

**RECENT DEVELOPMENTS IN
PRIVACY RIGHTS IN THE PUBLIC SECTOR WORKPLACE
RELATED TO ELECTRONIC COMMUNICATIONS**

January 2001

By Raymond L. Hogge, Jr.
Payne, Gates, Farthing & Radd, P.C.
Attorneys and Counsellors at Law
Dominion Tower, Suite 1515
999 Waterside Drive
Norfolk, Virginia 23510-3309
(757) 640-1500
RHogge@PayneGates.com
www.VirginiaLaborLaw.com

**This article is intended solely for educational purposes,
and does not constitute or contain legal advice.**

Introduction

“The Fourth Amendment prohibits unreasonable searches and seizures by government agents, including government employers or supervisors.” *United States v. Simons*, No. 99-4238, 206 F.3d 392 (4th Cir. 2/28/00). The courts have interpreted this prohibition on unreasonable searches and seizures to grant to public sector employees a constitutional right of privacy in the workplace. (This right normally does not extend to private sector workplaces, since Constitutional restricts do not apply there.) This right of privacy plays out in many ways in the public sector workplace. One of the most notable ways it has arisen in recent years is with respect to the alleged privacy rights of employees in their workplace computers, e-mail, and electronic communications.

United States v. Simons

One important recent case coming from the Fourth Circuit on these issues is *United States v. Simons*, No. 99-4238, 206 F.3d 392 (4th Cir. 2/28/00). In *Simons*, the Foreign Bureau of Information Services (“FBIS”) (a division of the CIA) employed Mark Simons as an electronic engineer. Simons was provided with a private office and a computer with internet access. The FBIS had a policy regarding internet use by its employees, which provided the internet was to be used solely for official government business, and which specifically prohibited accessing unlawful material. The policy further provided:

“Audits. Electronic auditing shall be implemented within all FBIS unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall . . . be capable of recording:

- Access to the system, including successful and failed login attempts, and logouts;

- *Inbound and outbound file transfers;*
- *Terminal connections (telnet) to and from external systems;*
- *Sent and received e-mail messages;*
- *Web sites visited, including uniform resource locator (URL) of pages retrieved;*
- *Date, Time, and user associated with each event."*

The policy also stated that "*[u]sers shall . . . [u]nderstand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate."*

During testing of FBIS's computer firewall, FBIS discovered that Simons had been visiting websites containing pictures of nude women. FBIS then examined, via remote access, the workplace computer used by Simons, and found pornographic picture files downloaded from the internet. FBIS then copied all of the files on Simons' hard drive, again via remote access. Soon thereafter, FBIS entered Simons' office, removed the original hard drive from Simons' computer, and replaced it with a copy. Further inspection of the files on Simons' hard drive by the FBI revealed that it contained child pornography. An OIG representative and two Assistant United States Attorneys then obtained a warrant to search Simons' office, which soon thereafter was executed. A second search warrant was later obtained and executed, and certain evidence was seized. Ultimately, Simons was indicted for receiving and possessing child pornography. Simons moved to suppress the seized evidence, arguing that the original warrantless searches violated his rights under the Fourth Amendment. The District Court denied the motion, and Simons appealed.

The Fourth Circuit, at the outset, noted that a public sector employee such as Simons, to establish a violation of his or her Fourth Amendment rights, "must first prove that he had a legitimate expectation of privacy in the place searched or the item seized. And, in order to prove a legitimate expectation of privacy, [the employee] must show that his subjective expectation of privacy is one that society is prepared to accept as objectively reasonable." It went on to explain that, "Government employees may have a legitimate expectation of privacy in their offices or in parts of their offices such as their desks or file cabinets. However, office practices, procedures, or regulations may reduce legitimate privacy expectations."

The Fourth Circuit found no violation of Simons' constitutional rights arising from the remote searches of Simons' computer. The court found that, "[i]n light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet." It explained, "Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy. The policy clearly stated that FBIS 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.' This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private. Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use. Accordingly, FBIS' actions in remotely searching and seizing the computer files Simons downloaded from the Internet did not violate the Fourth Amendment." It is notably that the court stated, in a footnote, that "Simons does not assert that he was unaware of, or that he had not consented to, the Internet policy." This

suggests that the court may have reached a different conclusion if either of those facts had been asserted and proven.

The Fourth Circuit next turned FBIS' warrantless removal of Simons' hard drive from his office. Initially, the court noted, "Simons has shown that he had an office that he did not share. As noted above, the operational realities of Simons' workplace may have diminished his legitimate privacy expectations. However, there is no evidence in the record of any workplace practices, procedures, or regulations that had such an effect. We therefore conclude that, on this record, Simons possessed a legitimate expectation of privacy in his office."

The Court rejected the argument that FBIS' Internet policy rendered Simons' expectation of privacy in his office unreasonable. The policy, observed the court, "does not mention employees' offices, and although it does not prohibit FBIS from carrying out its auditing, inspecting, and/or monitoring activities at employees' individual workstations, this fact alone is insufficient to render unreasonable an employee's subjective expectation of privacy in his office. Although the CIA may have had other policies that rendered unreasonable any expectation of privacy in an office occupied by an employee, such as Simons, with access to classified information, no such policies were made a part of this record and consequently we must assume that none existed."

