IN THE DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA
FIFTH DISTRICT JANUARY TERM 2005

BEVERLY ANN O'BRIEN,

Appellant,

v. Case No. 5D03-3484

JAMES KEVIN O'BRIEN,

Appellee.

_____/

Opinion filed February 11, 2005

Appeal from the Circuit Court
for Orange County,
Donald E. Grincewicz, Judge.

Ryan Thomas Truskoski of Ryan Thomas Truskoski, P.A., Orlando, for Appellant.

David F. Allen, Winter Park, for Appellee.

SAWAYA, C.J.

Emanating from a rather contentious divorce proceeding is an issue we must resolve regarding application of certain provisions of the Security of Communications Act (the Act) found in Chapter 934, Florida Statutes (2003). Specifically, we must determine whether the trial court properly concluded that pursuant to section 934.03(1), Florida Statutes (2003), certain communications were inadmissible because they were illegally intercepted by the Wife who, unbeknownst to the Husband, had installed a

spyware program on a computer used by the Husband that copied and stored electronic communications between the Husband and another woman.

When marital discord erupted between the Husband and the Wife, the Wife secretly installed a spyware program called Spector on the Husband's computer. It is undisputed that the Husband engaged in private on-line chats with another woman while playing Yahoo Dominoes on his computer. The Spector spyware secretly took snapshots of what appeared on the computer screen, and the frequency of these snapshots allowed Spector to capture and record all chat conversations, instant messages, e-mails sent and received, and the websites visited by the user of the computer. When the Husband discovered the Wife's clandestine attempt to monitor and record his conversations with his Dominoes partner, the Husband uninstalled the Spector software and filed a Motion for Temporary Injunction, which was subsequently granted, to prevent the Wife from disclosing the communications. Thereafter, the Husband requested and received a permanent injunction to prevent the Wife's disclosure of the communications and to prevent her from engaging in this activity in the future. The latter motion also requested that the trial court preclude introduction of the communications into evidence in the divorce proceeding. This request was also granted. The trial court, without considering the communications, entered a final judgment of dissolution of marriage. The Wife moved for rehearing, which was subsequently denied.

The Wife appeals the order granting the permanent injunction, the final judgment, and the order denying the Wife's motion for rehearing on the narrow issue of whether the trial court erred in refusing to admit evidence of the Husband's computer activities

obtained through the spyware the Wife secretly installed on the computer. The Wife argues that the electronic communications do not fall under the umbra of the Act because these communications were retrieved from storage and, therefore, are not "intercepted communications" as defined by the Act. In opposition, the Husband contends that the Spector spyware installed on the computer acquired his electronic communications real-time as they were in transmission and, therefore, are intercepts illegally obtained under the Act.

The trial court found that the electronic communications were illegally obtained in violation of section 934.03(1)(a)-(e), and so we begin our analysis with the pertinent provisions of that statute, which subjects any person to criminal penalties who engages in the following activities:

> (a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication;
>
> (b) Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:
>
> > 1. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
> >
> > 2. Such device transmits communications by radio or interferes with the transmission of such communication;
>
> (c) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

> (d) Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
>
> (e) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication intercepted by means authorized by subparagraph (2)(a)2., paragraph (2)(b), paragraph (2)(c), s. 934.07, or s. 934.09 when that person knows or has reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, has obtained or received the information in connection with a criminal investigation, and intends to improperly obstruct, impede, or interfere with a duly authorized criminal investigation;
>
> shall be punished as provided in subsection (4).

§ 934.03(1)(a)-(e), Fla. Stat. (2003). Enactment of these prohibitions connotes "a policy decision by the Florida legislature to allow each party to a conversation to have an expectation of privacy from interception by another party to the conversation." Shevin v. Sunbeam Television Corp., 351 So. 2d 723, 726-27 (Fla. 1977). The purpose of the Act is to protect every person's right to privacy and to prevent the pernicious effect on all citizens who would otherwise feel insecure from intrusion into their private conversations and communications. Id.

The clear intent of the Legislature in enacting section 934.03 was to make it illegal for a person to intercept wire, oral, or electronic communications. It is beyond doubt that what the trial court excluded from evidence are "electronic communications."[1]

[1]The term "electronic communications" is defined in section 934.02(12), Florida Statutes (2003), as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

The core of the issue lies in whether the electronic communications were intercepted. The term "intercept" is defined by the Act as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." § 934.02(3), Fla. Stat. (2003). We discern that there is a rather fine distinction between what is transmitted as an electronic communication subject to interception and the storage of what has been previously communicated. It is here that we tread upon new ground. Because we have found no precedent rendered by the Florida courts that considers this distinction, and in light of the fact that the Act was modeled after the Federal Wiretap Act,[2] we advert to decisions by the federal courts that have addressed this issue for guidance.[3]

The federal courts have consistently held that electronic communications, in order to be intercepted, must be acquired contemporaneously with transmission and that electronic communications are not intercepted within the meaning of the Federal Wiretap Act if they are retrieved from storage. See Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003); Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir.), cert. denied, 125 S. Ct. 48 (2004); United States v. Steiger, 318 F.3d 1039 (11th Cir.), cert.

---

electromagnetic, photoelectronic, or photooptical system that affects intrastate, inter-state, or foreign commerce . . . ."

[2]What we label the Federal Wiretap Act is found in 18 U.S.C. § 2501, et seq., as amended by Title I of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, Title I, 100 Stat. 1848 (1986).

