter.[28] Pursuant to a subsequent bankruptcy proceeding involving the company, a court trustee took possession of the corporate computers, including potentially privileged information from the former employees.[29] Counsel for the former employees realized that they had left privileged communications on the company servers and sought to protect both documents and emails under attorney-client privilege.[30] The trustee sought disclosure of the documents as part of his investigation.[31] The court presented four factors as relevant as to whether privilege was attached to data on the company computers: (1) the employer's policy banning or restricting personal use of company computers, (2) employer monitoring of company computers and employee email, (3) third party's access to the company computer and employee's email, and (4) the employee's awareness of the employer's use and monitoring policies.[32]

<6> The court found "the question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable."[33] To determine whether the former

employees had a reasonable expectation of privacy, the court weighed factors in the workplace environment that could compromise confidentiality: access by others in the corporation,[34] the employer's limitations on personal use of computers,[35] and the employer's intent to monitor the email system.[36] In this case, the court held that the employer failed to prove that the it's practices had compromised the former employees' expectation of confidentiality in their emails to their attorney.[37] The court based its decision on conflicting information regarding the employer's email monitoring policy and access to emails. While the company claimed to have a policy against personal use of email, the policy did not mention the employer by name and employees were unaware of the policy.[38] The court held that the facts of this case did not support a conclusion that, "as a matter of law," the email communications "eliminated any otherwise existing attorney-client privilege."[39]

<7> Similarly, in *People v. Jiang*[40] and *TBG Ins. Services*, the California Court of Appeals considered employees' expectations of privacy in light of these factors and the overall workplace environment.[41] In *Jiang*, a criminal defendant in a sexual assault case, sought to protect documents he had prepared for his attorney in connection with his defense.[42] The defendant had saved files on his company computer relating to the litigation, including a statement prepared to orient a medical expert.[43] The court found the defendant had a reasonable expectation of privacy because he did not expect monitoring by the employer and had password-protected the personal documents he prepared for his attorney.[44]

<8> In contrast, in *TBG*, the court found that the employee did not have a reasonable expectation of privacy based on his consent to workplace monitoring by his employer.[45] There, TBG Insurance Services dismissed an employee for allegedly accessing Internet pornography while at work in violation of company policy.[46] Following his dismissal, the employee sued for wrongful termination and the employer sought the production of the employee's company-owned home computer.[47] The employee had signed an agreement stating that he would use the company computers for "business purposes only" unless his employer "expressly approved" personal use of the computer.[48] The agreement further stipulated that the company could monitor the employee's computer use on an "as needed" basis and expressly rejected the use of the computer for "obscene or other inappropriate

purposes."[49] Based on this explicit agreement, the court held the employee did not have a reasonable expectation of privacy.[50]

<9> Similarly, in *Curto*, as in *TBG Ins. Services*, the company policy mandated that company computers could be used exclusively for business purposes and that employees' had no reasonable expectation of privacy in their computers.[51] Nonetheless, because the company did not enforce the policy, the district court held that an employee who sent memos to her attorney using an outside mail program had a reasonable expectation of privacy in those documents.[52] The court based its decision on the employee's reasonable precautions to protect the privacy of the documents and prompt assertion of attorney-client privilege following the recovery of the documents.[53]

WORKPLACE MONITORING: THE RISK OF WAIVER

<10> Workplace monitoring and networking may constitute a waiver of attorney-client privilege if these activities involve sharing information with a third party. In *United States v. Long*, a military employee sought to prevent emails written on her work computer communicating her fear of drug testing, from being introduced into evidence in support of drug charges against her.[54] The employee could not claim attorney-client privilege because she had not sent the emails to her attorney.[55] However, she asserted that the emails had been unlawfully seized without her consent or a "lawful search authorization" in violation of the Fourth Amendment of the United States Constitution.[56] The government argued that the employee did not have a reasonable expectation of privacy because she knew the government monitored her computer from the "Notice and Consent to Monitoring" banner that appeared every time she accessed the network.[57] However, the court held that the "Notice and Consent to Monitoring" banner did not indicate to the employee that she did not have a reasonable expectation of privacy in her email.[58] Accordingly, the trial court's admission of the evidence was overturned.[59]

<11> Where employees explicitly agree to workplace monitoring and understand that such monitoring compromises their privacy, there may be an insufficient basis for attorney-client privilege.[60] Employees who know their employers monitor work computers may not reasonably believe that information sent or stored on those computers is confidential. Thus, an employee may not be able to establish the reasonable expectation of

privacy crucial to attorney-client privilege. For example, in *TBG*, discussed above, a discharged employee expressly consented to employer monitoring and acknowledged that any communications sent via a company computer were not considered private.[61] The court found that the employee did not have a reasonable expectation of privacy in personal files he had stored on the company computer. While the court did not address attorney-client privilege, the holding implies that an explicit consent to workplace monitoring could negate an employee's expectation of privacy and thereby waive attorney-client privilege.[62]

