St. Thomas Law Review

Volume 17
Issue 2 *Winter 2004*

Article 6

2004

Dawn Raids Here at Home - The Danger of Vanishing Privacy Expectations for Corporate Employees

Sarah Plotkin Paul

DAWN RAIDS HERE AT HOME? THE DANGER OF VANISHING PRIVACY EXPECTATIONS FOR CORPORATE EMPLOYEES

SARAH PLOTKIN PAUL

INTRODUCTION

Imagine a large, multi-million dollar business, with offices all around the world. One morning, corporate officers in the company's London branch are treated to a knock at the door. Rather than being zealous young employees, ready to start the day early, the bearers of the knock are European Union ("EU") investigators, ready to raid the building. The investigators march in, unannounced and without a search warrant, and force the corporate officers to help them dig through confidential business materials. They leave hours later, taking with them copies of hundreds of documents, e-mails, and computer files, including key papers prepared by company attorneys. The investigators, having conducted a "dawn raid," now have evidence they may legally use against the company and its employees.

In America, of course, such investigative tactics are utterly at odds with the concept of the Fourth Amendment, which protects the right of people to "be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[1] The Fourth Amendment, on its face, clearly seems to prohibit dawn raids, searches where officials require little evidentiary backing, have no judicial oversight, and observe few limits in scope. In fact, the Fourth Amendment has given rise to privacy-protective measures such as the search warrant and probable cause requirements, which often come into play to prevent unsupported, invasive searches.[2]

But what happens when these measures do not come into play? In the corporate workplace in particular, traditional Fourth Amendment protections are frequently not invoked. The protections that do exist are becoming less and less robust in the post-September 11th world as personal civil liberties take a backseat to the war on terrorism. While business entities have retained most of their historical protections, their employees have been less fortunate. This development is potentially disastrous for

1. U.S. CONST. amend. IV.

2. *See generally* FED. R. CRIM. P. 41 (illustrating the search warrant requirement); Illinois v. Gates, 462 U.S. 213 (1983) (illustrating the probable cause requirement).

corporate employees, who spend most of their waking hours at work,[3] and deserve to enjoy important privacy protections there.[4] Employees are particularly vulnerable in this present heyday of corporate criminal investigations,[5] in which American law enforcement officials have an incentive to take advantage of instances when the Fourth Amendment does not apply. Traditional document-searching methods in these investigations can be time-consuming and may lack an element of surprise. For instance, by the time prosecutors served the anticipated grand jury subpoena in the Arthur Andersen scandal, they suspected that Andersen officials had already shredded hundreds of documents.[6] Federal agents also contemplated search warrants in the Andersen case, but the warrants did not come to fruition in time to stop the alleged shredding.[7] Given these pitfalls, a simpler alternative could become tempting,[8] should it ever appear legally permissible.

This article posits that, due to the limited and diminishing privacy protections for corporate employees, Fourth Amendment jurisprudence is closer to permitting dawn raids in the workplace than popular opinion might suggest. First, the employee "standing" requirement to challenge an illegal search means employees must have a privacy interest in the particular workspace searched.[9] In certain instances, then, individual employees have no way of protesting the use of illegally obtained corporate documents against them, including documents they have authored.[10]

---

3. *See* Peter J. Isajiw, *Workplace E-Mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers*, 20 TEMP. ENVTL. L. & TECH. J. 73, 75 (2001) (observing that American employees work more hours per year than any other industrialized nation and further noting that those hours are only going up).

4. *Cf.* Mapp v. Ohio, 367 U.S. 643, 656 (1961)("The right to privacy, no less important than any other right carefully and particularly reserved to the people, would stand in marked contrast to all other rights declared as 'basic to a free society.'").

5. *See* Kathleen F. Brickey, *From Enron to Worldcom and Beyond: Life and Crime After Sarbanes-Oxley*, 81 WASH. U. L.Q. 357, 358 (2003) (noting that since 2001, federal and state regulators have initiated fraud investigations into dozens of corporations, including Adelphia, HealthSouth, McKesson, Tyco, and Qwest, and have brought criminal charges against about ninety corporate owners, executives, and employees).

6. *See* Joel Seligman, *No One Can Serve Two Masters: Corporate and Securities Law After Enron*, 80 WASH U. L.Q. 449, 517 n.151 (2002) (quoting the indictment of Arthur Andersen).

7. *See* Kurt Eichenwald, *Enron Watch*, N.Y. TIMES, Jan. 27, 2002, § 4, at 2.

8. *See* Michael L. Weiner, *The Knock at the Door: Antitrust Search and Seizure in a Global Setting*, 10-SPG ANTITRUST 4, 4 (1996) (noting that in order to be more effective, American antitrust enforcement techniques have shifted away from document subpoenas and toward surprise, on-site searches).

9. *See* Mancusi v. DeForte, 392 U.S. 364, 368 (1968).

10. *See, e.g.*, United States v. Payner, 447 U.S. 727, 731-32 (1980) (holding that because defendant lacked Fourth Amendment standing, evidence seized from a clearly illegal search could not be excluded).

Second, there may be few protections available to employees insofar as modern, widely-used workplace technologies are concerned, such as company computers and e-mail accounts.[11] Finally, with the passage of the USA Patriot Act,[12] businesses can be coerced into helping the government perform still more invasive investigations of employees, particularly in the areas of "'wire communication' technology such as Internet access, e-mail, voice mail, and telephone service . . . ."[13]

This article examines each of these limitations in turn. Part I outlines the EU dawn raids in more detail to provide a basis for comparison with traditional American approaches. Part II discusses the employee standing requirement for challenging illegal searches. Part III discusses how technological advancements in the workplace have further impacted employee privacy expectations. Part IV examines the implications of the USA Patriot Act for businesses, hypothesizing that this legislation will prevent organizations from acting as a privacy shield for their employees. Part V concludes by arguing that Fourth Amendment jurisprudence must become more protective of employee privacy, or else American law enforcement officials will have the legal (if not yet the cultural) basis for taking a disturbingly dawn raid like approach to corporate crime.

I. THE EUROPEAN APPROACH: DAWN RAIDS

A. THE LEGAL STRUCTURE OF DAWN RAIDS IN THE EU

For many years, the European Commission ("EC"), the executive branch of the EU, has had the power to carry out dawn raids, unannounced searches of company premises for possible antitrust violations.[14] This power stems from Articles 85 and 86, the principal competition provisions

11. *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding that plaintiff did not have a reasonable expectation of privacy in his work e-mail); United States v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002) (holding that a professor had no reasonable expectation of privacy in his university-issued computer).

12. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter "Patriot Act"].

13. *See* Frank C. Morris, Jr., *The Electronic Platform: E-Mail and Other Privacy Issues*, SH039 A.L.I.-A.B.A. 365, 388 (December 5-7, 2002).

14. *See* EEC Council Regulation No. 17 (first regulation implementing articles 85 and 86 of the treaty), 13 O.J. EUR. COMM. 204 (1962) (*amended by* 58 O.J. EUR. COMM. 1655 (1962), 162 O.J. EUR. COMM. (1963), and SPECIAL ED., 1st Series O.J. COMM. (L 285) 1035 (1971)), *available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31962R0017&model=guichett* [hereinafter Regulation No. 17].

of EU law.[15] As the body responsible for investigating and punishing violations of Articles 85 and 86, the EC has certain enforcement capabilities under Council Regulation No. 17 ("Regulation 17"),[16] enacted in 1962.[17] These enforcement capabilities include the authority to conduct dawn raids, which take place during normal business hours,[18] but are nonetheless notorious for their element of surprise.[19] Damaging documents obtained at a dawn raid may be used to file an antitrust complaint against an offender, which can ultimately result in the imposition of very high fines, cease-and-desist orders, and injunctions.[20]

Few constraints are placed on EC investigators who wish to embark upon a dawn raid. Pursuant to Article 14 of Regulation 17, a dawn raid need only be supported by a decision stating the subject matter and purpose of the investigation, the date on which the raid is to begin, the penalties for non-cooperation, and the right to have the decision reviewed by a court of law.[21] The decision to allow a dawn raid does not have to be a "well-reasoned legal brief," but can "simply describe the suspected violation and the general documentation to be examined . . . ."[22] The European Court of Justice has held that, so long as the terms of the search are set out in a decision, a search warrant is not necessary.[23] Nor is there any requirement that investigators have probable cause to search, but rather inspectors may undertake "all necessary investigations" and enjoy "a large measure of discretion in this regard."[24] The only additional requirement imposed is the obligation to consult with the competition authority of the member state in whose territory the investigation is to take place, which may decide to send its own officials to accompany the EC inspectors on the raid.[25]

During the dawn raid itself, moreover, EC inspectors enjoy wide-

15. *See* Treaty Establishing the European Economic Community, Mar. 25, 1957, art. 85, 298 U.N.T.S. 11.

16. Regulation No. 17, *supra* note 14.

17. *See id.*

18. Kristien Kaelen, *Managing a Dawn Raid in Europe*, 18 NO. 8 ACCA DOCKET 33, 34 (2000).

19. *See* William Snyder, *Due Process in the European Economic Community: Rights of Businesses During Commission Inspections*, 22 U. TOL. L. REV. 955, 956 (1991).

