Decriminalizing Trivial Computer Use: The Need to Narrow the Computer Fraud and Abuse Act (CFAA) After *Van Buren*

Benjamin A. Soullier[*]

TABLE OF CONTENTS

[*] J.D., May, 2024, The George Washington University Law School; B.A. May, 2019, European History and Mass Communications, Washington and Lee University. I would like to thank Michael Beder and Thompson Hangen for their encouragement, feedback, and support throughout this process. I would also like to thank Bernard Baffoe-Mensah and Jordyn Johnson for their help during the editing stages. Most notably, I would like to thank Ryan Dickey for introducing me to the CFAA and for the many conversations involving the conception and reworking of the GPS hypotheticals. Finally, I would like to thank Isabelle Chancey for her support throughout my law school journey.

I. INTRODUCTION

Since its conception, the Computer Fraud and Abuse Act (1986) (the CFAA) has tried to play catch-up to tackle issues far more advanced than the current statutory language can support.[1] For years, courts applied the statute almost as broadly as allowable to rule on technologically complicated legal problems.[2] Yet, technological advancement creates the need to narrow certain provisions within the CFAA to prevent the federal government from charging someone for an offense that otherwise would not be considered a crime.[3]

The following hypotheticals are used solely to demonstrate the overbroad nature of the CFAA and how it could potentially be misapplied, thus proving the need to amend the statute.[4] For example, if an individual were to break into a car, start the ignition, and use the car's Global Positioning System (GPS)[5] to plug in a known address and drive to a "chop shop" to sell the car, under most state criminal codes, this is grand larceny.[6] Yet, on top of the state law criminal liability for theft, this scenario could quickly carry serious federal computer crime charges.[7] As implausible as it may seem, the federal hacking statute is engaged solely because of the use of the GPS to navigate to the chop shop.[8] In short, this individual could receive a five-year sentence, in addition to any sentence they receive for the grand larceny charge, for typing in an address he already knew.[9] It may seem equally implausible that a GPS is even a computer[10] and encompassed by the CFAA,

[1] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561-67 (2010); Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 475-77 (1990).

[2] *See* Greg Polaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 9 DUKE L. & TECH. REV. 1, 1-12 (2010).

[3] *Id.*

[4] 18 U.S.C. § 1030(c)(2)(B)(ii).

[5] *GPS Applications*, UNITED STATES SPACE FORCE: GPS.GOV (2014), https://www.gps.gov/applications/ [https://perma.cc/RRT7-ZSKP].

[6] VA. CODE ANN. § 18.2-152.8 (WEST 2011).

[7] 18 U.S.C. § 1030(c)(2)(B)(ii) (Anyone who violates § 1030(a)(2)(C) in "furtherance of any criminal or tortious act" that violates State or Federal law can be punished via fine or up to five years in prison.).

[8] 18 U.S.C. § 1030(a)(2)(C); United States v. Van Buren, 141 S. Ct. 1648, 1660-64 (2021) (The GPS scenario is based on the fact that the individual surpassed the computer's "gate," as the Supreme Court requires for a breach in authorized access, through breaking through the car's door locks and starting the ignition, thus meeting the elements for an (a)(2)(C) violation. In short, the door locks and ignition requirement to start the GPS system serve as the owner expressly intending to prevent access to the car and all its applications to strangers.).

[9] 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii) (The unauthorized use of the GPS to sell stolen goods qualifies as violating § 1030(a)(2)(C) to further another crime, thus triggering the felony enhancement for the CFAA hacking provision.).

[10] 18 U.S.C. § 1030(e)(1) (Any device with data processing or data storage capabilities is considered a "computer."); *See* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 1995) (considering a radio system as a computer).

as an instrumentality of interstate commerce.[11] Additionally, the car's door locks and ignition serve as a "gate" that prevents unauthorized access to the GPS.[12] While all of the above may seem somewhere between unlikely and impossible, this Note will prove otherwise.[13] Furthermore, this Note argues that this scenario is outside of the original scope and purpose of the CFAA, especially for § 1030(a)(2)(C), and as such, the language of the statute should be amended to prevent the prosecution of such actions.[14]