<12> Employer-employee agreements also help establish an employee's expectations of computer use and privacy. In addressing attorney-client privilege and employer-issued computers, at least three courts have considered the overall goals of the agreement[63] and the policies regarding personal use by employees[64] as determinative of the agreement's intent. In *Jiang*, the court found that the employee-employer agreement was intended to protect the employer's intellectual property rather than limit employees' personal use of their company's computers.[65] As the employee's documents pertained to his defense in a criminal case, not his employer's intellectual property, the court found the employer-employee agreement did not compromise the employee's expectation of privacy.[66] Furthermore, because the use agreement did not intend to prevent the defendant from using his employer-issued computer to communicate with his attorney, the court upheld attorney-client privilege.[67]

<13> In contrast, the use agreement in *TBG Ins. Services* expressly precluded personal use of company computers and reserved the employer's right to review, copy and disclose any files on company computers.[68] Accordingly, the court did not find that the employee had a reasonable expectation of privacy in documents saved on his employer-issued computer.[69] Thus, the substance of the employer-employee agreement plays a critical role in determining whether the requisite confidentiality for attorney-client privilege exists.

PASSWORD-PROTECTION

<14> Courts have upheld attorney-client privilege with regard to password-protected documents on employer-issued computers. In *Long*, discussed above, the United States Court of Military Appeals held that an employee had a reasonable expectation of privacy in her email because the employee could control access

to her email by creating a password.[70] Only the employee knew her password and agency policy recognized employees' privacy interest in their email. Although the network administrator had access to the employee's computer, such access did not affect the employee's reasonable expectation of privacy in her password-protected email.[71] Similarly, in *Jiang*, the defendant prepared documents in a folder labeled "Attorney," and password-protected each document.[72] The California appellate court held that this satisfied the defendant's initial evidentiary burden by proving that the documents had been password-protected to protect them from disclosure.[73]

<15> An employee's initial showing of attorney-client privilege may be overcome if the opponent can prove that the documents were not confidential.[74] For example, if the opposing party can show that the documents were "not private," in spite of password-protection, they may prove the employee had no reasonable expectation of privacy or that the employee waived attorney-client privilege.[75] For example, a Massachusetts district court held that an employee did not have a reasonable expectation of privacy where an employee knew his employer had access to his password-protected documents through a network.[76] Password-protection, therefore, supports an employee's claim of a reasonable expectation of privacy where it prevents access to documents or email by third parties, but only creates a presumption in favor of the employee.

LOCATION OF COMPUTER

<16> Courts have also considered the physical location of an employer-issued computer when determining whether the employee had a reasonable expectation of privacy. In *Curto*, a New York district court weighed the use of the employer-issued laptops in a home office and upheld the employee's assertion of attorney-client privilege.[77] However, this is not determinative. In *TBG*, the California Court of Appeals held that the opposing party could discover information on an employer-issued computer the employee used at home.[78] There the court held that the location of the computer did not affect the employee's expectation of privacy since the employer had the same computer use policy for home and workplace use.[79]

<17> The *Curto* court noted that attorney-client privilege cases are fact-specific and must be weighed on an individual basis.[80] Accordingly, courts are likely to determine whether the location of the computer played a role in the employee's expectations of privacy based on the particular facts of each case.

EMPLOYER ISSUED COMPUTER USED FOR CRIMINAL ACTIVITY

<18> Courts may be less likely to grant attorney-client privilege when the computer in question contains information relevant to a crime. In a New York case, a defendant used a personal laptop computer to communicate with his attorney; the same computer had been used to access the security system in a murder victim's building.[81] The court found strong reasons to believe the computer had been used as an "instrumentality of the crime" and held that attorney-client privilege could not be used to shield the defendant.[82] The court declined to extend attorney-client privilege over the computer itself, pointing out that attorney-client privilege does not extend to physical property where "reasonable grounds" exist to believe such property was used in a crime.[83] The court did not reach the issue of whether attorney-client privilege protected certain documents on the computer.

CONCLUSION

<19> Until definite standards are developed pertaining to attorney-client privilege and employer-issued computers, common law standards will continue to govern attorney-client privilege. Courts will likely consider the factors discussed above and weigh each factor against the narrow construction of attorney-client privilege.[84] Because such balancing tests vary from case-to-case, attorneys should advise employees to exercise caution when communicating on an employer-issued computer, particularly if that computer may be subject to workplace monitoring.

