Third District Court of Appeal

State of Florida

Opinion filed June 26, 2019.
Not final until disposition of timely filed motion for rehearing.

No. 3D17-734
Lower Tribunal No. 15-19792

Saintamen Edwards,
Appellant,

vs.

The State of Florida,
Appellee.

An Appeal from the Circuit Court for Miami-Dade County, Martin Zilber, Judge.

Marcia J. Silvers, P.A., and Marcia J. Silvers, for appellant.

Ashley Moody, Attorney General, and Michael W. Mervine, Assistant Attorney General, for appellee.

Before EMAS, C.J., and SCALES and HENDON, JJ.

EMAS, C.J.

INTRODUCTION

Saintamen Edwards, a former Miami-Dade County police officer, appeals her conviction and sentence for two counts of official misconduct. Her primary contention on appeal is that the trial court erred in denying her motion to suppress evidence obtained from a personal flash drive plugged into her work computer. Following our review of the record, and the issues raised on appeal, we affirm.

FACTS AND PROCEDURAL BACKGROUND

In 2013, Edwards was arrested and charged with two counts of official misconduct after an investigation revealed she had falsified police records in an apparent attempt to get her husband, Clyde Edwards (Clyde), fired from his job at a sports apparel and footwear store. Clyde's boss, Jose Raij, contacted police after he received a phone call from someone identifying herself as Miami-Dade police detective Diann Mich. The caller told Raij that Clyde should be fired because he was being investigated by police, and that there were police reports regarding the investigation. Raij asked to see a copy of the police reports and, at 4:09 p.m. on July 8, 2013, Raij received the following email:

> Mr. Raij, attached are two reports I am able to release to you at this time. As we discussed, please do not discuss the open case with the suspect. I will forward you the complete file in a couple of days. Thank you, Diann

Two police reports were attached to the email, indicating that Clyde was being investigated for selling counterfeit sports shoes. However, further investigation by

Raij and Miami-Dade Police revealed that the two police reports had been falsified, and were emailed to Raij from a copy machine located on the second floor of the Miami-Dade County Police Department Intracoastal District Station, where Edwards worked. The evidence against Edwards included the testimony of three fellow police officers, who testified that they saw Edwards near that copy machine on the second floor of the police department on July 8 around 4 p.m., and the contents of a USB flash drive (the "flash drive") that was seized from Edwards' work computer prior to her arrest.[1]

Edwards' defense was that she could not have created and sent the falsified police reports because she was not at the police department at the time the reports were emailed to Raij, having left work early that day not feeling well. She claimed that she had an office visit with her therapist from 2 to 3 p.m., and thereafter, had lunch and picked up her daughter from daycare at 4:20 p.m.[2]

---

[1] Police determined that the falsified records were placed on the flash drive on July 8, 2013 between 3:47 p.m. and 4:01 p.m.

[2] Edwards contends that the trial court erred in refusing to admit certain evidence which Edwards asserts would show she was not at the police department at the relevant time period and therefore could not have emailed the falsified police reports. We review the trial court's decision to admit or exclude evidence for an abuse of discretion. Penalver v. State, 926 So. 2d 1118, 1133 (Fla. 2006) (holding: "It is within the sound discretion of the trial judge to determine the admissibility of evidence, and the trial judge's ruling on such an issue will not be disturbed on appeal absent a showing of an abuse of discretion"); Linde v. Linde, 199 So. 3d 1102 (Fla. 3d DCA 2016). After reviewing the record, including the trial transcript, we find no abuse of discretion by the trial court in these evidentiary rulings.

Prior to trial, Edwards moved to suppress the evidence obtained from the flash drive attached to her work computer at the time it was seized, asserting that the flash drive was her personal property, and was thus illegally seized at the time her work computer was legally seized. After an evidentiary hearing, the court denied Edwards' motion to suppress the evidence obtained from the flash drive, determining she had no reasonable expectation of privacy in the flash drive and its contents.

Following trial, a jury convicted Edwards of both counts of official misconduct, and she was thereafter sentenced to probation.

STANDARD OF REVIEW

When reviewing a trial court's ruling on a motion to suppress, the appellate court "affords a presumption of correctness to a trial court's findings of fact but reviews de novo the mixed questions of law and fact that arise in the application of the historical facts to the protections of the Fourth Amendment." Wyche v. State, 987 So. 2d 23, 25 (Fla. 2008). Generally, a person's Fourth Amendment rights are implicated only if the search or seizure infringes on "an expectation of privacy that society is prepared to consider reasonable." O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (quoting U.S. v. Jacobsen, 466 U.S. 109, 104 (1984)). Importantly, "[g]iven the great variety of work environments in the public sector, the question whether any employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." Id. at 718.