20. *See* Peter H. Burkard, *Attorney-Client Privilege in the EEC: The Perspective of Multinational Corporate Counsel*, 20 INT'L LAW. 677, 679 (1986).

21. *See* Regulation No. 17, *supra* note 14, art. 14; *see also* Snyder, *supra* note 19, at 960.

22. Snyder, *supra* note 19, at 960.

23. *See* Case C46/87, Hoeschst AG v. Commission, 1989 E.C.R. 2859, 4 C.M.L.R. 410 (1989).

24. *See* Regulation No. 17, *supra* note 14, art. 14; *see also* James S. Venit, *EU Competition Law – Enforcement and Compliance: An Overview*, 65 ANTITRUST L.J. 81, 95 (1996).

25. *See* Regulation No. 17, *supra* note 14, art. 14.

ranging powers. Though inspectors cannot seize original documents,[26] they may make copies of "books and business records," including all papers and e-mail relating to the company's business.[27] Inspectors may also examine and copy handwritten documents, diaries, travel records, expense reports, electronically stored data, and printouts of telephone numbers dialed.[28] Target companies have a duty to "cooperate actively" with an inspection, which means that these companies must not only grant inspectors free access to all parts of the premises, but also direct the inspectors' attention to all relevant documents.[29] Failure to do so can result in fines, as well as in a higher financial penalty for any underlying violation being investigated.[30] Companies may appeal the decision supporting the search to the European Court of Justice,[31] but in practice such appeals have rarely succeeded.[32] There is thus little chance of stopping a dawn raid from taking place.

Given the relative ease of conducting a dawn raid, these searches have been a very powerful form of investigation in the EU. Evidence gathered during a dawn raid, if successful in proving an antitrust violation, can lead to EU fines as steep as 10% of a company's worldwide revenue.[33] Considering that criminally prosecuting a business entity in the United States is often tantamount to fining that entity, this power is quite significant indeed. Moreover, the element of surprise that dawn raids provide has been of great benefit to EC investigators, since companies have little opportunity to hide or destroy incriminating documents. As EU antitrust chief Mario Monti has stated, "[s]urprise, spot investigations are one key tool in the fight against cartels."[34]

B. THE COCA-COLA EXAMPLE

The EU investigation of Coca-Cola constitutes a particularly instructive example of dawn raids in action. In late July 1999, EC inspectors conducted a multi-day raid of Coca-Cola offices and plants in

26. *Id.*
27. *See id.*; *see also* Kaelen, *supra* note 18, at 38.
28. *See* Kaelen, *supra* note 18, at 38-40.
29. *See* Regulation No. 17, *supra* note 14, art. 15; *see also* Venit, *supra* note 24, at 96.
30. *See* Regulation No. 17, *supra* note 14, art. 15; *see also* Kaelen, *supra* note 18, at 42.
31. Regulation No. 17, *supra* note 14, art. 17.
32. Venit, *supra* note 24, at 94.
33. *Id.* at 86.
34. Philip Shishkin, *Tough Tactics: European Regulators Spark Controversy With "Dawn Raids"*, WALL ST. J., Mar. 1, 2002, at A1.

four EU countries: Austria, Denmark, Germany, and Great Britain.[35] The raids occurred pursuant to a tip suggesting that Coca-Cola was abusing its position in the market.[36] Specifically, investigators sought to find evidence establishing whether Coca-Cola had offered "incentives to retailers to carry its full range of products, to sell more of them and to stop selling competing brands."[37] As the investigation progressed, EC officials conducted additional raids in May 2000 at Coca-Cola offices in London and Brussels, as well as a Coca-Cola subsidiary in Brussels.[38]

The dawn raids of Coca-Cola's offices and plants involved a review of internal files relating to the company's commercial practices with retailers and other customers.[39] During the 1999 raids, EC investigators "scoured desktop computers and searched e-mail servers. They sifted through hundreds of messages and left with copies of those that contained [certain] key words . . . . They also took copies of confidential legal documents prepared by Coke's in-house lawyers."[40] Coca-Cola was essentially powerless to stop the European Commission agents, though the company denied that any wrongdoing had occurred.[41] The chief director of Coca-Cola Nordic Beverages in Denmark was quoted as saying, "[w]e were naturally very surprised by the raid . . . [b]ut we opened up our files and the materials the Commission wanted to see and tried to cooperate."[42] From a public relations standpoint, Coca-Cola was hardly in a position to protest, as it had recently suffered bad press because of a product health scare in Belgium.[43] Moreover, failing to cooperate could have resulted in

35. *See* BBC News, *Why Coca-Cola was Raided*, *at* http://news.bbc.co.uk/1/hi/business/the_company_file/400865.stm (last visited Sept. 12, 2004) [hereinafter *Why Coca-Cola was Raided*]; BBC News, *Coca-Cola Premises Raided*, *at* http://news.bbc.co.uk/1/hi/business/the_company_file/400738.stm (last visited Sept. 12, 2004) [hereinafter *Coca-Cola Premises Raided*].

36. *See* BBC News, *Why Coca-Cola was Raided*, *supra* note 35; *see also* Betsy McKay & Brandon Mitchener, *EC Raids Coke Bottlers in Antitrust Investigation*, WALL ST. J., May 19, 2000, at A3 (suggesting that the initial tip-offs came from PepsiCo and Coca-Cola's other competitors); Freshfields Deringer, *Competition Comment: Competition Law Developments in the EU*, Feb./Mar. 2000 (suggesting that the initial tip-offs came from PepsiCo and Esselung, a large supermarket chain).

37. *Coca-Cola Premises Raided*, *supra* note 35; *see also This is Money, Coke Hit as EU Raids Offices*, *at* http://www.thisismoney.com/19990722/nm5585.html (last visited Sept. 12, 2004) [hereinafter *This is Money*].

38. McKay, *supra* note 36.

39. *Coca-Cola Premises Raided*, *supra* note 35.

40. Shishkin, *supra* note 34.

41. *See Coca-Cola Premises Raided*, *supra* note 35.

42. Barry James, *EU Raids Coca-Cola Bottlers*, *available at* http://www.iht.com/IHT/BJ/99/bj 072399b.html (last visited Sept. 9, 2004).

43. *See This is Money*, supra note 37.

monetary penalties to the company. [44]

The final outcome of the Coca-Cola matter is, as of this date, uncertain. The dawn raids commencing in July 1999 are just the beginning of the company's antitrust concerns. The text of Regulation 17 suggests that information gathered during an EU dawn raid may not be used in unrelated investigations from other sources.[45] Yet it has also been recognized that a violation of EC competition law may give rise to personal and corporate liability under U.S. and Canadian antitrust laws, prompt private damage suits in national courts, and trigger national competition law inquiries.[46] In the case of Coca-Cola, the Autorita Garante in Italy has already imposed a $16 million dollar fine on the company for abuse of a dominant market position.[47] The fine, which was handed down approximately five months after the EU launched its dawn raids, is the third largest ever imposed by the Italian competition authority, corresponding to 3% of Coca-Cola's revenues from 1998 sales of drinks on the Italian market.[48] Whether Coca-Cola will face further penalties from the EU itself is still an open question.[49] Regardless, the dawn raids have left Coca-Cola and its executives a prime target to be sanctioned in a myriad of other venues.

C. THE FOURTH AMENDMENT AND THE AMERICAN PERSPECTIVE ON DAWN RAIDS

The United States Constitution would seem to prohibit conducting such dawn raids in America. The Fourth Amendment protects the right of an individual to be free from "unreasonable searches and seizures," stating that "no Warrants shall issue, but upon probable cause."[50] In practice, this means that American law enforcement officials must often secure a search warrant from a magistrate judge, pursuant to a showing of probable cause to search the particular area and items in question.[51] This process, at least

44. *See* Regulation No. 17, *supra* note 14, art. 15; *see also* Kaelen, *supra* note 18, at 42.

45. *See* Regulation No. 17, *supra* note 14, art. 20. "Information acquired as a result of the application of Articles 11, 12, 13 and 14 shall be used only for the purpose of the relevant request or investigation." *Id.*

46. *See* Venit, *supra* note 24, at 87.

47. Betty Liu, *Italian Competition Body Fines Coca-Cola for Abusing Position,* FIN. TIMES, Dec. 18, 1999.

48. *Id.*

49. *See Soft Drinks: Commission Denies Coca-Cola Fine is Imminent,* EUR. REP., June 21, 2003. The Commission indicated: "we are still actively pursuing the case but as yet we have not decided whether to send a Statement of Objections to the Company." *Id.*

50. U.S. CONST. amend. IV.

51. *See* FED. R. CRIM. P. 41.

in theory, provides for a neutral check on law enforcement officials and limits the scale of a search. Even where a warrant need not be obtained in advance, as in a search of a motor vehicle, the police must typically still have probable cause before proceeding;[52] otherwise, the items seized will not be admissible in a court of law.[53] By contrast, EC officials embarking upon a dawn raid need not obtain a search warrant, particularize their searches, or have anything close to probable cause.[54]

Accordingly, Americans have expressed concerns about dawn raids. The lack of accompanying judicial oversight, especially, has prompted critics to argue that dawn raids fail to provide for separation of powers or protect essential civil liberties.[55] Since Mario Monti became antitrust chief in 1999, the American Chamber of Commerce in Belgium has requested that European Commission investigators follow search warrant standards along the lines of those followed in the United States.[56] Thus far, however, the EU and antitrust chief Monti have refused to do so.