Now, focus on another hypothetical with mostly the same facts as above, but this time, the thief sees a suggested route titled "Home" on the navigation application on the car's dashboard.[15] The thief uses that address to navigate to the owner's home and break in.[16] At this point, the best-case scenario is stolen or damaged property, but if the owner or someone else happens to be in the house, the scenario could become violent very quickly if the burglar turns aggressive.[17] The only aspect that changed between the two scenarios is that in the second hypothetical, the thief used unauthorized access to the GPS to obtain the car owner's home address and burglarize the home.[18] Legally, the difference between the two acts is that in the second, the unauthorized access led to the acquisition of information that was essential to the thief burglarizing the car owner's home, satisfying the felony enhancement standard.[19] Without the electronically stored address and the GPS directions, the thief could not have burglarized the home, or in terms of the statute, advanced another crime or tort, whereas the information obtained in the first hypothetical was simply directions to a known location.[20]

The felony enhancements under § 1030(a)(2)(C)(ii) must be narrowed to exclude punishment for frivolous or insignificant use of technology during

[11] 18 U.S.C. § 1030(e)(2)(B) (A "protected computer" means a device "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."); Generally, courts hold any device that connects to the Internet, or similar interstate or international network, is considered a protected computer; *see* United States v. Auernheimer, 748 F.3d 525, 534 (3rd Cir. 2014); United States v. Yücel, 97 F. Supp. 3d 413, 419 (S.D.N.Y. 2015); United States v. Fowler, No. 8:10-cr-65-T-24, 2010 U.S. Dist. LEXIS 118260, at *4-*8 (M.D. Fla. Oct. 25, 2010); United States v. Morgan 748 F.3d 1024, 1032 (10th Cir. 2014) (finding GPS devices are instrumentalities of interstate commerce for the purposes of Federal kidnapping statutes).

[12] *Van Buren*, 141 S. Ct. at 1660-64.

[13] 18 U.S.C. § 1030(c)(2)(B)(ii).

[14] Griffith, *supra* note 1, at 475-77.

[15] *Connected Navigation*, FORD MOTOR CO.: TECH. (2023), https://www.ford.com/technology/connected-navigation/?gnav=footer-connetedNav [https://perma.cc/88MD-KRJF].

[16] *Id.*

[17] Deane Biermeier & Samantha Allen, *Surprising Home Burglary Facts and Stats*, FORBES (Jan. 23, 2023 8:00 AM), https://www.forbes.com/home-improvement/home-security/home-invasion-statistics/ [https://perma.cc/YPT3-YTGU].

[18] *Connected Navigation*, *supra* note 15.

[19] *Van Buren*, 141 S. Ct. at 1660-63.

[20] 18 U.S.C. § 1030(c)(2)(B)(ii).

the commission of a crime or tort.[21] On the other hand, the amended language must continue to serve the original purposes of the CFAA.[22] This Note specifically focuses on the technological components of car GPS devices to illustrate the need to amend the language of the felony enhancement, but this issue is not exclusive to automobiles or GPS devices.[23] Specifically, analysis of car technology through the two GPS hypotheticals depicts the "gate" breach of a protected computer and the crime of grand larceny as committed through a singular act, thus creating a nexus between two statutory interests: protections against cybercrime and physical crime.[24]

Section 1030(a)(2)(c) of the CFAA prohibits unauthorized use of any "protected computer" or exceeding authorized access.[25] The felony enhancement this Note discusses involves § 1030(c)(2)(B)(ii), which states that anyone who violates (a)(2)(c) "in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State" can be punished by fine or up to five years in prison.[26] Additionally, in *United States v. Yücel*, the Court defined "protected computers" as any device that connects to the Internet.[27] The Court also held that this definition maintained the constitutionality of the CFAA under the Interstate Commerce Clause.[28]

The potential for misapplication of this Section of the CFAA, as illustrated by the GPS hypotheticals, was amplified by the more recent U.S. Supreme Court decision in *Van Buren v. United States*.[29] While this case did not examine the felony enhancements, it clarified what counts as "unauthorized access," thus creating the possibility for the nexus act.[30] In *Van Buren*, the Court used a "gates up, gates down" test to determine if a user is authorized to access a "protected computer."[31] According to the Court, the "gates" must be sufficiently up to prevent access to the computer.[32] In other words, there must be an actual obstacle to access beyond implied permission such as employment agreement policies.[33]

The lasting and perhaps unintended consequence of *Van Buren* is that the Court implies that gates can include physical barriers, so long as they significantly signify to others that access is prohibited or actually restrict or

[21] *See generally* Kerr, *supra* note 1, at 1561-67 (examining the history of amending the CFAA, as technology advances, to restrict prohibitions to the original scope and purposes of the act).

[22] CONG. RSCH. SERV., RL97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS, at 1 (2014), HTTPS://CRSREPORTS.CONGRESS.GOV/PRODUCT/PDF/RL/97-1025 [https://perma.cc/4UQX-R6YQ] (describing the CFAA's purpose to "shield[] [protected computers] from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud").

