Explanation of effects of Aaron's law with EFF proposed amendments to "access without authorization"

(not including amendments to penalty/damages provisions)

EFF proposes a change to the definition of "access without authorization or exceeds authorized access" in both Section 8 of the Computer Fraud and Abuse Act and the Wire Fraud Act to a single definition as follows:

> **The term "access without authorization" means to circumvent technological access barriers to a computer, file, or data without the express or implied permission of the owner or operator of the computer to access the computer, file, or data, but does not include circumventing a technological measure that does not effectively control access to a computer, file, or data.**
>
> **The term "without the express or implied permission" does not include access in violation of a duty, agreement, or contractual obligation, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or employer.**

Note that this suggestion is slightly different from the one sent on January 17, 2013 to reflect some of the suggestions by Orin Kerr and our additional thinking about how to accomplish the same ends.

1) Codifying Ninth and Fourth Circuit law: First, the EFF amended version of Aaron's law codifies the law of the Ninth and Fourth Circuits, specifically the Ninth Circuit Court of Appeals in *U.S. v. Nosal*, 676 F.3d 854, 860 (April 10, 2012) and the Fourth Circuit Court of Appeals in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir., July 2, 2012). As the Ninth Circuit explained:

> "Employer-employee and company-consumer relationships are traditionally governed by tort and contract law; the government's proposed interpretation of the CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law. Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read."

Nosal, 676 F.3d at 860.

2) Protection for circumvention of simple measures that do not allow access to data: Second, it ensures that federal criminal liability does not attach to steps taken by users to protect their privacy and the right to anonymous speech and action online, as well as circumventions around very simple technological measures (like IP address blocking) that are used for commercial advantage or other purposes, but not to protect computers from actual intrusion. Such steps may, and likely will, remain a breach of contract or subject to other civil claims.

3) Criminal liability remains broad: The CFAA and the Wire Fraud Act would continue to penalize outsiders who access a computer system without right and insiders who abuse their credentials on a system to obtain access to sensitive business information to which they are not entitled. The change in federal law would also not impact state laws.

4) CFAA and the Wire Fraud Act now criminalize ordinary Internet behavior. The DOJ has used CFAA language from 1986 to prosecute common network practices on today's Internet, like violating terms of service agreements and downloading information published online without the protection of a password or encryption.

   a) Overbreadth: This makes the 78% of Americans that use the Internet potential criminals, subject to DOJ discretionary enforcement, since nearly everyone violates at least one TOS provision. As the *Nosal* Court observed:

> "Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. . . . The effect this broad construction of the CFAA has on workplace conduct pales by comparison with its effect on everyone else who uses a computer, smart-phone, iPad, Kindle, Nook, X-box, Blu–Ray player or any other Internet-enabled device."

Nosal, 676 F.3d at 860-861.

b) Privacy and security protection measures: Similarly, the law should be clear that no criminal liability attaches to steps that Americans take ensure their right to engage in anonymous speech and other legal activity online, to avoid price discrimination techniques or to gain access to information and services that are otherwise available to them. For example, the following should not be criminal activity, even if the activity might otherwise meet the thresholds for either a misdemeanor or a felony:

i) Using a different IP address to obscure legitimate activity including journalist investigations, human rights activity, whistleblowing, background checks, research into competitors' public practices like pricing or political opposition research.

ii) Using a different IP address or MAC to gain access to information that you otherwise have a right to access, such as information made available on an unencrypted website.

iii) Using a different IP address (*e.g.*, a VPN) to get a better deal based on geographic targeting such as that reportedly done by Staples and Capital One.

iv) Changing a device MAC or User-Agent to get a better deal based on device targeting, such as discounted in-flight wifi for smartphones/tablets, free hotspots for iPhones.

v) Changing the MAC to gain access to a network when device registration is broken, closed or otherwise unavailable.

vi) Changing IP addresses to avoid overbroad blocking by private entities such as spam blocking, botnet and virus blocking organizations.

c) Improper substitution for information protection laws. The CFAA has been used to substitute for information protection laws such as trade secrets and copyright infringement. Trade secret and copyright infringement, however, have limited definitions and

defenses such as misappropriation, non-copyrightability of facts and fair use, all of which balance the public interest with the information owners' rights. The CFAA is a bludgeon rather than a scalpel. The CFAA improperly serves as a tool for the DOJ to substitute its judgment about what should be protected information for the more targeted and intentional information and privacy laws passed by Congress and the States.

5) Other criminal laws, including state laws, penalize information misuse that causes significant harm

i) Insider theft as well as competitor schemes to steal corporate secrets can be prosecuted under the misappropriation of trade secrets statute, 18 U.S.C. § 1832, and state law.

ii) Privacy violations such as the theft of social security numbers can be prosecuted under 18 U.S.C. § 1028 and 18 U.S.C. § 1028A (which has a two year minimum mandatory sentence), the Electronic Communications Privacy Act, state identity theft laws and other statutes that protect such information.

iii) Violations of sanctions regimes and export restrictions, such as accessing restricted information from Iran or North Korea, are subject to severe punishment under those statutes.

iv) Co-conspirators or those who aid and abet criminal activities like stalking or identity theft can be charged under longstanding state and some federal criminal laws.

v) Copyright law contains criminal penalties for "willful" infringement. 17 U.S.C. § 506.

vi) Criminal penalties attach for the circumvention of technological protection measures aimed at protecting copyrighted works. 17 U.S.C. § 1204.