Yet, looking at Fourth Amendment jurisprudence more closely, one wonders if the United States is really justified in criticizing chief Monti. While the text of the Fourth Amendment seems to forbid dawn raids, numerous legal loopholes exist which allow prosecutors to avoid traditional Fourth Amendment requirements. In the business context, these loopholes have not yet seriously impacted the privacy rights of corporate entities. However, as will be discussed in detail below,[57] they have begun to pose a danger to individual employees, preventing employees from challenging certain constitutionally impermissible searches and taking some workplace searches outside the bounds of the Fourth Amendment altogether. Where these exceptions arise, the American legal system has opened the door to tactics like dawn raids.

52. *See* Cal. v. Carney, 471 U.S. 386, 392 (1985) (finding that, so far as motor vehicles are concerned, "the exigencies attendant to ready mobility justify searches without prior recourse to the authority of a magistrate so long as the overriding standard of probable cause is met").

53. *See Mapp,* 367 U.S. at 660.

54. *See* Regulation No. 17, *supra* note 14, art. 14.

55. *See* Shishkin, *supra* note 34.

56. *See id.*

57. *See* discussion *infra* Parts II-IV.

II. THE STANDING REQUIREMENT AND ITS LIMITATIONS ON EMPLOYEE PRIVACY

A. FOURTH AMENDMENT STANDING TO CHALLENGE AN ILLEGAL SEARCH

In America, individuals may only challenge the use of evidence seized pursuant to a government search if they have standing to do so. Under the exclusionary rule, items seized pursuant to an illegal, warrantless search[58] generally cannot be used in court.[59] An exclusionary rule challenge, however, can only be made by someone whose own reasonable expectations of privacy were violated by the search. In other words, unless someone has a reasonable expectation of privacy in an area searched, he has no standing to contest the search,[60] and the illegally seized items can be used against him.[61]

In the organizational setting, the standing requirement comes into play when employees or entities seek to challenge a government search of a company's premises. Collective enterprises, such as unions or corporations, are entitled to claim a form of "corporate standing" to challenge searches of their offices and seizures of records from those offices.[62] Under the corporate standing doctrine, a corporation will typically have little trouble showing a reasonable expectation of privacy in its business premises.[63] Individual employees, however, often have more difficulty making such a showing. Areas set aside for an employee's exclusive use, such as an individual office, are likely to qualify as areas for which that employee has a privacy expectation.[64] However, an employee might not have a privacy expectation in an area where he or she does not normally work, even if that area contains documents that he or she has

58. Not all warrantless searches are illegal. *See, e.g.*, United States v. Robinson, 414 U.S. 218, 236-37 (1973) (holding that a full search of the person may be made without a search warrant, if done pursuant to a valid arrest).

59. *See Mapp*, 367 U.S. at 660.

60. *See, e.g.*, Rawlings v. Kentucky, 448 U.S. 98, 104-06 (1980) (holding that defendant had no standing to challenge the search of his acquaintance's purse, despite the fact that defendant's drugs were inside the purse); Minnesota v. Carter, 525 U.S. 83, 90-91 (1998) (holding that houseguests only present in a house for two hours had no standing to challenge the search of that house).

61. *See, e.g.*, *Rawlings*, 448 U.S. at 104-06.

62. *See* G.M. Leasing Corp. v. United States, 429 U.S. 338, 352-55 (1977).

63. *See, e.g.*, United States v. Zhang, 833 F. Supp. 1010, 1013 (S.D.N.Y. 1993) (finding that a corporation had standing to challenge the search of its own offices, despite the fact that those offices were unlocked and on a floor with other offices).

64. *See, e.g.*, United States v. Hamdan, 891 F. Supp. 88, 94-95 (E.D.N.Y. 1995) (noting that "standing" of a corporate officer to challenge a search of business's premises is generally found if the area searched is a personal and exclusive office).

helped to prepare.[65]

The standing requirement is quite problematic for employees, for it leaves them susceptible to invasive treatment and encourages the police to engage in illegal conduct. Law enforcement officials currently require neither search warrants nor probable cause to engage in workplace searches so long as the items seized are used only against employees who lack a privacy expectation in them. In *United States v. Payner*,[66] for instance, the IRS illegally confiscated a bank official's briefcase and used the contents of that briefcase against another individual.[67] The Supreme Court held that this conduct was permissible,[68] though the Court did not directly speak to the issue of whether the government had intentionally manipulated the standing requirement of the Fourth Amendment.[69] Allowing the police free reign to circumvent the Fourth Amendment in this fashion, whether done intentionally or unintentionally, threatens the ability of employees to feel safe and secure while at work. The "reality of work in modern time," when employees spend the better part of their days and much of their evenings at work, requires that employee privacy "be carefully safeguarded and not lightly set aside."[70] By prohibiting employees from objecting to illegally-seized corporate documents, the standing requirement ignores this reality and leaves important rights without protection.

B. HISTORY AND DEVELOPMENT OF EMPLOYEE STANDING LAW

Historically, interpretations of the Fifth Amendment suggested that employees would have few privacy protections under the Fourth Amendment. Early Fifth Amendment case law indicated that employees had little right to object to the seizure of corporate documents, under the theory that the documents were the property of the corporate entity alone. For instance, in *Wilson v. United States*,[71] an employee attempted to use his privilege against self-incrimination to avoid producing corporate books that were in his custody.[72] In rejecting the employee's argument, the Supreme

65. *See, e.g.*, United States v. Judd, 889 F.2d 1410, 1413 (5th Cir. 1989) (holding that a company president who helped prepare certain records lacked standing to challenge their seizure pursuant to an investigation of his company, for he did not work in the corporate bookkeeping office from which the records were seized).

66. 447 U.S. 727 (1980).

67. *Id.* at 729-30.

68. *Id.* at 731-32.

69. *See* YALE KAMISAR, WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, MODERN CRIMINAL PROCEDURE 751-52 (West Group 2002) (1965).

70. *See* O'Connor v. Ortega, 480 U.S. 709, 739 (1987) (Blackmun, J., dissenting).

71. 221 U.S. 361 (1911).

72. *Id.* at 377.

Court found that the self-incrimination privilege "undoubtedly" protected the employee against the compulsory seizure of "his private books and papers," but that the corporate books in question were not his private effects.[73] The Court reaffirmed this principle in another Fifth Amendment case, *Oklahoma Press Publishing Co. v. Walling, Wage & Hour Adm'r*[74] again holding that the privilege against self-incrimination does not protect employees from being compelled to produce corporate records.[75] This "property" conception of the Fifth Amendment was thought at first to extend to searches and seizures under the Fourth Amendment,[76] leaving employees with very few privacy protections indeed.

Beginning in the 1960's, however, the Court opened the door to employee protection by making it clear that the Fourth Amendment protects people, rather than property. In *Jones v. United States*,[77] the Court held that an individual had standing to contest the illegal search of an apartment despite the fact that he did not own the premises.[78] In so holding, the Court explicitly did away with the notion that to establish standing one must show legal possession or ownership of the searched premises.[79] Several years later, in the famous case of *Katz v. United States*,[80] the Court found that attaching a listening device to the outside of a public phone booth constituted a search within the meaning of the Fourth Amendment.[81] Noting that the Fourth Amendment protects people, not places,[82] the Court stated that "[wherever] a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[83] This definitive shift to the "privacy" conception of the Fourth Amendment meant that it was now appropriate to ask whether an employee had a reasonable expectation of privacy in an area searched.

Shortly after deciding *Katz*, the Court confronted the employee standing issue head-on in *Mancusi v. DeForte*.[84] In *Mancusi*, the

73. *Id.* at 377-78.
74. 327 U.S. 186 (1946).
75. *Id.* at 205.
76. *See, e.g.*, Warden v. Hayden, 387 U.S. 294, 304 (1967) (discussing the historical conception of the Fourth Amendment as protecting property and the subsequent doctrinal shift from property to privacy).
77. 362 U.S. 257 (1960), *overruled on other grounds by* United States v. Salvucci, 448 U.S. 83 (1980).
78. *See id.* at 263-64.
79. *Id.* at 265-67; *see also Mancusi*, 392 U.S. at 369.
80. 389 U.S. 347 (1967).
81. *Id.* at 359.
82. *Id.* at 351.
83. *Id.* at 359.
84. *Mancusi*, 392 U.S. at 364.

government had conducted a warrantless search of a Teamsters Union office, and had used the evidence seized to indict Union vice president Frank DeForte on charges of conspiracy, coercion and extortion.[85] The question before the Court was whether DeForte had Fourth Amendment standing to object to the allegedly unreasonable search and seizure of records from an office that he shared with several co-workers.[86] The Court noted first that, given its rejection of ownership as a prerequisite for standing,[87] DeForte would have had standing if he had "occupied a 'private' office in the union headquarters, and union records had been seized from a desk or a filing cabinet in that office . . . ."[88] The Court then reasoned that the situation was not "fundamentally changed" simply because DeForte shared his office with several other individuals.[89] Finally, the Court concluded that DeForte had standing because he could "reasonably have expected that only [his officemates and their guests] . . . would enter the office, and that the records would not be touched except with their permission or that of union higher-ups."[90]

The Court's holding in *Mancusi*, while in some ways a boon to privacy in the workplace, did not provide lower courts with a clear-cut method for determining employee standing. With *Mancusi*, the Court did resolve two key points in favor of employee rights: "First, a defendant without property rights to either the place searched or the item seized may have a sufficient expectation of privacy to establish standing in a workplace search. Second, the use of an area need not be exclusive in order for a defendant to have standing."[91] Thus, *Mancusi* left room for lower courts to extend standing to broader categories of employee defendants. However, because the Court did not elect to set forth a formal framework for evaluating employee standing, *Mancusi* also left room for lower courts to analyze standing stringently. The Court's holding in *Mancusi* and its failure to revisit the employee standing issue since then has ultimately led to divergent and often narrow treatments of the subject.[92]

---

85. *Id.* at 365.