[23] Kerr, *supra* note 1, at 1561-67.

[24] *Van Buren*, 141 S. Ct. at 1658-63.

[25] 18 U.S.C. § 1030.

[26] *Id.*

[27] *Yücel*, 97 F. Supp. 3d at 419.

[28] *Id.*

[29] *Van Buren*, 141 S. Ct. at 1652; ORIN S. KERR, COMPUTER CRIME LAW, 50-61 (5th ed. 2022).

[30] *Van Buren*, 141 S. Ct. at 1652.

[31] *Id.* at 1658-59.

[32] *Id.*

[33] *Id.* at 1659-63.

prevent access to the protected computer.[34] While the Court did not explicitly define what constitutes a sufficient "gate" to prevent access to a protected computer, the Court broadly stated that at minimum, there must be a clear effort to prevent the access in question.[35] This leaves the possibility for physical barriers or non-code-based barriers[36] to potentially serve as "gates."[37]

Given the recency of *Van Buren*, the GPS hypotheticals are meant to serve as a lens to view the larger issue of the overbroad felony enhancements by analyzing simple technology and the nexus between a "gate" and a traditional auto theft.[38] The scope of this issue is not limited to car theft or GPS misuse. Conversely, the hypotheticals are used to demonstrate the larger issue which is the overbroad nature[39] of § 1030(c)(2)(B)(ii)'s felony enhancement leading to potential misapplication following the decision in *Van Buren* and the creation of the "gates up or down" standard.[40] In other words, the simple fact that these car theft hypotheticals could reasonably occur proves the need for a narrower statute and standard. Additionally, the Court in *Van Buren* refused to accept the government's argument that prosecutorial discretion would prevent arbitrary criminal charging based on private employer-drafted work policies.[41] The Court specifically said this argument would lead to prosecutions that "may not be warranted" and not expressly "prohibited," contradicting the CFAA's text and purpose.[42] Therefore, after evaluating the statute through the lens of the GPS hypotheticals, the law must be narrowed by either the Court or Congress in order to correct the problem and avoid the type of arbitrary prosecution the Court was concerned about in *Van Buren*.[43]

To address these issues, felony enhancements under § 1030(c)(2)(B)(ii) should be amended to apply only when an individual knowingly[44] uses the information obtained through unauthorized access to a protected computer to

[34] *Id.*

[35] *Id.*

[36] This Note does not address the issue of whether "breaching authorized access" should be narrowed to only apply to code-based restrictions because even if this were the case, the felony enhancements remain too broad and must be limited. Therefore, this Note focuses only on the nature of the felony enhancements and creating a more specific legal standard. *See generally* George F. Leahy, *Keeping Gates Down: Further Narrowing the Computer Fraud and Abuse Act in the Wake of Van Buren*, 14 WM. & MARY BUS. L. REV. 215, 218-22 (2022) (discussing the importance of code-based barriers protecting personal information).

[37] *Van Buren*, 141 S. Ct. at 1660-63 (The Court determined that the "gates" did not necessarily need to be limited to traditional passwords, encryption, or other cyber methods of securing computers, but that physical locks or other efforts to prevent access that were expressly communicated as security measures could also be considered "gates.").

[38] *Id.*

[39] Kerr, *supra* note 1, at 1561-67.

[40] *Van Buren*, 141 S. Ct. at 1660-63.

[41] *Id.* at 1662.

[42] *Id.*

[43] *Id.*

[44] Knowingly, as defined in the context of the CFAA damage statute 18 U.S.C. § 1030(a)(5), is an action taken where the result is practically certain; *see* United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991) (The court held whether or not a defendant intends to cause damage is irrelevant so long as the defendant knew or reasonably should have known their actions could cause damage.).

substantially[45] further "any criminal or tortious act."[46] The statute as amended would protect against the potential criminalization of computer acts that would not, if isolated, be violations of the CFAA, while also preserving the privacy protection interests the CFAA was originally intended to fortify.[47] In other words, the amended provision sufficiently gives citizens clear notice of potential violations, while punishing those who purposefully use a computer, without authorization, as a critical component to advance a criminal or tortious act or use a protected computer without authorization to significantly violate the owner's privacy rights to contribute to a criminal or tortious goal.[48] Ultimately, no one would receive jail time for frivolous or incidental use of technology.[49]

