[Cite as *State v. Poling,* 160 Ohio Misc.2d 84, 2010-Ohio-5429.]

IN THE HOCKING COUNTY MUNICIPAL COURT
LOGAN, OHIO

The State of Ohio	:	CASE NO: CRB0900555
	:	
v.	:	
Poling.	:	ENTRY
	:	June 25, 2010

Laina Fetherolf, Hocking County Prosecuting Attorney, and Jonah Saving, Assistant Prosecuting Attorney, for plaintiff.

James Kingsley, for defendant.

JOHN T. WALLACE, Judge.

{¶ 1} Defendant, Jacob W. J. Poling, challenges the use of evidence that the state of Ohio plans to introduce against him. More specifically, the defendant asks this court to suppress e-mails that were obtained by the mother of his underage girlfriend and were provided to the Hocking County Sheriff's Office.

{¶ 2} Defendant filed his motion to suppress on August 17, 2009. On November 16, 2009, the court held an oral hearing on the motion and asked for supplemental memoranda. On December 3, 2009, defendant filed a supplemental memorandum and a trial brief. On December

7, 2009, the state filed a memorandum contra. After consideration of the arguments, evidence and memoranda, the motion comes on for decision.

Facts

{¶ 3} The defendant is charged with a count of violating a protection order. These charges arose from defendant's alleged violation of a civil protection order that was obtained in the Common Pleas Court of Hocking County by Jana Kaiser. The order prohibited the defendant from having contact with Jana or any member of her family, including her 16-year-old daughter, Stephanie.

{¶ 4} On May 22, 2009, Stephanie was on the computer in the Kaiser home. The computer was centrally located in the family's living room. The computer was used by the whole family. Jana paid the bill for the home's computer service. Jana also made it a habit to police Stephanie's Internet use, and Stephanie knew it. On the evening in question, Jana saw that Stephanie was on MySpace. Two of Stephanie's young cousins were visiting the Kaiser home that evening.

{¶ 5} Jana asked Stephanie to walk the children down the block to their home. Stephanie left to escort the two young children home. When she left, she did not log off the computer or shut anything down. While Stephanie was gone, Jana checked on her daughter's activities on the Internet. Jana copied several recent messages that had come to Stephanie's MySpace account. She then placed the copies into a file that Jana maintained on the computer. Later, Jana reviewed the items that she had copied. The items were messages between Stephanie and the defendant. Jana then went to the Hocking County Sheriff's Office to make a report. Deputy Trent Woodgeard took a report and filed a charge against Poling.

{¶ 6} The issue in this case is whether the actions of Jana violated either Ohio or federal law and whether the e-mails are admissible against the defendant at trial. Defendant maintains that under R.C. 2933.62, the e-mails should be suppressed.

Legal Analysis

{¶ 7} Our starting point is federal law. Ohio's statute as to the illegal interception of oral, wire, or electric communications found in R.C. 2933.51 very closely tracks the Federal Wire Tap Act, Title I of the Electronic Communications Privacy Act ("ECPA"), Section 2510 et seq., Title 18, U.S.Code.

{¶ 8} However, it appears that the Federal Stored Communications Act ("SCA"), Title II of the Electronic Communications Privacy Act, Section 2701, Title 18, U.S.Code rather than Title I of the ECPA, Sections 2510 et seq., applies to the conduct at issue here. This is important because unlike the Wiretap Act (see Section 2515, Title 18, U.S.Code, prohibition of use as evidence), the SCA does not provide for the exclusion from evidence of material that has been unlawfully accessed. The SCA provides for civil damages and criminal punishment for its violation, see Sections 2701 and 2707, Title 18, U.S.Code, but unlike the Wiretap Act, it does not provide for the exclusion of evidence obtained illegally under the Act. See Section 2708, Title 18, U.S.Code (remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter); *United States v. Ferguson* (D.D.C.2007), 508 F. Supp.2d 7 (SCA does not provide for suppression of evidence as a remedy); Thus, even if Jana's conduct had violated the SCA, the evidence in question is not subject to exclusion under the statute. Moreover, it is possible that Jana's conduct could be deemed to be authorized under the SCA and thus lawful. Even if the conduct is not expressly

authorized, it may be deemed nevertheless to be lawful under the concept of implied consent or authorization based on Jana's parental authority.