86. *See id.* at 369.

87. *See Jones*, 362 U.S. at 265-67.

88. *Mancusi*, 392 U.S. at 369.

89. *Id.*

90. *Id.*

91. Michele Morris, *Constitutional Law - Employees' Fourth Amendment Rights Beyond Their Work Space: The Employment Relationship as a Source of Privacy Expectations*, 23 W. NEW ENG. L. REV. 191, 204 (2001).

92. The Court has subsequently addressed constitutional protections surrounding workplace searches, but only in the context of searches by public employers for work-related misconduct or for non-investigatory, work-related purposes. *See generally Ortega*, 480 U.S. 709. *Ortega* thus has no direct impact on *Mancusi*.

C. INTERPRETATIONS OF STANDING POST-*MANCUSI*

Post-*Mancusi*, the lower courts have applied at least two distinct frameworks of analysis to the employee standing issue. Specifically, the courts have differed over whether to use a "totality of the circumstances" approach or a "nexus" approach to assess legitimate expectations of privacy in the workplace context.[93] The totality of the circumstances approach[94] follows along the lines of Supreme Court standing jurisprudence in the non-workplace setting,[95] considering all the factors involved to see whether a privacy expectation exists. In a workplace setting, the totality of the circumstances could include "whether the employee has an ownership interest in the item seized, whether the employee took steps to guard [his or] her privacy, and whether the employee's position relative to the business gave [him or] her particular rights to the area searched."[96] The nexus approach[97] is more specifically tailored to the workplace environment, inquiring as to whether "the employee can demonstrate some 'nexus' between the area searched and their workspace."[98] A nexus may exist depending on the relationship between an area in question and one's employment activities.[99]

Neither the nexus nor the totality of the circumstances approach seems to be particularly sympathetic to employees seeking standing. For instance, the Kansas Supreme Court used the totality of the circumstances approach to find that a defendant did not have standing to challenge a search of a corporately owned warehouse.[100] Despite the fact that the defendant managed the warehouse and that the upper floors were not open to the public, the court reasoned that he did not have a reasonable expectation of privacy because the upper floors were each approximately the size of football field, he had no personal property stored there, and numerous corporate shareholders and employees also had access to the area.[101] Similarly, the Second Circuit used the nexus approach to conclude that a bank employee did not have standing to challenge a warrantless

93. Morris, *supra* note 91, at 208.

94. For an illustration of the "totality of the circumstances" approach, *see* United States v. Anderson, 154 F.3d 1225, 1232-34 (10th Cir. 1998).

95. *See generally Rawlings*, 448 U.S. 98.

96. Morris, *supra* note 91, at 208-09.

97. For an illustration of the "nexus" approach, *see* United States v. Britt, 508 F.2d 1052, 1055-56 (5th Cir. 1975).

98. Morris, *supra* note 91, at 213.

99. *Id.* at 213.

100. State v. Worrell, 666 P.2d 703, 705-06 (Kan. 1983).

101. *Id.* at 706.

search and seizure undertaken pursuant to an investigation of his bank.[102] The employee had some degree of proprietary interest in the bank, exercised significant operational control over the bank, and had ultimate control over the non-public areas searched.[103] Yet, the court was more persuaded by the fact that the employee knew the documents seized were subject to periodic examination by the Office of the Comptroller of the Currency, coupled with the fact that they were found in areas of the bank other than the employee's office.[104] As these cases illustrate, even employees with significant control or stake in a business cannot count on being able to challenge searches of their premises.

Moreover, despite the holding of *Mancusi*, the cases finding in favor of employee standing seem to be largely limited to those circumstances where the defendant has either exclusive use of an area or a significant proprietary interest at stake. In *United States v. Anderson*,[105] the Tenth Circuit held that the defendant had standing to challenge a warrantless search of a vacant room within his office building and the resultant seizure of videotapes; however, the defendant was alone in the locked building at the time, and had shut the door and covered the window to the room to maintain his privacy.[106] Thus, exclusive use played a key role in finding employee standing in *Anderson*, as it did in *United States v. Evaschuck*[107] and *United States v. Thomas*.[108] A strong proprietary interest, too, can weigh in favor of standing, as it did in *United States v. Lefkowitz*.[109] There, the Ninth Circuit considered a company president's ability to challenge a search and seizure undertaken during an investigation of the president and his several corporations for possible tax violations.[110] The court found that the president had standing to make such a challenge because he had a sufficient proprietary interest in the corporate suite from which the records

102. United States v. Chuang, 897 F.2d 646, 649-51 (2d Cir. 1990).

103. *Id.* at 650.

104. *Id.* at 650-51; *see also* United States v. Britt, 508 F.2d 1052, 1055 (5th Cir. 1975) (using the nexus approach to conclude that a company president had no standing to challenge the seizure of corporate records, and reaching that conclusion in part because the searches were directed at corporate activity generally rather than at him personally).

105. 154 F.3d 1225 (10th Cir. 1998).

106. *Id.* at 1233.

107. 65 F. Supp. 2d 1360, 1364-65 (M.D. Fla. 1999) (holding that defendant had standing to challenge search of corporate offices where defendant was the only person who used or had keys to those offices).

108. 746 F. Supp. 65, 67 (D. Utah 1990) (finding that defendant had standing to challenge search of his own personal office).

109. 618 F.2d 1313 (9th Cir. 1980).

110. *Id.* at 1315-16.

were seized.[111] The courts in *United States v. Willey*[112] and *United States v. Morton Provision Co.*[113] pointed to similar proprietary factors in ultimately deciding to rule in favor of standing in those cases. In practice, then, the lower courts have continued to gravitate towards property rights and exclusive use to resolve standing issues, despite *Mancusi*'s apparent extension of the standing doctrine beyond those two narrow categories.

The Supreme Court has also taken a narrow approach to standing since *Mancusi*. While the Court has not yet directly revisited *Mancusi*, it has issued two subsequent decisions on standing that may limit the *Mancusi* holding. First, in *Rakas v. Illinois*,[114] the Court held that car passengers who had neither a property nor a possessory interest in the automobile, and who had not demonstrated a legitimate expectation of privacy in the automobile, could not challenge a search of the glove compartment and the area under the seat.[115] In coming to this conclusion, the Court was harshly critical of *Jones*, stating that the *Jones* standard was so broad that it gave privacy expectations to even a casual visitor in a house.[116] The Court also signified a partial return to the "property" theory of the Fourth Amendment, commenting that "by focusing on legitimate expectations of privacy in Fourth Amendment jurisprudence, the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment."[117] This dictum may, in part, have caused lower courts to attach heightened importance to proprietary interests when evaluating employee standing.[118]

Even more limiting than the *Rakas* dictum may be the Court's decision in *Rawlings v. Kentucky*.[119] In *Rawlings*, the Court held that the petitioner did not have a legitimate expectation of privacy in an

111. *Id.* at 1316 n.2.

112. 57 F.3d 1374, 1390 n.30 (5th Cir. 1995) (holding that a debtor had standing to challenge the search of property that his corporation had purchased, given that the debtor's belongings were at the property on the day of the search).

113. 294 F. Supp. 385, 391-92 (D. Del. 1968) (finding that corporate officers had standing to object to a search where the officers were evidently the proprietors of the entire operations and had custody of the records in question at the time of the seizure).

114. 439 U.S. 128 (1978).

115. *Id.* at 128.

116. *Id.* at 142; *see also* Morris, *supra* note 91, at 205.

117. *Rakas*, 439 U.S. at 143 n.12; *see also* Morris, *supra* note 91, at 205.

118. The *Rakas* decision is also important for its apparent elimination of the analytical distinction between "standing" and the question of whether, with respect to a particular individual, there was a "search" for Fourth Amendment purposes. 439 U.S. at 138-40. For further discussion of this portion of *Rakas*, *see* discussion *infra* Part III, A.

119. 448 U.S. 98 (1980).

acquaintance's purse, despite the fact that his drugs were inside the purse.[120] On one hand, this holding re-affirmed the idea that privacy expectations do not automatically arise from property interests.[121] Yet, the opinion also indicated that access by others could diminish privacy expectations, for it attached importance to the fact that other people had access to the acquaintance's purse.[122] Applied in the workplace setting, this principle could mean that if other people have access to an office, an individual employee has no expectation of privacy in that office.[123] This idea of access goes directly back to the "exclusive use" concept, which *Mancusi* abandoned, but which lower courts analyzing employee standing have often relied upon. Thus, although the Supreme Court has not directly rejected *Mancusi*, its decisions in *Rakas* and *Rawlings* certainly appear to reduce employee privacy expectations.