This Note first describes Congress's motivation and purpose in drafting the CFAA.[50] Then, this Note will define § 1030(a)(2), the standard for breaching or exceeding authorized access, and the changes established by *Van Buren*.[51] Additionally, this Note will outline the felony enhancements under § 1030(c)(2)(B)(ii). This Note will subsequently define a "computer" and "protected computer" and establish car theft as a major issue throughout the U.S.[52] Finally, this Note will examine in more detail the hypothetical situations mentioned previously to illustrate the overbroad nature of the felony enhancements and the effectiveness of the proposed amended provision to correct this issue.[53]

II. BACKGROUND

A. The CFAA and Subsequent Jurisprudence

This Section first looks to the origins of the Computer Fraud and Abuse Act and the information privacy concerns it intended to address to establish why the § 1030(a)(2)(C) felony enhancements create opportunities for overbroad application and frivolous prosecution.[54] Next, it is important to examine what constitutes a § 1030(a)(2)(C) violation after the decision in *Van Buren,* because in order to apply the felony enhancements,[55] an individual must first breach the "gate" to a "protected computer."[56] Afterward, this Note

[45] The "substantial" prong of this standard is based on federal criminal attempt law, which requires the individual to take a "substantial step" towards completing the crime; *see* United States v. Taylor, 142 S. Ct. 2015, 2020 (2022) ("a substantial step . . . beyond mere preparation"); *see also* United States v. Resendiz-Ponce, 549 U.S. 102, 107 (2007); MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

[46] 18 U.S.C. § 1030(c)(2)(B)(ii).

[47] Griffith, *supra* note 1, at 475-77.

[48] *Id.*

[49] *Id.*

[50] 8 U.S.C. § 1030; *see also* Griffith, *supra* note 1, at 475-77.

[51] *Van Buren*, 141 S. Ct. at 1660-63.

[52] *Auernheimer*, 748 F.3d at 534; *Yücel*, 97 F. Supp. 3d at 419; *Fowler*, 2010 U.S. Dist. LEXIS, at *4-*8.

[53] Kerr, *supra* note 1, at 1561-67.

[54] Griffith, *supra* note 1, at 475-77.

[55] 18 U.S.C. § 1030(c)(2)(B)(ii).

[56] 18 U.S.C. § 1030(a)(2)(C); *Van Buren*, 141 S. Ct. at 1660-63.

will establish which devices constitute "computers"[57] and "protected computers."[58]

B. Origins of the CFAA

The CFAA is rooted in the protection of privacy, as well as the fear of how far technology could advance beyond the scope of statutory regulations drafted for traditional crimes of the physical world.[59] However, the CFAA was not the first attempt at addressing these issues.[60] The proposed Computer Trespass Act of 1984 was an attempt by Congress to regulate computer crimes in the early stages of computer development.[61] The bill, which never made it into law, would have targeted the unauthorized use, or use exceeding authorization, of computers to "obtain certain information classified under the Atomic Energy Act of 1954 or certain financial records covered by the Right to Financial Privacy Act of 1978."[62] Government and military computers would also have been protected, but the bill was not designed to protect the personal computers of individual citizens unless financial documents were involved.[63] Congress's initial focus on national security and the financial sector carried into the early drafting of the CFAA.[64] However, the final version that was passed in 1986 remains largely intact today and includes more general provisions intended to replicate traditional criminal code and tort law, specifically copyright infringement.[65]

Initially introduced in 1984 and passed in full in 1986, the Computer Fraud and Abuse Act was drafted to broadly regulate potential violations of

[57] 18 U.S.C. § 1030(e)(1).

[58] 18 U.S.C. § 1030(e)(2).

[59] Griffith, *supra* note 1, at 467-70.

[60] Computer Trespasses Act, H.R. 5616, 98th Cong. (1984), https://www.congress.gov/bill/98th-congress/house-bill/5616 [https://perma.cc/82C8-2ATL] (The act passed the House of Representatives and then passed the Senate with amendments, but the changes were not reconciled.).

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] *See generally* STEPHANIE RICKER SCHULTE, "THE WARGAMES SCENARIO" REGULATING TEENAGERS AND TEENAGED TECHNOLOGY 1-5 (1980–1984) (2008) (The plot of the 1983 hit movie "WarGames" follows a teenager, played by Matthew Broderick, who "hacked" into a military computer controlling the U.S. nuclear operations and accidentally almost started World War III. This influenced Congress to punish computer trespasses and, "hearings ultimately resulted in the nation's first comprehensive legislations about the Internet and the first ever federal legislation on computer crime: the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984."); *see* 18 U.S.C. § 1030(e)(2)(A) (The act mentions computers "exclusively for the use of a financial institution or the United States Government" when defining protected computers, suggesting the importance lawmakers placed on insuring these devices were secure.).