{¶ 9} The Wiretap Act provides:

> (1) Except as otherwise specifically provided in this chapter any person who:
>
> (a) *intentionally intercepts*, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, *any wire, oral, or electronic 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 * * * in violation of this subsection.

(Emphasis added.) Section 2511, Title 18, U.S.Code. The statute defines "intercept" 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." Section 2510(4), Title 18, U.S.Code. An "electronic communication" is defined as "any *transfer* of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system *that effects interstate or foreign commerce*." (Emphasis added.) Section 2510(12), Title 18, U.S.Code.

{¶ 10} By contrast, the SCA, as its name suggests, prohibits the unauthorized access of stored electronic communications:

> Except as provided in subsection (c) of this section whoever:
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;

> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

Section 2701(a), Title 18, U.S.Code. As explained in *Bunnell v. Motion Picture Assn. of Am.* (C.D.Cal.2007), 567 F. Supp.2d 1148, 1152, for purposes of the ECPA, "at any given time, an electronic communication may either be intercepted and actionable under the Wiretap Act, or acquired while in electronic storage and actionable under SCA. An electronic communication may not simultaneously be actionable under both the Wiretap Act and the SCA." (Citation omitted.) Bunnell at 1152; see *United States v. Szymuszkiewicz* (June 30, 2009), E.D.Wis. No. 07-CA-171, 2009 WL 1873657, *9 (describing the process by which e-mails are sent and received and the history of the Wiretap Act and the SCA and their different applications). The majority of federal courts have concluded that because the Wiretap Act prohibits only the interception of transmissions and because the unauthorized access to e-mails is not accomplished through the interception of transmissions, the SCA rather than the Wiretap Act applies to such unauthorized access.

{¶ 11} *Cardinal Health 414, Inc. v. Adams* (M.D.Tenn.2008), 582 F. Supp.2d 967, reached this same conclusion, but in a different factual context from the one presented here. The plaintiff in that case was a company that had filed suit against a former employee who had continued to log on to the company e-mail system without authorization by using the usernames and passwords of current employees, and who had read the e-mails received by those employees. The former employee had used information from those e-mails to pass along information to a competitor of his former company. The plaintiff argued that the former employee had violated the Federal and Tennessee wiretap statutes and the SCA. The court held that the former employee had clearly violated the SCA by accessing the e-mail accounts of current employers,

but concluded that none of the former employee's actions had violated the state or federal wiretap acts. Noting that the crucial issue was whether any transmission had been intercepted, the court found that "[t]he overwhelming body of case law, including from one district court in this circuit earlier this year, finds that, unless an e-mail is actually acquired in split second transmission over a computer network, it cannot be 'intercepted' as that term is reasonably understood." Id. at 979. More specifically, the court stated:

> The Third, Fifth, Ninth, and Eleventh Circuits all agree that, for a communication to be "intercepted" under the FWA, that communication must be acquired during the "flight" of the communication. *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3rd Cir.2003); *U.S. v. Steiger*, 318 F.3d 1039, 1047 (11th Cir.2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir.2002); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 463 (5th Cir.1994). In support of this view, there is, of course, the ordinary dictionary definition of "intercept," which is "to stop, seize, or interrupt in progress or course before arrival." *Konop*, 302 F.3d at 878 (citing *Webster's Ninth New Collegiate Dictionary* 630 (1985)). Also, there is the statutory history, which shows that Congress created the SCA for the express purpose of addressing "access to stored * * * electronic communications and transactional records." Id. at 879 (citing S. Rep. 99-541 at 3) (emphasis added). Also, until October 2001, the definition of "wire communication" in the FWA included information in electronic storage, such as a voicemail, but the definition of "electronic communication" in the FWA did not include information in electronic storage, indicating that something like an e-mail would not be covered by the FWA. Id.; *Fraser*, 352 F.3d at 114. Further, after 9/11, Congress amended the FWA to eliminate communications in electronic storage from the definition of "wire communication," further indicating a congressional intent that the FWA should be primarily concerned with information in active transport, not stored information. Id.