D. USE OF THE STANDING DOCTRINE IN CORPORATE CRIMINAL INVESTIGATIONS

Diminished privacy expectations in the workplace, or lack of standing, has left employees without important Fourth Amendment protections. Corporate employees today are often unable to challenge potentially illegal searches of their company's premises. Unless the search is of the employee's personal office, or of an area in which the employee has an undeniably strong property interest, the employee cannot anticipate a court finding that he or she has a reasonable expectation of privacy that implicates the Fourth Amendment. As a result, police and prosecutors technically have the power to search the premises of businesses without a warrant or probable cause, and to use various documents found therein against individual workers.

So far, at least two important legal considerations have kept law enforcement officials from taking full advantage of this power in corporate criminal investigations. First, the good-faith exception to the exclusionary rule makes obtaining a search warrant a fairly desirable course of action in many cases. Under the good-faith exception, most evidence seized under a search warrant will be admitted, regardless of whether the police properly seized that evidence.[124] Accordingly, conducting a search and seizure

120. *Id.* at 106.
121. *Id.* at 105.
122. *See id.* at 104-05; *see also* Morris, *supra* note 91, at 206.
123. *See* Morris, *supra* note 91, at 206-07.
124. *See* United States v. Leon, 468 U.S. 897, 919-22 (1984) (finding a good faith exception to the exclusionary rule where an officer's reliance on a warrant issued was objectively

pursuant to a warrant is a way of ensuring that the items seized can almost always be used, and may be an especially prudent course of action where officials are unsure of exactly who they are targeting. Second, when officials know they want to target a business entity as well as individual employees for criminal conduct, officials must be mindful of "corporate standing." The doctrine of corporate standing, which frequently allows corporations to challenge illegal searches of business premises,[125] may prevent the police from conducting illegal warrantless searches when the corporation itself is a known subject of the investigation. Nevertheless, police and prosecutors have free reign to make use of the employee standing doctrine in certain types of investigations, such as those targeting only specific employees or those where a corporation consents to a search. A company's decision to consent to a search,[126] which may result from a desire to appear cooperative and to maintain good public relations,[127] is an especially perilous prospect for its employees. In general, a third party's authority to consent to a warrantless search "rests . . . on mutual use of the property by persons generally having joint access or control for most purposes, so that . . . the others have assumed the risk that one of their number might permit the common area to be searched."[128] Courts have interpreted this language to mean that, in the employment context, an organization may consent to a search where the employee has no reasonable expectation of privacy in the place or object at issue.[129] Thus, although a company cannot waive an employee's Fourth Amendment rights

---

reasonable). *But see* United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (noting that in *Leon*, "[t]he United States Supreme Court recognized that in some circumstances a warrant may be so facially deficient – i.e., failing to particularize the place to be searched or the things to be seized – that the executing officer cannot reasonably presume it to be valid" (quotations omitted)).

125. *See, e.g.*, *Zhang*, 833 F. Supp. at 1013.

126. *See generally* Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (illustrating the concept of voluntary consent to a search).

127. *See* MANAGING THE FALLOUT: THE CRIMINAL INVESTIGATOR'S KNOCK ON THE DOOR MAY ONLY BE THE FIRST OF MANY, 127, 130-33 ("Criminalization" of Civil Law Claims) April 18, 1991 (discussing the importance of public relations "damage control" for a company under criminal investigation, and observing that poor handling of the media can multiply a company's difficulties by attracting the attention of other governmental agencies, shareholders, and other third parties).

128. United States v. Matlock, 415 U.S. 164, 171 n.7 (1974).

129. *See* United States v. Bilanzich, 771 F.2d 292, 296 (7th Cir. 1985) (finding that an employer had given valid consent to a search where the employee had no reasonable expectation of privacy in the area searched and the items seized); Donovan v. A.A. Beiro Constr. Co., 746 F.2d 894, 899 (D.C. Cir. 1984) (stating that in determining whether a worksite owner had the power to consent to a search, the inquiry focused upon determining the employee's reasonable expectations of privacy).

where those rights exist,[130] securing consent from a company is a way of getting at both corporations and employees where the relevant employees lack Fourth Amendment protections. Given that employees frequently do lack standing to challenge illegal searches,[131] corporate consent creates a significant opportunity to exploit the employee standing doctrine and to circumvent the Fourth Amendment in business crime investigations.

III. TECHNOLOGICAL ADVANCEMENTS IN THE WORKPLACE AND ASSOCIATED THREATS TO EMPLOYEE PRIVACY

A. APPLYING STANDING TO COMPUTER-RELATED TECHNOLOGY

The reasonable expectation of privacy test applies not only to a general area searched but also to items or activities taking place within that area.[132] The employee standing doctrine[133] has been used primarily to describe privacy expectations in a general area searched (*i.e.*, a particular part of the business premises such as the employee's own office). In some cases, though, even if an employee has sufficient privacy interests in an area, the Fourth Amendment still might not apply to a search of specific items or activities. For instance, an employee with standing to contest a search of his office might not be able to object to the search and seizure of the computer within that office; he might lack a reasonable expectation of privacy in the contents of that computer.[134]

Notably, *Rakas v. Illinois*[135] seems to have eliminated the notion that the "standing" inquiry is distinct from other Fourth Amendment inquiries into privacy expectations.[136] In *Rakas*, the Supreme Court determined that "the type of standing requirement discussed in *Jones* . . . is more properly subsumed under substantive Fourth Amendment doctrine."[137] The Court observed that the inquiry in *Katz*, which focused on whether a person in a

130. *See* United States v. Block, 590 F.2d 535, 539 n.5 (4th Cir. 1978) (observing that "when [a] third person 'consents' to search, this does not thereupon vicariously waive an existing Fourth Amendment right in the search victim"); United States v. Blok, 188 F.2d 1019, 1021 (D.C. Cir. 1951) (holding that an employee's superiors could not validly give consent to a search of the desk assigned to her exclusive use).

131. *See* discussion *infra* Part II, C.

132. *See, e.g.*, *Katz*, 389 U.S. at 352 (finding a reasonable expectation of privacy in the contents of a telephone call).

133. *See* discussion *supra* Part II.

134. *See Angevine*, 281 F.3d at 1134-35 (holding that a professor had no expectation of privacy in his university-issued computer).

135. 439 U.S. 128 (1978).

136. *Id.* at 138-39.

137. *Id.* at 139.

telephone booth may rely on Fourth Amendment protections, and the inquiry in *Mancusi*, which focused on employee standing to challenge a search, was essentially the same.[138] Given this observation, the Court concluded that "the better analysis forthrightly focuses on the extent of a particular defendant's rights under the Fourth Amendment, rather than on any theoretically separate, but invariably intertwined concept of standing."[139] Probably for ease of reference, however, lower courts have continued to speak of an employee's Fourth Amendment right to challenge the search of a particular area as "standing."

In light of *Rakas*, the ability to challenge searches of e-mail and computers in the workplace may be seen as an extension of the employee standing doctrine, but it also raises additional and significant concerns. The question for these purposes is whether an employee has Fourth Amendment rights with respect to items or activities within or originating from a location, regardless of whether that employee has Fourth Amendment rights with respect to the location in general. Although this question is not a new one (*i.e.*, it has long been asked with regard to telephone calls), its importance has risen dramatically in recent years as employees have become more dependent on computers and the Internet. While at work, employees are turning to e-mail and the Internet as the most efficient way to manage their personal and business affairs.[140] E-mail has become increasingly popular and widespread as a business tool, "replac[ing] the inter-office memorandum as the preferred method of communication in corporate America."[141] In addition, "[o]ver 85 percent of adults send or receive personal e-mail messages at work."[142] Computer usage, too, is quickly growing, with employers everywhere "experiencing an explosion in the growth of electronic data and networked computer systems . . . ."[143] Courts are attempting to apply the reasonable expectation of privacy test to both computers and e-mail, but given the rapid development of these advancements and their pervasiveness in the organizational setting, the traditional test has not been flexible enough to retain the appropriate employee protections.[144] Indeed, for employees "in

138. *Id.* at 139 n.7.

139. *Id.* at 139.

140. Isajiw, *supra* note 3, at 75.

141. Matthew H. Meade, *"I've Got My Eye on You" – Workplace Privacy in the Electronic Age,* 691 P.L.I./P.A.T. 225, 227 (2002).

142. Isajiw, *supra* note 3, at 75.

143. Rod Dixon, *With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age*, 4-S.P.G. J. TECH. L. & POL'Y 1, 10 (1999).