[65] *See* H. MARSHALL JARRETT AND MICHAEL W. BAILIE, PROSECUTING COMPUTER CRIMES 20 (Office of Legal Education Executive Office for United States Attorneys: Computer Crime and Intellectual Property Section Criminal Division 2017) (this U.S. Attorney's Office publication specifically mentions how the language of the felony enhancements for 18 U.S.C. 1030(a)(2)(C), detailed in 18 U.S.C. 1030(c)(2)(B)(ii), were borrowed from the copyright law and wiretap statutes); s*ee* Copyright Act, 17 U.S.C. §§ 101-1511 (1980); s*ee* Wiretap Act, 18 U.S.C. § 2511 (1968).

privacy and abuses of functionality regarding computers.[66] Congress hoped to enact a new set of laws to address issues of computer insecurity and protect the private information of American citizens.[67] In general, there are two types of "computer crimes" that the American legal system is equipped to regulate: (1) "computer misuse crimes," which are considered the "intentional interference with the proper functionality of computers" and (2) "traditional criminal offenses facilitated by computers."[68] Examples of computer misuse crimes include hacking, denial of service attacks, phishing, and virus implementation.[69] "Traditional" computer-facilitated offenses typically include fraud, online threats, child pornography, and gambling.[70] The CFAA was drafted to regulate both computer misuse crimes and computer-facilitated offenses, but §§ 1030(a)(1)–(5) are predominately concerned with acts of computer misuse.[71]

C. *Breaching Authorized Access Under § 1030(a)(2)(C) and* Van Buren

This Note specifically examines § 1030(a)(2)(C), which is ordinarily a misdemeanor but carries a felony enhancement under § 1030(c)(2)(B).[72] Section (a)(2)(C) reads, "whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section."[73] Cases involving violations of § 1030(a)(2) typically include breaching a computer's security measures but can also include the use of a computer or network for purposes other than its intended use.[74] So in the context of the GPS hypothetical, the computer's security measures or the "gate" preventing unauthorized access would be the combination of the car's locked doors and ignition powering on the GPS.[75]

In 2021, however, the Supreme Court clarified what exactly is required to determine when an individual is authorized to access a computer and, if

[66] 18 U.S.C. § 1030; Griffith, *supra* note 1, at 476 (The original format of the CFAA and specifically § 1030(a)(2), directly referenced the Right to Financial Privacy Act of 1978. Specifically, "[t]he premise of . . . [§ 1030](a)(2) was to protect, for privacy reasons, the computerized credit records and computerized information relating to customers' relationships with financial institutions. Congress wanted to extend the same privacy protection to the financial records of all customers of financial institutions, including individuals, partnerships, or corporations. To accomplish this aim, Congress redefined the terms "financial institution" and "financial record" in broader terms than those provided by the Right to Financial Privacy Act of 1978.").

[67] Griffith, *supra* note 1, at 476.

[68] KERR, *supra* note 29, at 1-5.

[69] *Id.*

[70] *Id.*

[71] 18 U.S.C. § 1030.

[72] 18 U.S.C. § 1030(a).

[73] *Id.*

[74] *Morris*, 928 F.2d at 504-08 (Defendant, a graduate student, was authorized to access Cornell University's computer equipment and network but used a computer program or "worm" that multiplied itself onto other systems, including U.S. military systems and caused significant damage, leading the court to hold Morris breached authorized access.).

[75] *Van Buren*, 141 S. Ct. at 1653, 1660.

they are, when authorized access is exceeded.[76] In *United States v. Van Buren*, police officer Nathan Van Buren (defendant) made a deal with Andrew Albo for a loan of $5,000 in exchange for Van Buren investigating a woman acquainted with Albo.[77] Albo then recorded his conversations and subsequent agreement with Van Buren and gave the tapes to the Federal Bureau of Investigation (FBI).[78] Using a police computer in his car, Van Buren conducted a full search of the woman in question.[79] Van Buren was then charged with violations of 18 U.S.C. § 1030(a)(2).[80]