PRACTICE POINTERS

- As workplace monitoring of employee computer use increases,[85] attorneys should exercise additional caution when communicating with clients, particularly when clients use an employer-issued computer to email or prepare documents for their attorney. Attorneys should also consider the employee's awareness and consent to workplace monitoring.
- Attorneys should advise their clients that information on an employer-monitored or networked computer may be insecure. The existence of networking and employee monitoring should alert attorneys to a

potential waiver of attorney-client privilege, even though networking or employer-monitoring in and of itself may not revoke the privilege.

- Attorneys should look to the employer-employee agreement regarding computer use to assess whether the employee has a reasonable expectation of privacy. Attorneys should take note that courts may also consider the enforcement, or lack of enforcement, of the policy.
- Attorneys representing employers should ensure that policies regarding computer use and employer monitoring are clearly communicated to employees, preferably in a signed employer-employee agreement.
- Attorneys representing employers should apply the same employer-employee agreement regardless of where the computer is used. Attorneys representing employees should caution their clients that using an employer-issued computer at home does not create a greater expectation of privacy.
- Password-protection may support an employee's reasonable expectation of privacy; attorneys should be aware, however, that password-protected documents accessible to a third-party will likely waive attorney-client privilege.
- Courts are unlikely to protect information stored on a computer that may constitute evidence of a crime under attorney-client privilege. Parties cannot use attorney-client privilege to shield otherwise discoverable information such as the facts of a crime.

<< Top

Footnotes

1. Kelcey Nichols, University of Washington School of Law, Class of 2007. Thank you to Professors Robert Aronson and Anita Ramasastry of the University of Washington School of Law, Terrance Keenan, Emma Scanlan, and Jamila Johnson.
2. *See* In re Asia Global Crossing, Ltd., 322 B.R. 247 (Bankr. S.D.N.Y. 2005); People v. Jiang, 33 Cal.Rptr.3d 184 (Cal. Ct. App. 2005), *modified*, 2005 Cal. App. LEXIS 1257 (Cal. Ct. App. 2005),

depublished, 2005 Cal. LEXIS 11250 (Cal. 2005); Curto v. Med. World Commc'ns, 2006 WL 1318387 (E.D.N.Y. 2006).

3. *Asia Global Crossing, Ltd.*, 322 B.R. at 251.
4. *Id.*
5. *Jiang*, 33 Cal.Rptr.3d at 199.
6. *Id.*
7. Curto v. Med. World Commc'ns, 2006 WL 1318387 (E.D.N.Y. 2006).
8. *Id*.
9. *Id.*
10. BLACK'S LAW DICTIONARY 1215-16 (8th ed. 2004).
11. United States v. Evans, 113 F.3d 1457, 1461 (7th Cir. 1997).
12. *Id.*
13. In re Grand Jury Subpoena Dated June 30, 2003, 1 Misc. 3d 510, 516-17 (N.Y. Sup. Ct. 2003).
14. In re Asia Global Crossing, Ltd., 322 B.R. 247, 255 (Bankr. S.D.N.Y. 2005).
15. United States v. Zolin, 491 U.S. 554, 562 (1989); see also, Fisher v. United States, 425 U.S. 391, 403 (1976), In re Grand Jury Matter No. 91-01386, 969 F.2d 995, 997 (11th Cir. 1992), *In re* Grand Jury Investigation No. 83-2-35, 723 F.2d 447, 451, (6th Cir. 1983), *Evans*, 113 F.3d at 1461.
16. United States v. Long, 64 M.J. 57, 58-59 (C.M.A. 2006).
17. TBG Ins. Serv. Corp. v. Superior Court of Los Angeles County, 96 Cal.App.4th 443, 449, (Cal. Ct. App. 2002).
18. People v. Jiang, 33 Cal.Rptr.3d 184 (Cal. Ct. App. 2005), *modified*, 2005 Cal. App. LEXIS 1257 (Cal. Ct. App. 2005), *depublished*, 2005 Cal. LEXIS 11250 (Cal. 2005).
19. When networking constitutes employer monitoring of email, an employee may not have a reasonable expectation of privacy in his or her email. *See Asia Global Crossing, Ltd.*, 322 B.R. at 257-258.

20. *See Long*, 64 M.J. 57; In re Currency Conversion Fee Antitrust Litigation, 2003 WL 22389169, *3 (S.D.N.Y. 2003)(unpublished), Asia Global Crossing, Ltd., 322 B.R. at 257.

21. *See* TBG Ins. Svcs Corp., 96 Cal.App.4th 443; Jian*g*, 130 Cal.App.4th at 1538-39.