144. *See* Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 DRAKE L. REV. 239, 241-42, 278

today's . . . computerized world, the potential danger to individual privacy interests exists at a level never before seen."[145]

B. SEARCHES OF E-MAIL IN GENERAL

At the outset, there has been some debate as to how and when there is ever a reasonable expectation of privacy in e-mail. If sending an e-mail from a computer is akin to making a phone call behind closed doors, the Supreme Court's opinion in *Katz* means that e-mail should implicate the Fourth Amendment.[146] Certain iterations of e-mail, such as instant messaging, fit well with the phone call analogy because they are real-time communications that typically do not leave a trace.[147] However, more traditional e-mail is distinct from a phone call in that it is written and has more permanence.[148] Accordingly, courts thus far have tended to analogize e-mail to letters rather than phone calls.[149] While letters are in the "general class of effects" protected by the Fourth Amendment, "[when] a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery."[150] The expectation of privacy will terminate even in cases where "the sender may have instructed the recipient to keep the letters private."[151] Under this framework of analysis, someone sending an e-mail loses a legitimate expectation of privacy in that e-mail once it has reached its recipient.[152]

In the non-workplace setting, at least two notable cases have articulated and explained the "e-mail as letter" analogy. First, in *United States v. Maxwell*,[153] the United States Court of Appeals for the Armed Forces held that an Air Force officer had a reasonable expectation of privacy, albeit a limited one, in e-mail messages that he sent or received on an Internet service provider's computer subscription service.[154] While the

(2000).

145. Kevin J. Baum, *E-Mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1012 (1997).

146. *See* Scott A. Sundstrom, *You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2081 (1998).

147. *See id.* at 2080.

148. *Id.* at 2082; *see also* Peter Schnaitman, *Building a Community Through Workplace E-Mail: The New Privacy Frontier*, 5 MICH. TELECOMM. & TECH. L. REV. 177, 180 (1999) (stating that "[e]-mail is more permanent than even a paper document").

149. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

150. United States v. King, 55 F.3d 1193, 1195-96 (6th Cir. 1995).

151. *Id.* at 1196.

152. *Guest*, 255 F.3d at 333.

153. 45 M.J. 406 (C.A.A.F. 1996).

154. *Id.* at 417-19.

court was "satisfied" that the Constitution required probable cause to search a personal and private computer, it noted that "when an individual sends or mails letters, messages, or other information on the computer, that Fourth Amendment expectation of privacy diminishes incrementally."[155] Analogizing e-mail to letters, the court concluded that the Air Force officer had a reasonable expectation that police officials would not intercept messages on the Internet service provider's server, because that would be like intercepting a letter en route.[156] However, the officer had no reasonable expectation of privacy in e-mails received by another person; "thus, any of the material or information seized and turned over to the FBI or to other police agencies by Mr. Dietz was 'fair game' for introduction into evidence and for use in procuring a search warrant."[157]

The court in *United States v. Charbonneau*[158] took this analysis one step farther, holding that an individual does not have a reasonable expectation of privacy in e-mails sent to an undercover agent in an Internet chat room.[159] Quoting extensively from the *Maxwell* decision, the *Charbonneau* court reiterated the idea that e-mail was "almost equivalent" to a letter, and that "the expectations of privacy in e-mail transmissions depend in large part on both the type of e-mail sent and the recipient of the e-mail."[160] From this premise, the court concluded that when the defendant engaged in chat room conversations, he "ran the risk of speaking to an undercover agent."[161] Further, the court decided as a general principle that individuals could never have a reasonable expectation of privacy in chat rooms.[162] The *Charbonneau* decision was thus even less privacy-protective than the *Maxwell* decision, for *Charbonneau* categorically excepted certain types of e-mail from Fourth Amendment protection.

Apart from these Fourth Amendment cases, there has also been at least one relevant case addressing the Federal Wiretap Act, a statute that theoretically offers an additional form of e-mail protection separate and apart from the Fourth Amendment. The Federal Wiretap Act was enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[163] The Federal Wiretap Act originally limited the circumstances in which a

155. *Id.* at 417.
156. *See id.* at 418.
157. *Id.* at 419.
158. 979 F. Supp. 1177 (S.D. Ohio 1997).
159. *Id.* at 1184-85.
160. *Id.* at 1185.
161. *Id.*
162. *Id.*
163. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended in 18 U.S.C. §§ 2510-2520 (2002)).

court could order a telephone wiretap,[164] but was amended in 1986 to cover "electronic communications" as well.[165] While the Federal Wiretap Act technically does prohibit unauthorized searches of e-mail, the Fifth Circuit has implied that the statute's scope might not be that expansive in this regard. In *Steve Jackson Games, Inc. v. United States Secret Service*,[166] the Fifth Circuit considered the Secret Service's search of e-mail stored on the hard drive of a computer seized from a company offering an electronic bulletin board service.[167] Holding that the search did not violate the Federal Wiretap Act, the court observed that the statute prohibited only "real-time" interceptions of electronic communications, i.e., interception of the communications while in transmission.[168] The court concluded that, because the e-mail that the Secret Service had reviewed was in storage rather than in transmission, the Federal Wiretap Act did not apply.[169] Given this holding, the Federal Wiretap Act would seem to be of limited use to employees who wish to challenge searches of their workplace e-mail.

Even taken together, the Federal Wiretap Act and the Fourth Amendment do not seem to offer extensive privacy protections for e-mail in the non-workplace setting. Under the Fourth Amendment, e-mail is not protected once it falls into the hands of another person[170] or into the hands of the public at large.[171] Under the Federal Wiretap Act, e-mail is only protected if it is "in transmission."[172] Thus, outside the workplace, the case law so far seems to say that only e-mail in transmission or e-mail stored on a home computer would necessarily be shielded from unreasonable searches.

C. SEARCHES OF WORKPLACE E-MAIL

While courts have begun to address privacy expectations in e-mail generally, there is little case law to date about how the Fourth Amendment (or the Federal Wiretap Act) impacts e-mail in the workplace. The best cases on this topic, thus far, have been in the employer-monitoring context.

164. *See* S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-56.
165. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(a)(6)(c), 100 Stat. 1848, 1848-49 (1986).
166. 36 F.3d 457 (5th Cir. 1994).
167. *Id.* at 458.
168. *Id.* at 461-63.
169. *Id.*
170. *See Maxwell*, 45 M.J. 417-19.
171. *See Charbonneau*, 979 F. Supp. at 1184-85.
172. *See Steve Jackson Games*, 36 F.3d at 461-62.

Although some of these cases are civil, and therefore do not implicate the Fourth Amendment, they at least present an initial picture of how courts have treated e-mail in a workplace setting. So far, employee e-mail seems to receive even less protection than e-mail outside the workplace.

Indeed, in several civil cases, courts have given employers free reign to search employee e-mail. For instance, in *Smyth v. Pillsbury Co.*,[173] the court found that an employer permissibly terminated an at-will employee for transmitting inappropriate and unprofessional comments over the company e-mail system.[174] The court concluded that, notwithstanding assurances that management would not intercept such communications, the plaintiff did not have a reasonable expectation of privacy in his work e-mail.[175] In reaching this conclusion, the district judge reasoned "once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."[176] *McClaren v. Microsoft Corp.*[177] echoed those sentiments, holding that there can be no reasonable expectation of privacy in an employer-owned e-mail system.[178] Going perhaps a step further than *Smyth*, the court in *McClaren* also found that even employees who create a personal password for their e-mail have no way of preventing employers from reviewing their messages.[179]

The low privacy interest afforded to e-mail during private employer searches has translated almost directly into the public employer context, where the Fourth Amendment is implicated. In *United States v. Monroe*,[180] the court examined an Air Force employee's Fourth Amendment challenge to a search of his e-mail messages and e-mail box.[181] The court held that the employee "had no reasonable expectation of privacy in his [workplace] e-mail messages or . . . box at least from the [government] personnel charged with maintaining the . . . system."[182] Further, the court in *Bohach*

173. 914 F. Supp. 97 (E.D. Pa. 1996).
174. *Id.* at 101.
175. *Id.*
176. *Id.*
177. No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (Tex. App. May 28, 1999).
178. *Id.* at *9-12.
179. *Id.* at *12; *cf.* Sundstrom, *supra* note 146, at 2085 (suggesting that, because e-mail systems with no password leave messages in plain view, employee users of such systems should have no reasonable expectation of privacy).
180. 52 M.J. 326 (C.A.A.F. 2000).
181. *Id.* at 329.
182. *Id.* at 330.

v. City of Reno[183] found that police officers suffered no injury either under the Fourth Amendment or under the Federal Wiretap Statute when their government employer accessed their e-mail messages.[184] Insofar as the Fourth Amendment claim was concerned, the court held that while the officers had a subjective expectation of privacy, they did not have a "reasonable" expectation of privacy when using the Alphapage message system.[185] The court then rejected the Federal Wiretap Statute claim on the grounds that searching "electronic storage" did not fall under the statute's prohibitions on interception of electronic communications.[186]

Notably, in both *Bohach* and *Monroe*, the government employer had somehow warned the employees that their e-mail would not be kept private. In *Bohach*, the court relied on the fact that the police department had notified all Alphapage users that their messages would be stored on the network[187] – absent this fact, perhaps the court would not have found the officers' privacy expectation "unreasonable." Likewise, in *Monroe*, a key consideration for the court seemed to be that the employees received a specific notice from their employer that all users logging onto the e-mail system "consent[ed] to monitoring . . . ."[188] Other courts, as well, have relied on "the presence or absence of search-authorizing notices or regulations in determining whether a government employee has a reasonable expectation of privacy in a work area."[189] Therefore, while e-mail privacy expectations are evaluated on a case-by-case basis, an employer's failure to notify employees of e-mail monitoring may move a court to rule in favor of privacy protection.