In analyzing the legitimacy of one's expectation of privacy in an office setting, a court must consider the following legal principles:

> To invoke the protection of the Fourth Amendment, a criminal defendant must establish standing by demonstrating a legitimate expectation of privacy in the area searched or the item seized. A legitimate expectation of privacy consists of both a subjective expectation and an objectively reasonable expectation, as determined by societal standards. The reasonableness of an expectation of privacy in a particular place or item depends on context. Specifically, the reasonableness of an employee's expectation of privacy in his or her office or the items contained therein depends on the "operational realities" of the workplace, and not on legal possession or ownership. The likelihood that a person has an objectively reasonable expectation of privacy in an office setting is increased where the area or item searched is "reserved for [the defendant's] exclusive personal use." Other factors that have been considered in determining the legitimacy of an expectation of privacy in an item seized from an office include the employee's relationship to the item, whether the item was in the employee's immediate control when it was seized, and whether the employee took actions to maintain a sense of privacy in the item. Many times, an employee may have a legitimate expectation of privacy in his or her personal office and in personal items stored in a desk or file cabinet.

Kelly v. State, 77 So. 3d 818, 822-23 (Fla. 4th DCA 2012) (quoting State v. Young, 974 So. 2d 601, 608 (Fla. 1st DCA 2008) (internal citations omitted)). It is the defendant's burden to establish she had a subjective expectation of privacy and that such an expectation was objectively reasonable. Hicks v. State, 929 So. 2d 13 (Fla. 2d DCA 2006).

THE MOTION TO SUPPRESS HEARING

The relevant testimony adduced at the evidentiary hearing on the motion to suppress can be summarized as follows:

Edwards' work computer was located on her desk in the station control office at the police station, an office which is known as "the armory" because it contains various items needed by the officers (such as extra weapons). The armory is kept locked at all times, but several administrative officers had keys to the office, and one master key is hidden somewhere in the department in case officers get locked out. At all relevant times, Edwards and her co-worker, Officer Michnowicz, both had desks and computers in the armory. The password for Edwards' work computer was written down on the calendar blotter, in open view on Edwards' desk, so that Michnowicz could access Edwards' computer at any time.

The computers owned by the Miami-Dade Police Department, including Edwards' work computer, are all connected to a network, and anyone with county credentials can access the County's "O Drive" from any County computer, using their own login credentials. When an employee logs in to a County computer, a login banner appears, setting forth a warning and terms and conditions of use. The employee is required to acknowledge this warning and consent to the terms of use before inputting their individual password for access. The login banner reads:

> This computer system is the property of the Miami-Dade Police Department. It is for authorized use only. **Users have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded,**

> **copied, audited, inspected, and disclosed to authorized personnel. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection and disclosure.** Unauthorized or improper use of this system may result in administrative disciplinary action or civil/criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions.

(Emphasis added.)

When internal affairs officers seized Edwards' computer in July 2013, Edwards' flash drive was plugged into a USB port in her work computer.[3] Accordingly, and following police department protocol that anything attached to the work computer, including external media, is part of the "computer system," the officers seized the flash drive as well.

Officer Tompkins, with the police department's digital forensic unit, testified that if he had logged onto Edwards' computer with his own password, he could have accessed the contents of Edwards' flash drive. Edwards was not present at the time her work computer and flash drive were seized; at the request of internal affairs, her superior had sent Edwards out on an errand so that the computer could be seized without interference.

The flash drive was later returned to the police department—specifically to Officer King, who had assumed Edwards' duties and position as Station Control

[3] Edwards testified that she purchased the flash drive at Kmart and that it was her personal property. There is no evidence to the contrary.

Officer. Officer King accessed the contents of the flash drive because Edwards told King it contained documents which King would need to perform her job as Station Control Officer.[4] King testified that she did in fact find work-related documents on the flash drive, which she utilized, and that Edwards never asked King to return the flash drive to her. Edwards testified that she kept recipes and pictures of her daughter on the flash drive, but she acknowledged there were work-related documents on the flash drive as well, documents which she needed to perform her duties.

DISCUSSION AND ANALYSIS

In Kelly, 77 So. 3d at 823, the appellate court held that the defendant had no expectation of privacy in the contents of his desk where he: (1) shared the office with another employee and other employees had full access to the office; and (2) there were no locks on the desk and others occasionally looked through the desk without the defendant's permission. Similarly, in the present case, Edwards shared an office with a co-worker who had access to Edwards' work computer at all times because Edwards left a sticky note with her computer password on her desk for that express purpose.