Because Simons had a reasonable expectation of privacy in his office, the court continued, the warrantless search of his office was "per se unreasonable unless it falls within one of the specifically established and well-delineated exceptions to the warrant requirement." However, stated the court, "one exception to the warrant requirement arises when the requirement is rendered impracticable by special needs, beyond the normal need for law enforcement," and "the Supreme Court has held that a government employer's interest in the efficient and proper operation of the workplace may justify warrantless work-related searches." In particular, noted the court, the Supreme Court in *O'Connor v. Ortega*, 480 U.S. 709 (1987), "held that when a government employer conducts a search pursuant to an investigation of work-related misconduct, the Fourth Amendment will be satisfied if the search is reasonable in its inception and its scope. A search normally will be reasonable at its inception when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct. The search will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the[misconduct]."

Therefore, concluded the court, "the question thus becomes whether the search of Simons' office falls within the ambit of the *O'Connor* exception to the warrant requirement, i.e., whether the search was carried out for the purpose of obtaining "evidence of suspected work-related employee misfeasance. The district court found that all of the warrantless searches, and thus the office search, were work-related. The court reasoned that FBIS had an interest in fully investigating Simons' misconduct, even if the misconduct was criminal. We agree. As it does not appear from the record that FBIS utilized the hard drive for internal investigatory purposes before turning it over to the criminal investigator at OIG, we will assume that the dominant purposes of the warrantless search of Simons' office was to acquire evidence of criminal activity, which had been committed at FBIS using FBIS equipment. Nevertheless, the search remains

within the *O'Connor* exception to the warrant requirement; FBIS did not lose its special need for the efficient and proper operation of the workplace merely because the evidence obtained was evidence of a crime. Simons' violation of FBIS' Internet policy happened also to be a violation of criminal law; this does not mean that FBIS lost the capacity and interests of an employer.”

In closing, the Court observed, “We have little trouble concluding that the warrantless entry of Simons' office was reasonable under the Fourth Amendment standard announced in *O'Connor*. At the inception of the search FBIS had reasonable grounds for suspecting that the hard drive would yield evidence of misconduct because FBIS was already aware that Simons had misused his Internet access to download over a thousand pornographic images, some of which involved minors. The search was also permissible in scope. The measure adopted, entering Simons' office, was reasonably related to the objective of the search, retrieval of the hard drive. And, the search was not excessively intrusive. Indeed, there has been no suggestion that Harper searched Simons' desk or any other items in the office; rather, Harper simply crossed the floor of Simons' office, switched hard drives, and exited. In the final analysis, this case involves an employee's supervisor entering the employee's government office and retrieving a piece of government equipment in which the employee had absolutely no expectation of privacy--equipment that the employer knew contained evidence of crimes committed by the employee in the employee's office. This situation may be contrasted with one in which the criminal acts of a government employee were unrelated to his employment. Here, there was a conjunction of the conduct that violated the employer's policy and the conduct that violated the criminal law. We consider that FBIS' intrusion into Simons' office to retrieve the hard drive is one in which a reasonable employer might engage. For the foregoing reasons, we agree with the district court that Simons' Fourth Amendment rights were not violated by any of FBIS' activities in searching his computer and office.”

Lessons for Public Employers

In *United States v. Simons* the employee's right of privacy based on the Fourth Amendment was asserted defensively. However, that right could be asserted offensively by an aggrieved public employee in, for example, a lawsuit under 42 U.S.C. Section 1983, which provides a remedy for deprivation of constitutional rights under color of state law. *Simons* provides valuable guidance for public employers that desire to reduce the risk of such claims. Such employers should consider the following lessons from *Simons*:

1. Employers that allow internet access to employees should adopt a written internet policy. As with all policies, it must be communicated to employees, and the employer should be prepared to prove that each employee received it. Also, as with all policies, it should be consistently enforced.
2. The internet policy should inform employees that the computer system, and all communications sent or received on it, are the property of the employer.
3. The internet policy should inform employees that the computer system, including internet access, is to be used solely for business purposes, and that personal or illegal use of the system is prohibited.

4. The internet policy should provide specific illustrations of inappropriate usage. For example, it should expressly state that the computer system is not to be used to download or display pornographic material, and that employees are prohibited from harassing other employees via e-mail.
5. The internet policy should clearly inform employees that the employer may engage in electronic auditing, including monitoring of internet activity. The language used in the policy at issue in *Simons* provides a good starting point.
6. The internet policy should inform employees that warrantless searches may be conducted in accordance with the principles stated in *O'Connor*.
7. The internet policy should be coordinated with the employer's e-mail policy. In many situations, the best approach is to adopt a comprehensive policy governing the use of workplace computers and networks, including e-mail and the internet.