Both parties agreed Van Buren was authorized to access the computer generally and conduct investigative searches for police purposes, but the two sides disputed whether he exceeded this access by conducting personally motivated searches in exchange for money.[81] The government argued individuals must be expressly approved to conduct each individual search and searches for personal gain were prohibited by department policy.[82] Whereas Van Buren argued that he was generally authorized to use the system and could conduct the search he chose without criminal liability.[83] In other words, the government argued that even though Van Buren technically could access the information and was allowed to conduct searches on his police computer, the search for Albo violated the interests of his employer.[84] On the other hand, Van Buren argued that the statute meant he must be prevented from searching altogether.[85] The Court agreed with Van Buren and held he did not breach or "exceed authorized access" to a protected computer because there was no barrier preventing him from accessing the information.[86] He was authorized, as a police officer, to search the system for information on individuals, and department policies about when such searches are permitted were not sufficient to serve as a "gate."[87]

After *Van Buren*, courts have looked for barriers preventing individuals from accessing the computer or the functionality of the computer.[88] In *Zap Cellular v. Weintraub*, the Eastern District of New York applied the *Van Buren* standard and held that a company terminating an employee was sufficient to close the gate on that individual's access to the computer system.[89] The Court explained that the company took an overt action to expressly prohibit the defendant's actions when it terminated the defendant's employment.[90] Thus, moving forward, the legal standard would likely accept

[76] *Id.* at 1662.
[77] *Id.* at 1653.
[78] *Id.* at 1663.
[79] *Id.* at 1653.
[80] *Id.*
[81] *Van Buren*, 141 S. Ct. at 1653-54.
[82] *Id.*
[83] *Id.* at 1654-55. (Civil liability or employment termination are separate issues.).
[84] *Id.*
[85] *Id.*
[86] *Id.* at 1660.
[87] *Id.*
[88] Zap Cellular, Inc. v. Weintraub, No. 15-CV-6723, 2022 U.S. Dist. LEXIS 168735, at *1-*3 (E.D.N.Y. Sept. 19, 2022).
[89] *Id.*
[90] *Id.*

any clear indicator or effort to prevent access, stronger than employment policies, as a "gate" under *Van Buren*.[91]

Van Buren creates the need to narrow the scope of the statute because physical barriers can serve as security measures to prevent access to a computer, such as locking a car door to prevent access to the ignition.[92] Thus, the car door locks and ignition can become physical barriers to the dashboard computer.[93] More specifically, the lock on the car door prevents access to the ignition, and the ignition prevents access to the car's dashboard computer.[94] So technically, there are two gates, both connected to the crime of grand larceny because a burglar must bypass the door locks and ignition system.[95] Once both "gates" are breached, the ignition being the more vital to accessing the computer, and the burglar using the car's computer in relation to another crime or tort, the felony enhancements can be implemented.[96] In short, the Supreme Court's test allowing for physical barriers to determine who is authorized to access a computer presents the opportunity for the GPS hypothetical to be charged as a felony violation of § 1030(a)(2)(C).[97]

D. Felony Enhancements for § 1030(a)(2)(C) Crimes

Next, it is important to determine when the § 1030(a)(2)(C) felony enhancements are applicable.[98] The CFAA's hacking felony enhancements apply if "the [hacking of a protected computer] was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[99] If convicted, individuals could be subject to a fine and up to five years in prison.[100] The underlying tort or criminal act being advanced cannot be the same as the action that violates § 1030(a)(2)(C); however, that act is not limited to traditional crimes or torts of the physical world.[101] In *United States v. Steele*, the defendant was fired by his employer but continued to use his account via a "backdoor" login to "access and download documents and emails" concerning active government contract bids involving the parent company.[102] The court held that termination of Steele's employment meant he was no longer "authorized" to access the system and thus violated § 1030(a)(2)(C), although he technically could still access the company's server.[103] The court also held that the application of the felony enhancements to the Virginia state crime of grand larceny did not merge with the defendant's hacking into his former employer's computer to steal company data because the data qualified as property under Va. Code

[91] *Van Buren*, 141 S. Ct. at 1658-59; *Zap Cellular*, 2022 U.S. Dist. LEXIS, at *26-*28.
[92] *Van Buren*, 141 S. Ct. at 1658-59.
[93] *Id.* at 1658-59; FORD, *supra* note 15.
[94] *Van Buren*, 141 S. Ct. at 1658-59.
[95] VA. CODE ANN. § 18.2-95 (LEXIS 2022).
[96] 18 U.S.C. § 1030(c)(2)(B)(ii).
[97] *Van Buren*, 141 S. Ct. at 1658-59; 18 U.S.C. § 1030(c)(2)(B)(ii).
[98] 18 U.S.C. § 1030(c)(2)(B)(ii).
[99] *Id.*
[100] *Id.*
[101] United States v. Steele, 595 F. App'x 208, 216 (4th Cir. 2014).
[102] *Id.* at 210.
[103] *Id.* at 212.