In this context, the U.S. Supreme Court has said:

[4] Edwards denied that she had such conversation with Officer King, but both King and her supervisor, Sergeant Gilligan, testified otherwise, and the trial court was free to determine which competing version of the evidence to accept.

> The workplace includes those areas and items that are related to work and are generally within the employer's control . . . . These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board. Not everything that passes through the confines of the business address can be considered part of the workplace context, however. An employee may bring closed luggage to the office prior to leaving on a trip, or a handbag or briefcase each workday. While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the *contents* of the luggage is not affected in the same way. The appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address. Within the workplace context, this Court has recognized that employees may have a reasonable expectation of privacy against intrusions by police.

Ortega, 480 U.S. at 715-16. A "public employee's expectation of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." Id. at 717.

In assessing the reasonableness of a search or seizure involving a work computer, relevant factors "include whether the office has a policy regarding the employer's ability to inspect the computer, whether the computer is networked to other computers, and whether the employer (or a department within the agency) regularly monitors computer use." Young, 974 So. 2d at 609. See also U.S. v. Angevine, 281 F.3d 1130 (10th Cir. 2002) (holding, where professor made "a careless effort to maintain a privacy interest" in his office computer, he had no

reasonable expectation of privacy.") And "where an employer has a clear policy allowing others to monitor a workplace computer, an employee who uses the computer has no reasonable expectation of privacy in it." Young, 974 So. 2d at 609.

In the instant case, Edwards' work computer contained a login banner, warning users about the police department's computer policy and requiring their acknowledgment before logging in. However, the issue here is not whether Edwards had a reasonable expectation of privacy in her work computer, but whether she had an expectation of privacy in her flash drive, which at the time of its seizure was plugged into her work computer. We hold, under the facts of this case, that the trial court correctly concluded Edwards did not have a reasonable expectation of privacy.

In an analogous situation, the Eleventh Circuit Court of Appeals in U.S. v. Durdley, No. 10-13756, 2011 WL 3476812 (11th Cir. Aug. 9, 2011)[5] considered whether a county-employed paramedic had a reasonable expectation of privacy in a thumb drive he had inadvertently left plugged into a computer at work. The

[5] The Florida Constitution contains a provision protecting against unreasonable searches and seizures. See Art. I, § 12, Fla. Const. (providing in part: "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures . . . shall not be violated.") However, that same section contains a conformity clause: "This right shall be construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court." In the absence of controlling precedent from the United States Supreme Court, our appellate courts may look to other state and federal court decisions for guidance. See D.P. v. State, 65 So. 3d 123, 129 n.6 (Fla. 3d DCA 2011); Higerd v. State, 54 So. 3d 513 (Fla. 1st DCA 2010).

computer itself was located at a medic station, in a common area available to all the county medic employees. Durdley had left his personal thumb drive plugged into the computer when his shift was over, and it was discovered by a co-worker who accessed the files on the thumb drive and discovered child pornography. The police were contacted, and seized the thumb drive without a warrant. Durdley later admitted that it was his thumb drive and that he commonly used it for storing work-related information. The Eleventh Circuit held that "Durdley did not have a reasonable expectation of privacy in the thumb drive he left in a county-owned, common-use computer."

Similarly, U.S. v. King, 509 F.3d 1338 (11th Cir. 2007), considered whether King, a civilian contractor stationed at an American air base in Saudi Arabia, had a reasonable expectation of privacy in his personal laptop computer which he had left in his dormitory room connected to the base network. As a user of the base network, King understood his activities were subject to monitoring, but he believed he had secured his computer so others could not access its contents. However, when an airman came across the contents of King's hard drive on the base network, he discovered pornographic material, which later led to an investigation and King's arrest for possession of child pornography. The Eleventh Circuit held that King did not have a legitimate expectation of privacy in the contents of his personal laptop

computer when it was connected to the base network from his dorm room because everyone on the network had access to his files.

In Miller v. State, 335 S.W.3d 847 (Tex. App. 2011), a police officer moved to suppress evidence seized from his personal thumb drive, which he left in a computer located in the patrol room accessible to other police department employees. The trial court denied the motion to suppress, and the appellate court affirmed, holding that Miller "did not exhibit an actual subjective expectation of privacy in the thumb drive" because he left it in the patrol room, it had no external identifying marks, and he did "nothing to prevent others from accessing the thumb drive, such as protecting it with a password, encrypting the data, or even placing the drive in a locked case." Id. at 855. Further, the court held, even if Miller had a subjective expectation of privacy in the thumb drive, such an expectation was not objectively reasonable under the circumstances. Id. The court listed several factors to consider in reaching this conclusion: (1) whether the accused had a property or possessory interest in the place invaded; (2) whether he was legitimately in the place invaded; (3) whether he had complete dominion or control and the right to exclude others; (4) whether, before the intrusion, he took normal precautions customarily taken by those seeking privacy; (5) whether he put the place to some private use; and (6) whether his claim of privacy is consistent with historical notions of privacy.