In addition, the public employer cases must be viewed in light of the United State Supreme Court's decision in *O'Connor v. Ortega*.[190] In *Ortega*, the Court considered the 42 U.S.C. § 1983 claim of a hospital supervisor who contended that his public employer's search of his office violated the Fourth Amendment.[191] In analyzing this question, the Court noted that "[t]he operational realities of the workplace . . . may make *some* employees' expectations of privacy unreasonable when an intrusion is by a

183. 932 F. Supp. 1232 (D. Nev. 1996).
184. *Id.* at 1236-37.
185. *Id.* at 1234.
186. *Id.* at 1236.
187. *Id.* at 1234.
188. *Monroe*, 52 M.J. at 330.
189. Ralph V. Seep, *Warrantless Search by Government Employer of Employee's Workplace Locker, Desk, or the Like as Violation of Fourth Amendment Privacy Rights – Federal Cases*, 91 A.L.R. FED. 226, 2 (1989).
190. 480 U.S. 709 (1987).
191. *Id.* at 712-14.

supervisor rather than a law enforcement official."[192] The Court then remanded the case so that the following new standard could be applied: "public employer intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."[193] Thus, the public employer cases might have come out differently if government agents, rather than government employers, had conducted the e-mail searches.

Nonetheless, the overall judicial trend against e-mail privacy rights does not bode well for employee privacy. Although *Bohach* and *Monroe* were both public employer cases, neither mentioned the *Ortega* decision and both referenced the familiar Fourth Amendment "reasonable expectation of privacy" language.[194] This implies, perhaps, that the line between the public employer context and the investigative search context is not so sharply drawn, and that courts may ultimately apply the same standard for e-mail in both settings. Indeed, one court has recently blurred the line between the two settings rather overtly, holding that an employee lacked standing to challenge the warrantless seizure of business records by the government, but relying on *Ortega* to support its analysis.[195] Moreover, if employer notifications/warnings continue to be the linchpin of the privacy expectation analysis, employee e-mail will likely remain largely unprotected. Companies have an interest in being able to search employee e-mail,[196] and correspondingly, an interest in giving warnings that could eliminate an employee's reasonable expectation of privacy in that e-mail. In sum, if future government search cases proceed in a remotely similar manner as the cases decided so far, the outlook for privacy expectations in workplace e-mail appears bleak. Given the fact that e-mail "is rapidly supplementing, and often replacing, traditional forms of personal and business communication,"[197] such as telephone calls, the decision to assign a low expectation of privacy to e-mail will leave employees with even fewer privacy rights at work than they enjoyed in the past.

---

192. *Id.* at 717.

193. *Id.* at 725-26.

194. *See Bohach*, 932 F. Supp. at 1234-35; *Monroe*, 52 M.J. at 330.

195. *See* United States v. Cooper, 283 F. Supp. 2d 1215, 1244-48 (D. Kan. 2003).

196. *See* Paul E. Hash & Christina M. Ibrahim, *E-Mail, Electronic Monitoring, and Employee Privacy*, 37 S. TEX. L. REV. 893, 897 (1996) (noting the corporate world's interest in electronically monitoring employees in order to, among other things, measure productivity, efficiency, and quality control).

197. Sundstrom, *supra* note 146, at 2064.

D. SEARCHES OF WORKPLACE COMPUTERS

Whether an employee has a reasonable expectation of privacy in his office computer seems to depend, first and foremost, on company practices and policies. As an illustration, if a company does not require passwords to access data on each computer, the "plain view" doctrine might apply.[198] Under the plain view theory, there would be no reasonable expectation of privacy in computerized information that all employees could access freely, because the information would essentially be in plain view. However, because most employers do provide their employees with individual passwords, this situation is fairly rare.[199] As with e-mail, a more typical scenario where an employer's policy may be dispositive is where the employer takes an official stance on workplace monitoring, as reflected either by words or by actions.

If an employer has an actual practice of searching workplace computers, that practice is likely to cut against a reasonable expectation of privacy. In *Leventhal v. Knapek*,[200] for instance, a state agency employee brought a § 1983 action against his agency and various agency officials alleging Fourth Amendment violations arising out of the search of his workplace computer.[201] The Second Circuit found that, based on the particular facts of the case at hand, the employee did have a reasonable expectation of privacy in the contents of his office computer.[202] However, crucial to the court's holding was the fact that the company performed only infrequent and selective searches for maintenance or document retrieval purposes; it did not have a "general practice of routinely conducting searches of office computers."[203] Had the employer adopted different search tactics in practice, the court might well have decided the *Leventhal* case in the reverse.

Moreover, when a company has an official policy of monitoring computers, courts tend to find that the company's employees do not have reasonable privacy expectations in those computers. For example, the Fourth Circuit held in *United States v. Simons*[204] that an employee did not have a legitimate expectation of privacy in his office computer files.[205]

198. *See* Bayens, *supra* note 144, at 242-43.
199. *See id.* at 243.
200. 266 F.3d 64 (2d Cir. 2001).
201. *Id.* at 70-71.
202. *Id.* at 73.
203. *See id.* at 74.
204. 206 F.3d 392 (4th Cir. 2000).
205. *Id.* at 398.

"The critical factor in reaching this result was the stated policy of the employer."[206] This policy, which clearly stated that the company "would 'audit, inspect, and/or monitor' employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, 'as deemed appropriate[,]' . . . placed employees on notice that they could not reasonably expect that their Internet activity would be private."[207] In a Fourth Amendment setting, observed the court, "office practices, procedures, or regulations may reduce legitimate privacy expectations" for a government employee.[208]

Although *Simons* and *Leventhal* involved public employer searches implicating the *O'Connor v. Ortega*[209] framework,[210] recent cases have applied a similar analysis to genuine police searches. While these cases have concerned child pornography, rather than truly "corporate" crimes, they nonetheless shed light on the general treatment of police-initiated workplace computer searches. For instance, in *United States v. Angevine*,[211] the Tenth Circuit found that, because of a university's explicit policy reserving a right to access any university-owned computer on a need to know basis, a professor did not have a reasonable expectation of privacy in his university-issued computer.[212] As a result, the professor could not contest a police search of that computer.[213] Interestingly, the *Angevine* court referenced the *Ortega* decision,[214] implying that, at least insofar as computers are concerned, the relaxed *Ortega* standard has now migrated into the investigative search context. Even more recently, in *United States v. Bailey*,[215] the United States District Court for the District of Nebraska denied an employee's motion to suppress evidence gathered in a police search of his workplace computer.[216] In finding that the employee had no reasonable expectation of privacy in that computer, the court pointed to the fact that his employer had informed him on multiple occasions that employees' computers could be searched.[217] The court stated that employees "have no objectively reasonable basis to believe that their

206. RAYMOND T. NIMMER, LAW OF COMPUTER TECHNOLOGY § 12:5 (2002).
207. *Simons*, 206 F.3d at 398.
208. *Id.*
209. 480 U.S. 709 (1987).
210. *See supra* Part III, C.
211. 281 F.3d 1130 (10th Cir. 2002).
212. *Id.* at 1134-35.
213. *See id.* at 1135.
214. *See id.* at 1134.
215. 272 F. Supp. 2d 822 (D. Neb. 2003).
216. *Id.* at 837.
217. *Id.* at 836.

activities on a company computer are private when, through the company's screen notification, they have actual knowledge that the computer can be searched . . . ."[218] Like the *Angevine* court, the *Bailey* court referenced the *Ortega* case.[219]

Besides looking at company policies and practices to analyze office computer searches, courts may choose to revert back to more traditional approaches to employee standing. One court appeared to do so in *United States v. Criminal Triumph Capital Group*,[220] a public corruption case in which a corporation and several employees were charged with bribery, racketeering, and numerous other offenses.[221] The court found that, absent evidence that the CEO and controlling shareholder of the corporation had any personal or proprietary interest in a company-issued laptop, the CEO lacked standing to challenge a search of the laptop's hard drive.[222] This analysis shows that the property rights/exclusive use requirement still has life in the realm of computer searches, despite the fact that most courts are analyzing these searches in terms of company policies and practices. Neither approach, though, appears to grant employees many privacy protections.

E. IMPLICATIONS OF THE E-MAIL AND COMPUTER SEARCH JURISPRUDENCE FOR CORPORATE CRIMINAL INVESTIGATIONS

To date, employees appear to have alarmingly limited Fourth Amendment rights in their workplace e-mail and computers. While the case law on these matters is still in the early stages of development, the decisions so far have indicated that employees will typically have an uphill battle in demonstrating reasonable expectations of privacy in these modern workplace technologies. The constraints on Fourth Amendment protections in this realm are disconcerting given that, in the modern workplace, an employee may do the bulk of his written work on his office computer and a large portion of his professional and personal correspondence via his office e-mail account.[223] Like the employee

218. *Id.*
219. *Id.* at 835.
220. 211 F.R.D. 31 (D. Conn. 2002).
221. *Id.* at 35-36.
222. *Id.* at 53-54.
223. *See, e.g.*, United States v. Hunter, 13 F. Supp. 2d 574, 581 (D. Vt. 1998) (observing that today, "computers and computer disks store most of the records and data belonging to businesses and attorneys"); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 290 (2002) (stating that in the year 2000, "forty million American employees sent sixty billion e-mails").

standing doctrine, the limited employee protections associated with these activities threaten fundamental workplace privacy rights[224] and interfere with employee dignity and autonomy.[225]

In certain types of business crime investigations, law enforcement officials already have a legal basis for taking advantage of these limited protections. An organization's own privacy rights can protect employees not only from the negative effects of the employee standing doctrine,[226] but also from the lack of employee privacy protection in e-mail and computers; for instance, if a company wants to object to the search of a workplace computer, the "corporate standing" doctrine will likely make such an objection possible. Yet, where a company gives consent to a search or where a search targets specific, individual employees,[227] the door opens for police and prosecutors to take advantage of the low expectations of privacy afforded to employees using e-mail and computers at work. In these instances, the Fourth Amendment may be of little use to the corporate employees being investigated.

