HEADLINE: White v. White,
EVIDENCE -- Computers -- E-Mail -- Right to Privacy -- Wiretap Act

CASE-INFO: FM-20-00567-00; Chancery Division, Family Part, Union County; opinion by Issenman, J.S.C.; decided May 31, 2001; approved for publication September 26, 2001. DDS No. 46-4-8238

BODY:
The parties were married on April 26, 1980, and three children, aged 19; 15; and 13, were born of their marriage. Although plaintiff filed for divorce in October 1999, he continues to reside with defendant. He sleeps in the sun room, where the family computer and entertainment center are located. Defendant and the children are often in this room to use the computer, watch television, or adjust the stereo volume. It is also the only way to get to the grill out on the deck. It was in this room that defendant discovered a letter from plaintiff to his girlfriend. According to defendant, it was in plain view; plaintiff denies this.

Shortly afterward, defendant hired Gamma Investigative Research (Private Investigators) and, unbeknownst to plaintiff and without using plaintiff's password, Gamma copied his files from the computer's hard drive. These files contained e-mail between plaintiff and his girlfriend; they also contained images that he viewed on Netscape. Gamma sent a written report detailing its findings to defendant and her attorney. It was only while being deposed that plaintiff learned that defendant had accessed his e-mail. He had thought -- incorrectly as it turns out -- that his e-mail and attachments could not be read without his AOL password.

The technical workings of America Online Service (AOL), plaintiff's chosen Internet Service Provider (ISP), were explained by defendant's expert, John Passerini. Additionally, in the "Notes" section of [the Help screens], America On Line informs the user that he can read mail stored in the PFC when he is not signed onto AOL, i.e. the PFC is on the hard drive. Similarly ... America On Line informs the user that e-mail saved in the PFC will remain on the hard drive until the user deletes it.

Passerini stated that the only way to be sure "that e-mail will be saved permanently is to use the PFC file on the user's hard drive" because "e-mail cannot be saved permanently on AOL's server." It is clear that plaintiff was saving his e-mails -- received and sent -- to the Personal Filing Cabinet (PFC) of the family computer. It is also clear that he did not realize he was doing so. Obviously, not knowing they were being saved, he took no steps to delete them, nor any steps to protect them with a password -- a task easily accomplished. As Passerini states:

[T]he PFC file on the user's hard drive is not automatically password protected.... While the AOL sign-on password is ... required by AOL to establish a dial-up connection, if no PFC password is created, any computer user may view a PFC and e-mails contained in a PFC by simply opening the AOL software on the hard drive. (Emphasis added.)

This is precisely what occurred here: defendant's expert simply opened the AOL software on the family computer's hard drive and viewed and copied plaintiff's e-mails. (The court has no knowledge of the contents of these e-mails. Suffice it to say, defendant believes that they are highly relevant and material to the custody determination yet to be made.)

Held: It is settled law that the New Jersey Wiretapping and Electronic Surveillance Control Act applies when one spouse illegally records the communications of the other spouse. Scott v. Scott, 277 N.J. Super. 601 (Ch. Div. 1994).

It is clear that the language of the N.J. Wiretapping Act contains no explicit exemption for any wiretapping by an aggrieved spouse. It is not the function of the courts to graft an exemption where the Legislature has not seen fit to provide one. M.G. v. J.C., 254 N.J. Super. 470, 477 (Ch. Div. 1991).

The M.G. logic applicable to spousal wiretapping is equally applicable to spousal electronic communications. The Legislature has amended the Act several times since M.G. v. J.C. and Scott v. Scott were decided but did not see fit to enact a spousal exemption. This court, therefore, concludes that the Act applies to unauthorized access of electronic communications of one's spouse, even though there was no violation of the Act in this case.

N.J.S.A. 2A:156A-1 et seq. was enacted in 1968. It is identical to the Federal Wiretap Act. Congress enacted 18 U.S.C. § 2510 et seq. in 1968 to protect wire and oral communications from being intercepted. New Jersey quickly followed suit. Since then, both Congress and state legislatures "have been trying to keep pace with technology, while struggling with the question of what protection certain devices deserve." Vanessa Winter, Note, "What Is a Private Communication: An Analysis of the New Jersey Wiretap Act," 19 Seton Hall Leg. J. 386 (1994).

In 1986 Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) to "update and clarify" federal privacy protections and standards "in light of dramatic changes in new computer and telecommunications technologies." Senate Report No. 99-541, 99th Cong., 2d Sess. 1 (1986). It represented a "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." Ibid.

New Jersey's 1993 amendments, regulating access of stored electronic communications, were identical to the amendments made to the Federal Wiretap statute by the ECPA. Cacciarelli v. Boniface, 325 N.J. Super. 133, 136 (Ch. Div. 1999). At first blush, it would appear that accessing electronic communications in electronic storage without authorization is a violation of N.J.S.A. 2A:156A-27(a). But electronic storage, as used in the Act, means:

(1) Any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (2) Any storage of such communication by an

electronic communication service for purpose of backup protection of the communication.... N.J.S.A. 2A:156A-1(q).