Id. at 979-980.

{¶ 12} The *Cardinal Health 414* also referred to *Bailey v. Bailey* (Feb. 6, 2008), E.D.Mich. No. 07-116-72, 2008 WL 324156, which had rejected a Wiretap Act claim brought by an ex-wife against her ex-husband. Before the divorce, the ex-husband had obtained a keystroke logger on a computer that he shared with his wife, and he had used it to track and read her e-mails and private messages. *Bailey* noted that the Sixth Circuit had yet to rule on a similar issue,

but that the courts of appeals that have addressed the issue have agreed that the definition of "intercept" encompasses only acquisitions contemporaneous with transmission, citing the same cases cited in *Cardinal Health 414*. The court thus granted summary judgment to the ex-husband on the Wiretap Act claim. However, the court declined to grant summary judgment to the ex-husband on the SCA claim, noting that "the plain language of the statute seems to include e-mails received by the intended recipient where they remain stored by an electronic communication service." Id., 2008 WL 324156, at *7. The court added as a "point of clarification" that the SCA protection does not extend to e-mails and messages stored only on plaintiff's personal computer. Id. citing *In re DoubleClick, Inc. Privacy Litigation* (S.D.N.Y.2001), 154 F.Supp.2d 497, 511. ("[T]he cookies' residence on plaintiffs' computers does not fall into 2510(17)(B) because plaintiffs are not 'electronic communications service' providers").

{¶ 13} For other similar recent cases, see *Columbia Pictures, Inc. v. Bunnell* (C.D.Cal.2007), 245 F.R.D. 443 (communications are in electronic storage under the SCA, and thus outside the scope of the Wiretap Act, even when the storage is transitory and lasts only a few seconds); *Pure Power Boot Camp v. Warrior Fitness Boot Camp* (S.D.N.Y.2008), 587 F. Supp. 2d 548 (unauthorized access to e-mails that had previously been sent or received did not constitute an "interception" of an electronic communication under the ECPA; however, employer's access of employee's personal e-mails, which were stored and accessed directly from accounts maintained by outside electronic communication service provider, was unauthorized and thus violated SCA); *Evans v. Evans* (N.C.App.2005), 610 S.E.2d 264 (sexually explicit e-mails that wife had sent to physician, offered by husband in divorce action in support of grounds for divorce and in support of denying postseparation spousal support to wife, were not illegally

intercepted in violation of ECPA, where interception of e-mails was not contemporaneous with transmission; e-mails were stored on and recovered from hard drive of family computer).

{¶ 14} Based on the foregoing authority, it appears that the SCA rather than the Wiretap Act is applicable to the conduct at issue. Thus, even if Jana's conduct violated the SCA, the evidence at issue is not subject to exclusion under the statute.

{¶ 15} Moreover, although no on-point authority was located, it appears that Jana's conduct did not violate the SCA, as her conduct would seem to be authorized, at least implicitly, given her status as parent and how she observed the e-mails on the family computer without the use of her daughter's password. For example, in *Sherman & Co. v. Salton Maxim Housewares* (E.D.Mich.2000), 94 F. Supp. 2d 817, 821, the court stated that "for 'intentional' access in excess of authorization to be a crime and actionable civilly, the offender must have obtained access to private files without authorization (e.g., using a computer he was not to use, or obtaining and using someone else's password or code without authorization)." See also *Pietrylo v. Hillstone Restaurant Group* (Sept. 25, 2009), D.N.J. No. 06-5754, 2009 WL 3128420 (employee's managers violated SCA by knowingly accessing a chat group on a social networking website without authorization; even though employee provided her login information to manager, she did not authorize access by managers to the chat group); *Sporer v. UAL Corp.* (Aug. 27, 2009), N.D.Cal. No. C 08-02835JSW, 2009 WL 2761329 (employer did not violate Wiretap Act when he viewed a pornographic video employee sent from his work account to his personal account; employer had a policy to monitoring employees' computer use and warned employees of policy; thus, employee gave implied consent to his employer to monitor work e-mail account).