IV. THE EFFECT OF THE USA PATRIOT ACT ON AN ORGANIZATION'S ABILITY TO PROTECT ITS EMPLOYEES

In business crime investigations to date, the corporate entity has enjoyed some success in its role as an indirect protector of employee privacy. Particularly at the inception of such an investigation, law enforcement officials are unlikely to know whether they should target the corporation, the employees, or all of the above. Perhaps this uncertainty is a large part of what motivates officials to proceed cautiously. Rather than risk warrantless searches, which could be subject to a Fourth Amendment challenge, officials conducting business crime investigations have often either sought out search warrants or obtained grand jury subpoenas before proceeding.[228] Getting a search warrant is also a good plan for risk-adverse prosecutors in light of the good-faith exception to the exclusionary rule, which usually allows evidence seized under a search warrant to be admitted in court.[229] As a result, the limited employee privacy protections discussed above have not always come into play.

---

224. *See Ortega*, 480 U.S. at 739.

225. *See, e.g.*, Sundstrom, *supra* note 146, at 2066 (observing that e-mail monitoring may affect the ability of employees to maintain dignity and autonomy in the workplace).

226. *See supra* Part II.D.

227. *See id.*

228. *See* Ronald H. Levine, *Practice Tips the Unwary Records Custodian – Pitfalls for Potential Targets*, BUSINESS CRIMES LAW REPORT NOW (Aug. 2002).

229. *See supra* Part II.D.

However, the recently enacted USA Patriot Act ("Patriot Act")[230] threatens the ability of organizations to act as protective shields for their employees. The Patriot Act, passed in response to the September 11, 2001 terrorist attacks on the United States, was designed "to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."[231] As it relates to the domestic workplace, the Patriot Act "gives the government enhanced surveillance powers that may affect every employer and provider of Internet communications."[232] While the Patriot Act will likely affect employee privacy expectations on an individual basis, its more significant effect may be on the role of organizations as a deterrent to potentially illegal workplace searches.

Several provisions of the Patriot Act directly alter corporate crime investigation procedures in America. For instance, section 209 of the Patriot Act removes stored voicemail messages from the requirements of Title III, amending section 2510 of the Federal Wiretap Act accordingly.[233] This change means that the analysis in *Steve Jackson Games, Inc. v. United States Secret Service*,[234] where the Fifth Circuit concluded that the Federal Wiretap Act did not protect stored e-mail,[235] now applies to stored voicemail as well.[236] In addition, section 213 of the Patriot Act allows for delayed notification of the exercise of search warrants.[237] Under Federal Rule of Criminal Procedure 41(e), a person whose property is searched must be given notice whenever a search takes place.[238] By contrast, under Patriot Act § 213, notice may now be delayed in certain circumstances,[239]

---

230. *See* Patriot Act *supra* note 12.

231. *Id.*

232. R.J. Cinquegrana & Richard M. Harper II, *The USA Patriot Act: Affects* [sic] *on American Employers and Businesses*, 46 B. B.J. 10, 10 (May/June 2002).

233. *See* Patriot Act § 209.

234. 36 F.3d 457 (5th Cir. 1994).

235. *Id.* at 461-62.

236. *See* Cinquegrana, *supra* note 232, at 10.

237. *See* Patriot Act § 213.

238. FED. R. CRIM. P. 41(e).

239. Patriot Act § 213. A delay of notification may be granted if:

> (1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result . . . (2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication . . . or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and (3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.

Id.

thus "authorizing law enforcement officials to conduct a search secretly."[240] Finally, section 214 of the Patriot Act expands the pen register statute to include addressing information in Internet communications such as e-mail and web browsing.[241] In *Smith v. Maryland*,[242] the United States Supreme Court held that the use of pen registers, which record the numbers dialed from telephones, does not constitute a search for Fourth Amendment purposes.[243] Patriot Act § 214 extends the logic of *Smith* to the Internet and e-mail context; however, critics have pointed out that the "connection contained in URL addresses will inevitable [sic] disclose much more information than traditional pen register and trap and trace devices."[244]

Particularly significant for corporate investigations, though, is section 217 of the Patriot Act. Patriot Act § 217 allows government agents to engage in extrajudicial monitoring of e-mail traffic for the purpose of investigating a computer trespasser.[245] Under this provision, the government can engage a computer's owner, such as an employer, to intercept the wire or electronic communications of a computer trespasser without either a search warrant or a wiretap order.[246] "Computer trespasser" is broadly defined as "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer . . . ."[247] Given this expansive definition, a "computer trespasser" could conceivably be any employee who uses a workplace computer that he does not have express authorization to use, such as his officemate's computer. This provision of the Patriot Act thus effectively gives "a company maintaining an e-mail system, or a computer-based telephone or voicemail system [the power to] . . . authorize the government to intercept real time e-mail communication and voicemail without any judicial involvement."[248]

Section 217 seriously threatens the ability of employers to protect employee privacy at work. The practical effect of this provision, while somewhat analogous to the effect of a company's consent to a search, spans

240. Cinquegrana, *supra* note 232, at 11.

241. John B. Kennedy & Mary Wong, *Recent Developments in U.S. Privacy Law, Including Post-September 11, 2001*, 701 P.L.I./PAT 11, 48 (2002) [hereinafter Kennedy]. *See* Patriot Act § 214.

242. 442 U.S. 735 (1979).

243. *Id.* at 745-46.

244. Kennedy, *supra* note 241, at 48.

245. Patriot Act § 217.

246. *See id.*

247. *Id.*

248. Cinquegrana, *supra* note 232, at 12; *see also* Kennedy, *supra* note 241, at 48.

far beyond the traditional notion of consent. Now, it seems that the government can request that a company's system be monitored on a real-time basis, potentially without employee knowledge and for an unspecified amount of time. When taken in conjunction with sections 209, 213 and 214, section 217 chips substantially away at the employer's ability to preserve Fourth Amendment and statutory privacy protections for employees.

In sum, where the Patriot Act applies, it effectively pierces the shield of company protection. When law enforcement officials are acting pursuant to the Patriot Act, typical concerns about violating the privacy rights of business entities may not be implicated. To illustrate, suppose that the government, pursuant to Patriot Act § 217, secures company cooperation to monitor an employee's e-mail and voicemail. After obtaining certain investigation-related facts through the monitoring process – which may be conducted in secret, under Patriot Act § 213 – the government may then want to conduct a workplace search. By that point, the government may have a clearer idea of its targets, which may not include the business entity. [249] Under this set of circumstances, officials conducting an investigation can and may choose to circumvent the Fourth Amendment altogether.

V. CONCLUSION: PREVENTING DAWN RAIDS IN AMERICA

For American employees, the Fourth Amendment is more comforting in theory than in practice. Serious exceptions to Fourth Amendment protection, such as the employee standing requirement to challenge a search and the limited privacy expectations in workplace e-mail and computers, make employees vulnerable to government intrusions in their business affairs. Moreover, while an employee's business entity can protect him or her to some extent, legislation such as the USA Patriot Act gives prosecutors more incentive and ability to bypass even those protections. Given these developments, the American legal framework for corporate criminal investigations is closer to permitting a dawn raid than many Americans might believe.

This EU tactic is one that we should be hesitant to adopt. While dawn raids do seem to be effective investigative tools, the fact that EC officials need not obtain search warrants, particularize their searches, or have probable cause to search is cause for serious concern. These facets of a

249. Notably, the results of the monitoring may have furnished investigators with probable cause to secure a warrant. Nonetheless, the investigators would still have the option of conducting a warrantless, and possibly illegal, search if necessary.

dawn raid conflict directly with the Fourth Amendment and with long-cherished American ideas of privacy.

United States law enforcement officials, however, may one day take a more "dawn raid"-like approach to corporate criminal investigations if the loopholes in our Fourth Amendment jurisprudence are not addressed and corrected. Obtaining either a search warrant or a grand jury subpoena is a burdensome, time-consuming task, and understandably, many officials in this country might prefer a simpler approach to business crime investigations. A simpler approach could prevent problems like document shredding, which seems to have occurred in the Arthur Andersen case. Thus, if our Fourth Amendment jurisprudence continues to give police and prosecutors ways to avoid the text of the Fourth Amendment, they may ultimately have both the opportunity and the incentive to conduct "dawn raid"-like searches on businesses. Unless courts begin to give corporate employees privacy protections that comport with traditional Fourth Amendment ideals, we may soon see dawn raids here at home.