[3]See Jackson v. State, 636 So. 2d 1372, 1374 (Fla. 2d DCA 1994) (stating, in reference to the Act, that "[w]e also examine its interpretation by the federal courts under Florida's established rule of statutory construction 'which recognizes that if a state law is patterned after a federal law on the same subject, the Florida law will be accorded the same construction as in the federal courts to the extent the construction is harmonious with the spirit of the Florida legislation.'") (quoting O'Loughlin v. Pinchback, 579 So. 2d 788, 791 (Fla. 1st DCA 1991)), approved, 650 So. 2d 24 (Fla. 1995).

denied, 538 U.S. 1051 (2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003). These courts arrived at this conclusion based on the federal law definitions of (1) the term "intercept," which is very similar to the definition in the Florida Act, (2) the term "wire communication," which provides for electronic storage, and (3) the term "electronic communication," which does not provide for electronic storage. The fact that the definition of "wire communication" provides for electronic storage while the definition of "electronic communication" does not, suggests to the federal courts that Congress intended "intercept" to include retrieval from storage of wire communications, but exclude retrieval from storage of electronic communications. The definition of "wire communication" in the Florida Act, unlike the Federal Wiretap Act, does not include a provision for retrieval from storage and, therefore, it is not clear whether the same rationale would be applied by the federal courts to provisions identical to the Florida Act. However, we need not decide whether electronic communications may never be intercepted from storage under the Florida Act because the particular facts and circumstances of the instant case reveal that the electronic communications were intercepted contemporaneously with transmission.

The Spector spyware program that the Wife surreptitiously installed on the computer used by the Husband intercepted and copied the electronic communications as they were transmitted. We believe that particular method constitutes interception within the meaning of the Florida Act, and the decision in Steiger supports this conclusion. In Steiger, an individual was able to hack into the defendant's computer via a Trojan horse virus that allowed the hacker access to pornographic materials stored on the hard drive. The hacker was successful in transferring the pornographic material

from that computer to the hacker's computer. The court held that because the Trojan horse virus simply copied information that had previously been stored on the computer's hard drive, the capture of the electronic communication was not an interception within the meaning of the Federal Wiretap Act. The court did indicate, however, that interception could occur if the virus or software intercepted the communication as it was being transmitted and copied it. The court stated:

> [T]here is only a narrow window during which an E-mail interception may occur—the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

Steiger, 318 F.3d at 1050 (quoting Jarrod J. White, E-Mail@Work.com: Employer Monitoring of Employee E-Mail, 48 Ala. L. Rev. 1079, 1083 (1997)). Hence, a valid distinction exists between a spyware program similar to that in Steiger, which simply breaks into a computer and retrieves information already stored on the hard drive, and a spyware program similar to the one installed by the Wife in the instant case, which copies the communication as it is transmitted and routes the copy to a storage file in the computer.

The Wife argues that the communications were in fact stored before acquisition because once the text image became visible on the screen, the communication was no longer in transit and, therefore, not subject to intercept. We disagree. We do not believe that this evanescent time period is sufficient to transform acquisition of the communications from a contemporaneous interception to retrieval from electronic

storage. We conclude that because the spyware installed by the Wife intercepted the electronic communication contemporaneously with transmission, copied it, and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act.

We must next determine whether the improperly intercepted electronic communications may be excluded from evidence under the Act. The exclusionary provisions of the Act are found in section 934.06, Florida Statutes (2003), which provides that "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence . . . ." Conspicuously absent from the provisions of this statute is any reference to electronic communications. The federal courts, which interpreted an identical statute contained in the Federal Wiretap Act, have held that because provision is not made for exclusion of intercepted electronic communications, Congress intended that such communications not be excluded under the Federal Wiretap Act. See Steiger. We agree with this reasoning and conclude that the intercepted electronic communications in the instant case are not excludable under the Act. But this does not end the inquiry.

Although not specifically excludable under the Act, it is illegal and punishable as a crime under the Act to intercept electronic communications. § 934.03, Fla. Stat. (2003). The trial court found that the electronic communications were illegally intercepted in violation of the Act and ordered that they not be admitted in evidence. Generally, the admission of evidence is a matter within the sound discretion of the trial court. See Stewart & Stevenson Servs., Inc. v. Westchester Fire Ins. Co., 804 So. 2d

584, 587 (Fla. 5th DCA 2002); Forester v. Norman Roger Jewell & Brooks Int'l, Inc., 610 So. 2d 1369, 1372 (Fla. 1st DCA 1992) ("[T]he admission of evidence is within the sound judicial discretion of the trial judge, whose decision in such regard must be viewed in the context of the entire trial.") (citation omitted); see also Globe v. State, 877 So. 2d 663, 672 (Fla. 2004) ("'A trial judge's ruling on the admissibility of evidence will not be disturbed absent an abuse of discretion.'") (quoting Blanco v. State, 452 So. 2d 520 (Fla. 1984), cert. denied, 469 U.S. 1181 (1985)); Shearon v. Sullivan, 821 So. 2d 1222, 1225 (Fla. 1st DCA 2002) ("The standard of review of a trial court's exclusion of evidence is abuse of discretion") (citation omitted). Because the evidence was illegally obtained, we conclude that the trial court did not abuse its discretion in refusing to admit it. See Daniels v. State, 381 So. 2d 707 (Fla. 1st DCA 1979), aff'd, 389 So. 2d 631 (1980); Horn v. State, 298 So. 2d 194 (Fla. 1st DCA 1974), cert. denied, 308 So. 2d 117 (Fla. 1975).

We affirm the orders and the final judgment under review in the instant case.

AFFIRMED.

SHARP, W. and MONACO, JJ., concur.