

UNAUTHORIZED USE OF PASSWORDS AND PIN(s) IN DIVORCE ACTIONS

By: Mark Gruber, Esq., J. D., L.L.M.

UNAUTHORIZED ACCESS TO STORED COMPUTER FILES – PASSWORD OR PIN(s)

When one spouse accesses stored computer files or e-mails utilizing the other's Password or PIN(s) without their permission, it may be a violation of the Wiretap Statute, if the information is in the transmission stage and not in post-transmission storage. In addition, there is a common-law tort of invasion of privacy or invasion of seclusion. This unauthorized access may also invoke criminal penalties for computer related theft.

WIRETAP VIOLATION?

The basic rule of the New Jersey Wiretap and Electronic Surveillance Control Act is that the interception of wire, electronic or oral communications, by means of electronic, mechanical or other devices is illegal. N.J.S.A. 2A:156A-1, et seq. It is, therefore, illegal when one spouse records the communications of the other spouse, including retrieving e-mail transmissions. However, at least one trial Court in New Jersey has held that retrieving stored e-mail from a hard drive of the family's computer did not constitute unlawful access to stored electronic communications in violation of the New Jersey Wiretap Statute. In the case of White v. White, 344 N.J. Super 211 (Ch. Div. 2001), the Union County Court held that it was not a wiretap violation when the wife accessed information by roaming in and out of different directories on the family's computer hard drive. The Court drew a distinction between e-mails that were in active transmission, as opposed to post transmission storage. When e-mails are in post-transmission storage, they do not fall within the definition of "electronic storage" within the purview of the New Jersey Wiretap Act. Thus, it was not unlawful for a wife to retrieve and use a husband's e-mails that have been stored on the family's computer hard drive, when the wife had access to the family's computer, and did not use a Password or PIN (Personal Identification Number) without the husband's consent or knowledge. The Court reasoned that the husband did not have an objective reasonable expectation of privacy in e-mails stored in the family's computer hard drive, where the computer was in a family room and the entire family had access to the computer.

The New Jersey Wiretap Statute provides criminal penalties for the unlawful access to stored communications. N.J.S.A. 2A:156A-27 provides:

- a. A person is guilty of a crime of the fourth degree if he (1) knowingly accesses without authorization a facility through which an electronic communication service is provided or exceeds an authorization to access that facility, and (2) thereby obtains, alters, or prevents authorized access to a wire or electronic communication while that communication is in electronic storage.

- b. A person is guilty of a crime of the third degree if, for the purpose of commercial advantage, private commercial gain, or malicious destruction or damage, he (1) knowingly accesses without authorization a facility through which an electronic communication service is provided or exceeds an authorization to access that facility, and (2) thereby obtains, alters, or prevents authorized access to a write or electronic communication while that communication is in electronic storage.

In an interesting case, State v. Gaikwad, 349 N.J. Super 62 (App. Div. 2002), the Defendant accessed ATT's computer system without authorization and accessed the accounts of various individuals and copied and read their electronic mail, thereby obtaining sensitive information. The Appellate Division in Gaikwad upheld Mr. Gaikwad's conviction under N.J.S.A. 2A:156A-27b. The Court specifically ruled that Gaikwad's knowing, unauthorized access, reading and copying of a electronic mail in storage in another's mailbox violated N.J.S.A. 2A:156A-27b. This would appear to conflict with the trial court's holding in White v. White, which held that the statute did not apply to electronic communications received by the recipient and placed in post-transmission storage.

THEFT OF COMPUTER DATA?

N.J.S.A. 2C:20-25 provides as follows:

"A person is guilty of theft if he purposely or knowingly and without authorization: (a) alters, damages, takes or destroys any data, database, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network, (b) alters, damages, takes or destroys a computer, computer system or computer network, (c) accesses or attempts to access any computer, computer system or computer network for the purpose of executing a scheme or fraud, or to obtain services, property or money, from the owner of a computer or any third party, or (d) alters, tampers with, obtains, intercepts, damages or destroys a financial instrument."