22. *See* Long, 64 M.J. 57, *Jiang*, 130 Cal.App.4th 1512.

23. *See* United States v. Regan, 281 F. Supp. 2d 795, 802 (D. Va. 2002).

24. *See In re Grand Jury Subpoena Dated June 30, 2003*, 1 Misc. 3d 510, 516-17 (N.Y. Sup. Ct. 2003).

25. *TBG Ins. Services Corp*., 96 Cal.App.4th at 449-50.

26. *In re Asia Global Crossing, Ltd*., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (*citing O'Conner v. Ortega*, 480 U.S. 709, 717 (1987)).

27. *Id.* at 252.

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.* at 252-253.

32. *Id.* at 257.

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id*. at 261.

38. The court noted that the employees' lack of awareness regarding the employer's email policy alone would not mean the employees were not on notice of the policy. *See id.*

39. *Id.*

40. *People v. Jiang*, 33 Cal.Rptr.3d 184, 199 (Cal. Ct. App. 2005), *modified*, 2005 Cal. App. LEXIS 1257 (Cal. Ct. App. 2005), *depublished*, 2005 Cal. LEXIS 11250 (Cal. 2005).

41. *See Jiang*, 33 Cal.Rptr.3d at 199; *TBG Ins. Serv.*

Corp. v. Superior Court of Los Angeles County, 96 Cal.App.4th 443, 451 (Cal. Ct. App. 2002).

42. *Jiang*, 33 Cal.Rptr.3d at 199.
43. *Id.*
44. *Id.* at 204-205.
45. *TBG Ins. Services Corp.*, 96 Cal.App.4th at 451.
46. *Id.*
47. *Id.* at 446.
48. *Id.*
49. *Id.*
50. *TBG Ins. Services Corp*., 96 Cal.App.4th at 451.
51. *Curto v. Med. World Commc'ns*, , 2006 WL 1318387 (E.D.N.Y. 2006)..
52. *Id.*
53. *Id.*
54. United States v. Long, 64 M.J. 57 (C.M.A. 2006).
55. *Id.*
56. *Id.*
57. *Id.*
58. *Id.* at 65.
59. United States v. Long, 64 M.J. at 59 (C.M.A. 2006).
60. *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 261 (Bankr. S.D.N.Y. 2005)..
61. *TBG Ins. Serv. Corp. v. Superior Court of Los Angeles County*, 96 Cal.App.4th 443, 452-53 (Cal. Ct. App. 2002).
62. Dion Messer, *To Client@Workplace.com: Privilege at Risk?*, 23 J. Marshall J. of Computer & Info. L. 75, 92 (2004).
63. *People v. Jiang*, 33 Cal.Rptr.3d 184, 204 (Cal. Ct. App. 2005), *modified*, 2005 Cal. App. LEXIS 1257 (Cal. Ct. App. 2005), *depublished*, 2005 Cal. LEXIS 11250 (Cal. 2005).
64. *TBG Ins. Services Corp*., 96 Cal.App.4th at 443.

65. *Jiang*, 33 Cal.Rptr.3d at 204.

66. *Id.*

67. *Id.*

68. *Id.* at 199.

69. *TBG Ins. Services Corp.*, 96 Cal.App.4th at 454.

70. United States v. Long, 64 M.J. at 64 (C.M.A. 2006).

71. *Id.*

72. *People v. Jiang*, 33 Cal.Rptr.3d 184, 188 (Cal. Ct. App. 2005), *modified*, 2005 Cal. App. LEXIS 1257 (Cal. Ct. App. 2005), *depublished*, 2005 Cal. LEXIS 11250 (Cal. 2005)..

73. *Id.* at 203.

74. *See id.*

75. *See id.* at 206.

76. *Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. 2002).

77. *Curto v. Med. World Commc'ns*, 2006 WL 1318387 (E.D.N.Y. 2006)..

78. *TBG Ins. Serv. Corp. v. Superior Court of Los Angeles County*, 96 Cal.App.4th 443, 455 (Cal. Ct. App. 2002).

79. *Id.*

80. *Curto*, 2006 WL 1318387.

81. *In re Grand Jury Subpoena Dated June 30, 2003*, 1 Misc. 3d 510, 517 (N.Y. Sup. Ct. 2003).

82. *Id.* at 516-17.

83. *Id.*

84. *United States v. Zolin*, 491 U.S. 554, 562 (1989).

85. *2005 Electronic Monitoring & Surveillance Survey*, American Management Association and The ePolicy Institute, http://www.amanet.org/research/pdfs/EMS_summary05.pdf (last visited September 28, 2006). Based on a study of 526 companies, as many as 76% of employers now monitor their employees' computer use.

<< Top