**Lab Assignment 04:**

**United States Law**

Micah Flack

Department of Computer Science, Dakota State University

CSC 840 DT1, Cyber Operations I

Dr. Michael Ham

September 23, 2022

**Summary**

In 2018, police officer Nathan Van Buren, was convicted of a felony in violation of the Computer Fraud and Abuse Act (CFAA). Specifically, statutes U.S.C. § 1030(a)(2), which states, access of any computer system "without authorization or exceeds authorized access" to obtain protected information, financial records, or federal government information is considered a federal crime. Despite being a police officer with previous authorization to access the Georgia Crime Information Center (GCIC), it was argued that Van Buren violated the CFAA when he agreed to accept money for information regarding a license plate about a potential undercover cop for $6,000. Typically, rulings such as this one are favored by law enforcement because it allows flexibility towards apprehending cyber criminals, however, such precedents can cut both ways should they abuse their privileges (Larson et al., 2021; Stanton, 2021). The Supreme Court decided otherwise though, with the majority stating that ‘Improper Motives’ do not suppose exceeded use of prior authorization. Putting the final decision aside, there is significance with this case because it generates discussion about the applicability of CFAA and the need for stronger legal language for cybercrime.

**Sections of the Law and Verdict**

Van Buren was charged with violating statutes U.S.C. § 1030(a)(2) of the CFAA, which specifically states:

Whoever having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; accesses [of] a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer … or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act; information from any department or agency of the United States; or information from any protected computer.

Since he was a police officer with access to the GCIC, which contains protected information, the Justice department argued he violated section 2(b)(c) by abusing said access with malicious intent and no prior context to suggest he had proper authorization to access that information. Ultimately, because of some verbiage changes in 1986 to the law and specific language regarding the use of “so” under section 1, the High Court decided that Van Buren was entitled to the information and not exceeding any prior authorizations. Justice Barrett went on to say during the final decision that, it is best understood as “information that a person is not entitled to obtain by using a computer that he is authorized to access" (Stanton, 2021). Meaning, he was already “entitled” to obtain any information from the GCIC and it was done with a computer he had authorized access from making it legal. Had he used a computer from home to access the GCIC and then pull the license plate information, maybe it would have been interpreted differently.

**Reform**

My understanding is that sections 1 and 2(b)(c) do not, technically, cover the intent of the user regarding their actions when gaining unauthorized access (*Prosecuting Computer Crimes*, n.d.). And any attempts at misusing protected information on those systems with access that was provided only for clearly defined situations, should be considered a textual and spiritual violation of the statutes. For the foreseeable future then, until the necessary laws are passed which do not use vague language but (again) clearly defined situations and intents, we will continue to see murky cases such as Van Buren v United States. I think, this also stems from the fact that US law prefers to be ambiguous when passed to allow prosecution of future crimes. Which allows us to catch more criminals in some creative ways, but it also produces wildly variable sentencing times and inconsistent convictions.

Already, there have been several cases (not under the CFAA) where journalists or programmers have been arrested or convicted because of knee jerk reactions from uneducated local governments. To name a few: the contractors from Iowa arrested during a scheduled penetration test (Goodin, 2020), the journalist who reported on Missouri SSNs being publicly displayed (Brodkin, 2021), or even the programmer whose code was reused by malware authors which led to his arrest (Goodin, 2017). So, because of bad actors and bad laws, we are not allowed to have nice things.

**References**

Brodkin, J. (2021, October 14). *Missouri gov. Calls journalist who found security flaw a “hacker,” threatens to sue*. Ars Technica. https://arstechnica.com/tech-policy/2021/10/missouri-gov-calls-journalist-who-found-security-flaw-a-hacker-threatens-to-sue/

Goodin, D. (2017, August 18). *Code chunk in Kronos malware used long before MalwareTech published it*. Ars Technica. https://arstechnica.com/information-technology/2017/08/code-chunk-in-kronos-malware-used-long-before-malwaretech-published-it/

Goodin, D. (2020, January 30). *Exonerated: Charges dropped against pentesters paid to break into Iowa courthouse*. Ars Technica. https://arstechnica.com/information-technology/2020/01/criminal-charges-dropped-against-2-pentesters-who-broke-into-iowa-courthouse/

Larson, M., Cantor, E., Caron, G., Lopez, A., & Weals, D. (2021). Computer Crimes. *The American Criminal Law Review*, *58*(3), 611.

*Prosecuting Computer Crimes*. (n.d.). 213.

Stanton, L. (2021). High Court Says User’s “Improper Motives” Don’t Create CFAA Violation. *Cybersecurity Policy Report*, 1.