{¶ 16} In addition, case law under the Wiretap Act holds that a parent may vicariously consent for the child to the intentional interception of communications as long as the parent has a

good-faith basis that is objectively reasonable for believing that such consent is necessary for the welfare of the minor child. See, e.g., *Pollock v. Pollock* (C.A.6, 1998), 154 F.3d 601, 610; *Babb v. Eagleton* (N.D.Okla.2007), 616 F.Supp.2d 1195; *People v. Clark* (2008), 855 N.Y.S.2d 809. Similarly, it is reasonable and within the parent's authority for the parent to monitor her child's use of the computer in the home for the welfare of the child, particularly under the circumstances presented here. If so, then Jana's conduct would have been "authorized" and thus not in violation of the SCA. In any case, as discussed above, the SCA does not provide for exclusion of the evidence as a remedy for its violation.

Ohio Statutes

{¶ 17} The Ohio statute pertaining to the illegal interception of wire, oral, or electronic communications is set forth in R.C. 2933.51 et seq. The statute is substantially similar to the Wiretap Act. Ohio does not have any statutory provisions comparable to the SCA. R.C. 2933.62(A) excludes evidence derived from the contents of any "intercepted * * * electronic communication" if the disclosure is in violation of R.C. 2933.51 to 2933.66. Similarly, R.C. 2933.63(A) provides that an "aggrieved person" may request that the court "suppress the contents or evidence derived from the contents of a * * * electronic communication * * * unlawfully intercepted." See *State v. Davies* (2001), 145 Ohio App. 3d 630, 763 N.E.2d 1222 (9th Distict) (suppression of evidence under R.C. 2933.62 and 2933.63); *State v. French*, Summit App. No. 24252, 2009-Ohio-2342 (suppression under R.C. 2933.62(A)).

{¶ 18} In *State v. Bell*, 142 Ohio Misc.2d 72, 2007-Ohio-2629, 870 N.E.2d 1256 (Clermont County), the court addressed some of the issues presented here under the Ohio wiretap statute, but in the context of a search warrant issued to seize the defendant's computer. The warrant in *Bell* "sought acquisition of all internal and external computer storage devices thought

to contain e-mail and other electronic messages and images previously transmitted between defendant and T.W. [the alleged victim of defendant's sexual offenses]." Id. at ¶ 17. In addition, the sheriff's office "extracted or copied much of this information from defendant's computer using electronic or mechanical means." Id.

{¶ 19} In ruling on the defendant's motion to suppress, the court addressed the definition of various terms in the Ohio statute that are relevant here, including the term "temporary intermediate storage." As the court discussed, under the Ohio statute, "intercept" is defined as "the aural or other acquisition of the contents of any wire, oral or electronic communication *through the use of an interception device*." (Emphasis added.) R.C. 2933.51(C).