To understand the import of this language, a basic understanding of how e-mail communication works is essential. As explained in Fraser v. Nationwide Mutual Insurance Co.:

Transmission ... is indirect.... After a message is sent, the system stores the message in temporary or ... "intermediate storage" ... in a separate storage for back-up protection, in the event that the system crashes before transmission is completed.... After the message is retrieved by the intended recipient [from intermediate storage], the message is copied to a third type ... "post-transmission storage." A message may remain in post-transmission storage for several years. 2001 WL 290656, 7-8 (E.D. Pa., March 27, 2001).

In other words, all e-mail is stored at some point in the transmission process. David J. Loundy, "E-Law 4: Computer Information Systems Law and System Operators Liability," 21 Seattle U.L. Rev. 1075, 1145 (1998).

The e-mail in the hard drive of the White family computer accessed by defendant was in post-transmission storage. The Act was not meant to extend to e-mail retrieved by the recipient and then stored. It protects only those electronic communications that are in the course of transmission or are backup to that course of transmission. Fraser, 2001 WL 290656 at 11.

The conclusion that the Act does not apply to electronic communications received by the recipient, placed in post-transmission storage, and then accessed by another without authorization appears to make sense when one considers that the "strong expectation of privacy with respect to communication in the course of transmission significantly diminishes once transmission is complete." Id. And, while Congress was concerned with the protection of privacy interests against unjustified intrusions in the original wiretap act, it did not attempt to deal with all such intrusions. See U.S. v. Turk. 526 F.2d 654, 658-59 (5th Cir. 1976), cert. denied, 50 L.Ed.2d 84 (1976). The ECPA and the New Jersey statute represent the "fair balance" between privacy expectations and legitimate intrusion that Congress and the Legislature attempted to achieve in trying to keep pace with the advances in technology.

Furthermore, defendant did not access plaintiff's e-mail "without authorization" in violation of 2A:156A-27(a). It has been held that "without authorization" means using a computer from which one has been prohibited, or using another's password or code without permission. Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F.Supp.2d 817 (E.D. Mich. 2000). Although she did not often use the family computer, defendant had authority to do so. Additionally, defendant did not use plaintiff's password or code without authorization. Rather, she accessed the information in question by roaming in and out of different directories on the hard drive. Where a party "consents to another's access to its computer network, it cannot claim that such access was unauthorized." Id.

at 821.

Moreover, defendant's actions did not constitute an "intercept" as defined by 2A:156A-3(a). The treatment of messages in "electronic storage" is not governed by the restrictions on interception. "Congress did not intend for 'intercept' to apply to 'electronic storage.'" Steve Jackson Games Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994). Said another way,

An "electronic communication," by definition, cannot be "intercepted" when it is in "electronic storage," because only "communications" can be "intercepted," and ... the "electronic storage" of an "electronic communication" is by definition not part of the communication. Bohach v. City of Reno, 932 F.Supp. 1232, 1236 (D. Nev. 1996).

Here, the electronic communications had already ceased being in "electronic storage" as defined by the Act. They were in post-transmission storage -- therefore, defendant did not intercept them.

Interestingly, the Act refers to "access" rather than "disclosure" or "use." Thus, one court has held that a person "can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage." Wesley College v. Pitts, 974 F.Supp. 375, 389 (D. Del. 1997), aff'd o.b. 172 F.3d 861 (3d Cir. 1998). Therefore, because there is no prohibition regarding disclosure or use of the information defendant obtained from the family computer's hard drive, she cannot be barred from using it.

Finally, plaintiff argues that defendant needed a warrant or court order before accessing and copying the contents of his e-mail. That argument is specious because it misconstrues N.J.S.A. 2A:156A-29, which deals with who may compel disclosure of an electronic communication: only a law-enforcement agency and only if the agency has first obtained a warrant or a court order. Not only is defendant not obligated to obtain a warrant, she is legally incapable of doing so.

"The common law recognizes various causes of action relating to the right to privacy." Hennessey v. Coastal Eagle Point Oil Co., 129 N.J. 81, 95 (1992). Plaintiff alleges that, by accessing his e-mail, defendant committed the tort of "intrusion on seclusion." The Restatement (Second) of Torts, § 652B at 378 (1977), states

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

That turns on one's reasonable expectation of privacy. A "reasonable person" cannot conclude that an intrusion is "highly offensive" when the actor intrudes into an area in which one has either a limited or no expectation of privacy.

"[E]xpectations of privacy are established by general social norms." State v. Hempele, 120 N.J. 182, 200 (1990). And, using a Fourth Amendment analysis for purposes of

analogy, one's expectation of privacy must be objectively reasonable; a person's expectation of privacy to a room used for storage and to which others have keys and access is not reasonable, and a subjective belief that the room was private is irrelevant. State v. Brown, 282 N.J. Super. 538, 547 (App. Div.) certif. denied, 143 N.J. 322 (1995).

The same is true here. Whatever plaintiff's subjective beliefs were, objectively, any expectation of privacy under the conditions in this case is not reasonable. Indeed, even subjectively, plaintiff knew his living accommodations were not private: he avers that he did not leave the letter to his girlfriend in plain view.

In DelPresto v. DelPresto, 97 N.J. Super. 446 (App. Div. 1967), the plaintiff-wife found love letters sent to the defendant-husband by his paramour and a receipt for jewelry not given to his wife "in files to which she had a full freedom of entry." Id. at 454. The Appellate Division overruled the trial court's suppression of this evidence. Is rummaging through files in a computer hard drive any different than rummaging through files in an unlocked file cabinet? Not really.

Plaintiff's motion was denied.