Ann. § 18.2-152.[104] In other words, the defendant could be punished for breaching the gate to commit a crime and for stealing the data as property.[105] The data regarding the contract bids were obtained via Steele's unauthorized access, but the court found that Steele used that unauthorized access to commit grand larceny, and thus the government was not in danger of unconstitutionally subjecting Steele to double jeopardy.[106]

The felony enhancements in the CFAA were borrowed from the language in copyright law and wiretap statutes and, therefore, were never specifically drafted to address computer hacking issues.[107] According to a manual published by the U.S. Attorney's Office's Computer Crime and Intellectual Property Section Criminal Division, when investigating these crimes, a prosecutor should use their discretion to determine, "whether the defendant manifested an intent to commit a state tort" when they violated § 1030(a)(2)(C).[108] For hacking crimes in furtherance of a criminal act, prosecutors must simply prove a defendant committed a criminal act, and that act was progressed by an action that violated § 1030(a)(2)(C).[109]

While the use of prosecutorial discretion is the preferred method of the U.S. Attorney's Office for enforcing the CFAA, the Supreme Court refuses to accept these types of arguments and maintains statutory specificity through legislative action as the proper course of action.[110] Specifically, in *Van Buren*, the government argued that charging § 1030(a)(2) for computer use that violated workplace guidelines would not be arbitrary because prosecutorial discretion would only lead to charges that warranted punishment.[111] However, the Court refused to accept this argument, stating this strategy would be arbitrary because "[t]he policy instructs that federal prosecution 'may not be warranted'—not that it would be prohibited—'if the defendant exceed[s] authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website.'"[112] In other words, the Court clarified the statute to require actual prevention of access (code-based or otherwise), instead of spoken or written employer policies serving as a gate.[113]

E. Defining a "Computer"

For the GPS hypothetical to become an issue of CFAA over-broadness, the car's navigation system must first be proven to be a computer and then

[104] *Id.* at 216.

[105] *Id.*

[106] *Id.*

[107] Jarrett, *supra* note 65, at 19-20, ("[T]he legislative history of § 1030 reveals that Congress intended the phrase to have the same meaning as identical language under the Wiretap Act, and cases construing that language hold the phrase encompasses state common law torts."); *see also* S. Rep. No. 104-357, at 8 (1996).

[108] Jarrett, *supra* note 65, at 19-20.

[109] *Id.* at 94.

[110] *Van Buren*, 141 S. Ct. at 1660-62.

[111] *Id.*

[112] *Id.* at 1662.

[113] *Id.*

subsequently a protected computer.[114] For CFAA prosecution, computers are devices subject to illegal manipulation or abuse, or tools for committing traditional crimes.[115] The CFAA's definition of computers is not limited to conventional understandings of desktops, laptops, or even smartphones.[116] According to 18 U.S.C. § 1030(e)(1), a "computer" is defined as:

> An electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable handheld calculator, or other similar device.[117]

In *United States v. Mitra*, the Seventh Circuit examined whether a radio system was considered a "computer" under the statute.[118] In this case, the city of Madison, Wisconsin, like most other cities, frequently used radio communications for their police, fire, and emergency response departments.[119] Mitra was able to analyze and eventually block radio communications for the city of Madison's emergency response personnel on a weekend when the city had a large number of visitors.[120] The appellate court held that radio signals, similar to the devices listed in the statute, are computers and in this case, protected computers.[121] Judge Frank Easterbrook wrote in his opinion for the court, "[E]very cell phone and cell tower is a 'computer' under the statute's definition; so is every iPod, every wireless base station in the corner coffee shop, and many another gadget[s]."[122] This definition of computers appears to be consistent with the statute's broad language describing computers as any device with "processing' capabilities.[123]

In a similar case in 2011, the Eighth Circuit held a cell phone, not a smartphone, used solely for voice calls and text messages was a "computer" under the statutory language.[124] In *United States v. Kramer*, the defendant pled guilty to "transporting a minor in interstate commerce with the intent to

[114] 18 U.S.C. § 1030(a)(2)(C) (The statute requires information be acquired from a "protected computer.").

[115] KERR , supra note 29, at 1-5; 18 U.S.C. § 1030(e)(2).

[116] 18 U.S.C. § 1030(e)(2).

[117] 18 U.S.C. § 1030(e)(1).

[118] United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005); 18 U.S.C. § 1030(e)(1); KERR, *supra* note 29, at 82-83.

[119] *Mitra*, 405 F.3d at 493.

[120] *Id.* at 495.