{¶ 20} An "interception device" is thereafter defined as "an electronic, mechanical, or other device or apparatus that can be used to intercept a wire, oral or electronic communication." R.C. 2933.51(D) (the definition excludes certain devices not relevant here). "Electronic communication" is defined as "a transfer of a sign, signal, writing, image, sound, datum, or intelligence of any nature that is transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system." R.C. 2933.51(N) (it excludes wire or oral communications). An "electronic communications system" is defined as a wire, radio, electromagnetic, photoelectronic, or photo-optical facility for the transmission of electronic communications, and a computer facility or related electronic equipment for the electronic storage of electronic communications. R.C. 2933.51(P). "Electronic storage," which is particularly important in this case, is defined as "a temporary, intermediate storage of a wire or electronic communication that is incidental to the electronic transmission of the communication, and a storage of a wire or electronic communication by an electronic communication service for

the purpose of backup protection of the communication." R.C. 2933.51(S). Based on the above definitions, which the court viewed "as both unwieldly and circular," the court concluded that an "interception" is "the electronic or mechanical acquisition of writing or images initially transferred by electronic means and thereafter temporarily stored on electronic equipment. It necessarily follows that if the state plans to acquire electronic writing or images temporarily stored on an individual's computer by using electronic or mechanical means of extraction, the law requires a properly issued interception warrant." *Bell*, 142 Ohio Misc.2d 72, 2007-Ohio-2629, at ¶ 16.

{¶ 21} The court then considered the import of the phrase "temporary, intermediate storage * * * incidental to the electronic transmission of the communication" in the definition of "electronic storage." See R.C. 2933.51(S). The court explained:

> While Ohio courts have apparently been without occasion to expressly address the "temporary storage" of electronic communications incidental to their transmission, the state points out that the statutory definitions of the terms "intercept" and "electronic storage" mirror their federal counterparts. Compare R.C. 2933.51(C) and 2933.51(S) with Sections 2510(4) and 2510(17)(A), Title 18 U.S. Code.

Bell, 142 Ohio Misc.2d 72, 2007-Ohio-2629, at ¶ 18. The state argued that federal law defined "interception" as the government's acquisition of data contemporaneous to its transmission (citing federal cases) and contended that since the information targeted by the warrant was not then being transmitted by the defendant to a third party (but was stored in the computer), the interception-warrant statutes were inapplicable. Id. The court agreed, stating:

> For the several reasons that follow, the court agrees with the state's argument that the reference made in R.C. 2933.51(S) to a "temporary, intermediate storage * * * incidental to the electronic transmission of the communication" is properly characterized as referring to a "real time" acquisition of electronic information upon transfer (i.e., wiretapping or electronic eavesdropping) as opposed to an

> after-the-fact seizure of stored information contained inside a computer. Even with a minority of federal courts rejecting a "rigid storage-transit dichotomy," the period of time for which defendant apparently retained the seized prior communications in his computer demonstrates to this court's satisfaction that it was indeed stored. *Cf. In re Pharmatrak, Inc.* (C.A.1, 2003), 329 F.3d 9, 21; *Potter v. Havlicek* (Feb. 14, 2007), S.D. Ohio No. 3:06-CV-211, 2007 WL 539534.

Id. at ¶ 19. The court then explained its reasons for that determination and concluded that the "retrieval of stored electronic communications may occur without an interception warrant." Id. at ¶ 24.

{¶ 22} Although *Bell* pertains to "interception warrants," I find its holding and reasoning very persuasive. Thus, I find that the conduct here does not fall within the scope of Ohio's wiretap statute. Therefore, the exclusionary rule of this state statute would not be applicable.

{¶ 23} Ohio also has a criminal statute pertaining to unauthorized use of computer or telecommunication property. See R.C. 2913.04. That statute provides:

> (A) No person shall knowingly use or operate the property of another without the consent of the owner or person authorized to give consent.
>
> (B) No person, in any manner and by any means, including, but not limited to, computer hacking, shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service or other person authorized to give consent.

{¶ 24} The affirmative defenses contained in R.C. 2913.03(C) are affirmative defenses to a charge under R.C. 2913.04 (reasonable belief that the actor had consent or

authorization are affirmative defenses). I do not believe that the above statute would apply in a situation such as the one here.

Conclusion

{¶ 25} From the above analysis, this court finds that the admission of the disputed e-mails is permitted under Ohio law. Therefore, defendant's motion is overruled.

So ordered.