SECTION-BY-SECTION SUMMARY of Aaron's Law

Legislation Introduced by Senators Ron Wyden and Rand Paul and Representatives Zoe Lofgren, Jim Sensenbrenner, Mike Doyle, Dan Lipinski and Jared Polis

Sec. 1 – SHORT TITLE

Aaron's Law

Sec. 2 – CLARIFYING "ACCESS WITHOUT AUTHORIZATION"

This section modifies definitions in the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. The section strikes the definition of "exceeds authorized access," removes the phrase "exceeds authorized access" from the statute, and creates a definition for "access without authorization." The proposed definition for "access without authorization" is to obtain information on a computer that the accesser lacks authorization to obtain, by knowingly circumventing technological or physical measures designed to prevent unauthorized individuals from obtaining that information.

The proposed changes make clear that the CFAA does not outlaw mere violations of terms of service, website notices, contracts, or employment agreements. The proposed definition of "access without authorization" includes bypassing technological or physical measures via deception (as in the case with phishing or social engineering), and scenarios in which an authorized individual provides a means to circumvent to an unauthorized individual (i.e., sharing login credentials). Examples of technological or physical measures include password requirements, cryptography, or locked office doors. The proposed definition of "access without authorization" is based on recent appellate rulings in the Ninth and Fourth Circuits,[1] which are also followed by some district courts.[2]

The use of viruses, malicious code, denial-of-service attacks, and other hacking attacks would continue to be fully prosecutable under this proposed change to CFAA. The CFAA provision that directly covers these types of hack attacks – 18 U.S.C. 1030(a)(5)(A) – does not use the phrases exceeds authorized access" or "access without authorization," and is thus unaffected by the definitional change proposed in this section. Misuse or theft of information would also continue to be outlawed under numerous statutes, including the Stored Communications Act, Theft of Trade Secrets, wire fraud, copyright law, HIPAA, the Privacy Act, and more.

---

[1] *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), and *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012).

[2] See, e.g., *JBCHoldings NY, LLC vs. Janou Pakter, LLC*, 2013 U.S. Dist. LEXIS 39157 (S.D.N.Y. Mar. 20, 2013).

Sec. 3 – ELIMINATING REDUNDANCY

This section would repeal 18 U.S.C. 1030(a)(4) as redundant.

18 USC 1030(a)(2)(c) is the broadest CFAA provision forbidding "access without authorization." Charges brought under 1030(a)(4) can also be brought under 1030(a)(2)(c), and violations for both provisions carry identical punishments. Under 1030(a)(4), a person who knowingly and with intent to defraud accesses a protected computer without authorization and obtains anything of value over $5,000 can be punished with a fine and imprisonment for not more than five years. Under 1030(a)(2)(C), a person who intentionally accesses a computer without authorization and obtains information valued at more than $5,000 from any protected computer can be punished with a fine and imprisonment for not more than five years. Repealing 1030(a)(4) does not weaken protections under the CFAA, but would preclude charging for redundant violations.

Sec. 4 – MAKING PENALTIES PROPORTIONAL TO CRIMES

This section would modify the penalty enhancement provisions for violations of 18 U.S.C. 1030(a)(2)-(3) and (a)(6). Currently, penalties under 1030(c)(2) rise – from imprisonment for not more than a year to not more than ten years – if the offense occurs after a conviction for another offense of the CFAA. However, the phrase "conviction for another offense" is ambiguous regarding whether the penalty enhancement applies to individuals facing multiple charges in the same case or proceeding.[3] This section would replace the phrase "conviction for another offense" with "subsequent offense" to ensure that the penalty enhancement is directed at repeat offenders rather than individuals facing multiple charges.

The section would also make two additional changes to penalty enhancements for violations of 1030(a)(2). Currently, penalties for violations of 1030(a)(2) rise – from imprisonment for not more than a year to not more than five years – if the value of the information obtained in the course of the violation exceeds $5,000, or if the offense was committed in furtherance of any criminal or tortious act under state or federal laws. First, the section would make clear that the value of the information must be fair market value. Second, the section would establish that the penalty enhancement would not apply to tortious acts (non-criminal violations of law), other CFAA violations, or violations of state equivalents to the CFAA. This would limit the ability of prosecutors to inflate sentences by stacking multiple charges for the same conduct and turning non-felony charges (punishable by imprisonment for a year or less) into felonies.

END

[3] See *Deal. v. U.S.*, 508 U.S. 129 (1993).