Assessing these factors, the Miller court held that the defendant's expectation of privacy was not objectively reasonable because, inter alia, he "did not take precautions to maintain his expectation of privacy;" "did not protect his drive with a password or secure the drive in a locked case;" and "he used the thumb drive for storing police activity reports, which the district court could have reasonably inferred was not a private use." Id. at 856.

Similarly, in Kane v. State, 458 S.W.3d 180 (Tex. App. 2015), a university student left his flash drive in a public computer at the university, where it was later discovered by a university employee, who found child pornography on the drive, and called police. Relying upon its sister court's earlier decision in Miller, the Kane court held that the student had no subjective expectation of privacy because he left the drive in a classroom available to other students, faculty and staff, with no identifying marks and without it being password protected or locked. Id. at 184-85. Further, the Kane court held, even assuming a subjective expectation of privacy, such an expectation was not objectively reasonable under the circumstances. Id. at 185.

Finally, in U.S. v. Barrows, 481 F.3d 1246 (10th Cir. 2007), a city treasurer shared desk space with the city clerk in an area where "city employees regularly entered their space to use the city's fax machine and photocopier." Because the city provided the treasurer and the clerk with only one computer, the treasurer, Barrows,

brought his personal computer to work, which he kept on the common desk and connected via the city network to the office computer. Barrows conducted all of his city work on his personal computer, and he did not install a password or attempt to exclude anyone from using it, rather leaving it running at all times on his shared desk at the office. When a city employee attempted to troubleshoot a problem with the office computer, he went on Barrows' personal computer, while Barrows was absent, and discovered child pornography. When this was reported to the sheriff, Barrows' computer was seized. The trial court denied Barrows' motion to suppress the files found on his computer.

The appellate court affirmed, finding that Barrows had no reasonable expectation of privacy in the personal computer. Although the court recognized that "private ownership is an important factor telling in favor of Fourth Amendment protection, . . . the significance of personal ownership is particularly weakened when the item in question is being used for business purposes." Id. at 1248. Furthermore, the court held that even more important "is Mr. Barrows's failure to password protect his computer, turn it off, or taken any other steps to prevent third-party use. . . . Given these facts, we are hard-pressed to conclude that Mr. Barrows harbored a subjective expectation of privacy. He certainly did not possess a reasonable one." Id. at 1248-49. Finally, the court pronounced: "Those who bring personal material into public spaces, making no effort to shield that material from public view, cannot reasonably

expect their personal materials to remain private." Id. at 1249. See also, Katz v. U.S., 389 U.S 347, 351 (1967) (noting: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.") Compare Young, 974 So. 2d at 611 (in which the defendant, a pastor, kept his computer, which was only used by him, in his private office, which was locked at all times, and only himself and the church administrator had keys).

CONCLUSION

In this case, the evidence established that Edwards' flash drive was plugged into a work computer owned by her employer, the Miami-Dade Police Department. The computer was kept in an office Edwards shared with another police officer who had full access to Edwards' computer, because Edwards left the password in plain view on her desk for the express purpose of allowing her co-worker to use the computer. The computer was connected to a network which anyone with county credentials could access.

A login banner warned the employee that the computer system is the property of the Miami-Dade Police Department; that users of the computer system have no expectation of privacy; and that all uses of the system, and all files on the system, may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized personnel.

The item for which Edwards claims an expectation of privacy—the flash drive—was normally kept in Edwards' possession, but at the time it was seized, she had left it plugged into the work computer. We hold that the trial court properly denied the motion to suppress, as Edwards had no reasonable expectation of privacy in the flash drive and its contents.

Affirmed.

HENDON, J., concurs.

SCALES, J. concurring.

I concur in Chief Judge Emas's excellent opinion, but write separately to emphasize how Fourth Amendment jurisprudence may sometimes upset common sense. The Chief's opinion skillfully, methodically, and with unassailable precedential support, concludes that this public sector worker has no reasonable expectation of privacy in the contents of a personally owned flash drive when the flash drive is confiscated while plugged into her work computer. This holding, while correct, may come as quite a surprise to anyone who has ever used a personally owned flash drive at work with non-nefarious intentions.