In the case where a party obtains financial records or other evidence for use in a divorce action, the information taken will usually have little or no monetary value. N.J.S.A. 2C:20-29. In most instances, that crime will be a petty disorderly person's offense as defined in N.J.S.A. 2C:20-29(b):

"A person is guilty of petty disorderly person's offense if he purposely or knowingly accesses and recklessly alters, damages, or destroys or obtains any data, database, computer, computer program, computer software, computer equipment, computer system, or computer network with a value of \$200 or less."

The Criminal Code defines additional criminal activities as follows:

- 2C:20-30. Damage or Wrongful Access to Computer System; No Accessible Damage; Degree of Crime.

A person is guilty of a crime of the third degree if he purposely and without authorization accesses, alters, damages or destroys a computer system or any of its parts, where the accessing and altering cannot be assessed a monetary value or loss.

L.1984, c.184, § 9, eff. March 14, 1985.

- 2C:20-31. Disclosure of Data from Wrongful Access; No assessable Damage; Degree of Crime.

A person is guilty of a crime of the third degree if he purposely and without authorization accesses a computer system or any of its parts and directly or indirectly discloses or causes to be disclosed data, data base, computer software or computer programs, where the accessing and disclosing cannot be assessed monetary value or loss.

L.1984, c.184, § 10, eff. March 14, 1985.

- 2C:20-32. Wrongful Access to Computer; Lack of Damage or Destruction; Disorderly Persons Offense

A person is guilty of a disorderly persons offense if he purposely and without authorization accesses a computer or any of its parts and this action does not result in the altering, damaging or destruction of any property or services.

L.1984, c.184, § 11, eff. March 14, 1985.

Criminal violations of unauthorized use of Password or PIN(s) to obtain data stored in computers fall into two distinct categories – (1) data retrieved from a computer system such as a network of a corporation, business or financial institution, and (2) data unlawfully retrieved from a stand-alone computer. The Court in Gaikwad pointed out that the prohibition proscribed in N.J.S.A. 2C: 20-30 applies only to a computer system and not an individual computer. Thus, when a person accesses a computer system, such as the system containing financial records of a corporation or financial institution, the criminal penalties would apply. When the unauthorized retrieval of data is from a stand-alone computer, it may violate N.J.S.A. 2C:20-25, N.J.S.A. 2C:20-29 or N.J.S.A. 2C:20-32.

COMMON-LAW TORT OF INVASION OF PRIVACY

There is a common-law tort of invasion of privacy, which may be pursued when a spouse obtains information in a way considered “highly offensive to a reasonable person.” This common-law tort will exist even if the action is not prohibited by the New Jersey Wiretap Statute.

RESTATEMENT (SECOND) OF TORTS, §652B (1977) provides:

“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.”

The invasion may be by “physical intrusion into a place in which the Plaintiff has secluded himself ... or it may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank accounts... The intrusion itself makes the Defendant subject to liability, even though there is no publication. (Id. at comment b. 378-79.)

CONCLUSION

The law surrounding the unauthorized access of computer and internet information is evolving. If the unauthorized access of information is obtained from an individual’s computer, the common-law tort of invasion of privacy provides a civil remedy. N.J.S.A. 2C:20-32 (Wrongful Access to Computer) provides a disorderly person’s offense when the unauthorized access does not result in the altering, damaging or destruction of any property or services. It remains unclear whether the retrieval of electronically stored materials in the post-transmission storage is a violation under N.J.S.A. 201256A-27b.

If the unauthorized access is from a computer system, such as a corporation or financial institution, there exists the common-law tort of invasion of privacy, as well as the civil remedies under the New Jersey Wiretap Statute. Additionally, accessing a computer system will violate the criminal statutes of N.J.S.A. 2C:20-25 (Computer-Related Theft), N.J.S.A. 2C:20-30 (Damage or Wrongful Access to Computer System), N.J.S.A. 2C:20-31 (Disclosure of Data for Wrongful Access), and/or N.J.S.A. 2C:20-32 (Wrongful Access to Computer).

Thus, if a spouse uses, without authorization or consent, a private Password or PIN or otherwise obtains personal information of the other spouse, which intentionally intrudes upon their privacy, there is redress.