ASSEMBLY, No. 3308

STATE OF NEW JERSEY

219th LEGISLATURE

INTRODUCED FEBRUARY 25, 2020

Sponsored by:
Assemblyman GREGORY P. MCGUCKIN
District 10 (Ocean)
Assemblyman JOHN CATALANO
District 10 (Ocean)

SYNOPSIS

Clarifies crime of unlawful access concerning certain password protected communications in electronic storage.

CURRENT VERSION OF TEXT

As introduced.

AN ACT concerning unlawful access to certain communications in electronic storage, and amending P.L.1993, c.29.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. Section 21 of P.L.1993, c.29 (C.2A:156A-27) is amended to read as follows:

21. Unlawful access to stored communications.

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. For purposes of this subsection, a person "knowingly accesses without authorization" or "exceeds an authorization to access" if he obtains, alters, or prevents authorized access to a communication that is protected by a password or other personal code, without first knowing and inputting that password or other personal code, or otherwise having the express consent of at least one of the parties to whom that password or other personal code belongs.

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 wire or electronic communication while that communication is in electronic storage. For purposes of this subsection, a person "knowingly accesses without authorization" or "exceeds an authorization to access" if he obtains, alters, or prevents authorized access to a communication that is protected by a password or other personal code, without first knowing and inputting that password or other personal code, or otherwise having the express consent of at least one of the parties to whom that password or other personal code belongs.

c. This section does not apply to conduct authorized: (1) by the person or entity providing a wire or electronic communication service; or (2) by a user of that service with respect to a communication of or intended for that user; or (3) by section 10 of P.L.1968, c.409 (C.2A:156A-10), section 13 of P.L.1968, c.409 (C.2A:156A-13), or by section 23 or 24 of P.L.1993, c.29 (C.2A:156A-29 or C.2A:156A-30).

(cf: P.L.1993, c.29, s.21)

EXPLANATION – Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.

2. This act shall take effect immediately, and apply to any act of unlawful access occurring on or after the effective date.

STATEMENT

This bill amends the provisions of New Jersey's wiretapping statute dealing with unlawful access to stored communications, section 21 of P.L.1993, c.29 (C.2A:156A-27), to clarify criminal liability concerning password protected wire or electronic communications in electronic storage, such as e-mail accounts.

A person would be guilty of a fourth degree crime if that person obtains, alters, or prevents authorized access to any such communication that is protected by a password or other personal code, without first knowing and inputting that password or other personal code, or otherwise having the express consent of at least one of the parties to whom that password or other personal code belongs. As such, there would be no implied consent and no defense from criminal liability for a person who accessed communications after a party to those communications had failed to properly log out or otherwise exit the electronic storage medium containing the communications, leaving such communications unprotected by password or other personal code.

A person would be guilty of a third degree crime for unlawful access, if the person additionally acted for the purpose of commercial advantage, commercial gain, or malicious destruction or damage.

A fourth degree crime is ordinarily punishable by a term of imprisonment of up to 18 months, a fine of up to $10,000, or both. A third degree crime is ordinarily punishable by a term of imprisonment of three to five years, a fine of up to $15,000, or both.

This clarification to criminal liability for unlawful access would also clarify liability in any civil action brought by an aggrieved person whose communications were accessed, due to the availability of such civil actions arising from criminal unlawful access, as set forth in section 26 of P.L.1993, c.29 (C.2A:156A-32).