[121] *Id.*

[122] *Id.*

[123] 18 U.S.C. § 1030(e)(1).

[124] 18 U.S.C. § 1030(e)(1); United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011); KERR, *supra* note 29, at 82-83.

engage in criminal sexual activity with her."[125] While committing this crime, Kramer used a cell phone to call and text the victim for the six months leading up to the offense.[126] Although Kramer was not charged with violating the CFAA, the court examined § 1030(e)(1)'s definition of a computer to see if Kramer's cell phone met the requirements for sentence enhancement through the use of technology during a kidnapping offense.[127] The defendant argued that the phone's ability to make voice calls and send text messages did not make it a computer under the statute.[128] However, the court disagreed and found Kramer's cell phone was a computer under the statute, reasoning that "the definition captures any device that makes use of a[n] electronic data processor," which Kramer's cellphone possessed.[129] The court also held that "computers" do not necessarily need an Internet connection but instead simply require storage and processing capabilities.[130] It is also worth noting that in evaluating the sentence enhancement, the appellate court held that "the enhancement does not apply to every offender who happens to use a computer-controlled microwave or coffeemaker . . . [but] limits application of the enhancement to those offenders who use a computer 'to communicate directly with a minor.'"[131] Ultimately, the court seems to reason that (1) the cellular phone meets the broad definition of "data processing" device from the statute and (2) the cellphone was critical to the commission of the crime, justifying the sentence enhancement.[132] Overall, courts generally accept a broad definition of computers under the CFAA.[133]

F. Defining a "Protected Computer"

For someone to violate § 1030(a)(2), they must gain unauthorized access to or exceed authorized access to a "protected computer."[134] In other words, it does not matter if the gates are up or down if the device is not considered a "protected computer."[135] While the definition of a "computer" is primarily reliant on the device's data processing and storage capabilities and does not necessarily require an Internet connection, a "protected computer" carries a much narrower definition.[136] A "protected computer" includes any "computer," as defined above, "used in or affecting interstate or foreign

[125] *Kramer*, 631 F.3d at 901 (Kramer was sentenced to 168 months in prison by the district for his offense, and in reaching this decision, the district court, "applied a two-level enhancement for its use to facilitate the offense, *see* U.S. SENT'G GUIDELINES MANUAL § 2G1.3(b)(3) (2009).").

[126] *Kramer*, 631 F.3d at 902-03.

[127] *Id.*

[128] 18 U.S.C. § 1030(e)(1); Kramer, 631 F.3d at 903.

[129] *Kramer*, 631 F.3d at 902-03.

[130] *Id.* at 904.

[131] *Id.* at 903; U.S. SENT'G GUIDELINES MANUAL § 2G1.3(b)(3) cmt. N.4 (U.S. SENT'G COMM'N 2009).

[132] 18 U.S.C. § 1030(e)(1); *Kramer*, 631 F.3d at 904.

[133] *Kramer*, 631 F.3d at 902-903; *Mitra*, 405 F.3d at 493; KERR, *supra* note 29, at 82-83.

[134] 18 U.S.C. § 1030(a)(2).

[135] *Id.*

[136] 18 U.S.C. § 1030(e)(1)-(2)(B).

commerce or communication" or any computer used by financial institutions or the U.S. government.[137]

In practice, courts usually hold any computer with access to the Internet as a protected computer because these computers are connected to a larger network involved with or impacting interstate commerce.[138] In *United States v. Fowler*, the defendant accessed Suncoast Community Health Centers' computer system and caused damage, under § 1030(a)(5)(A).[139] Fowler transmitted a program after she was fired that prevented Suncoast employees from accessing their accounts.[140] Fowler argued that the Suncoast computers were not "protected computers" because they were not government or financial institution computers, and they were not involved in interstate commerce.[141] However, the court disagreed and held that since the computers were connected to the Internet, they were involved in interstate commerce.[142] The court heavily emphasized the longstanding doctrine that "the Internet is an instrumentality of interstate commerce," [143] or in other words, is a vessel through which "commerce" between the states is facilitated.[144] Thus, Congress is constitutionally authorized to regulate devices connected to a national and international network.[145] After establishing Internet-connected computers are considered an instrumentality of interstate commerce, the court in *Fowler* concluded that Suncoast's computers met the definition of "protected computer," as they could be, "used in or affecting interstate or foreign commerce or communications," as defined by the statute.[146]

A few years later in 2015, the Southern District of New York followed the principles established in *Fowler*.[147] In *United States v. Yücel*, the defendant was charged with being a leader of a group that "distributed malicious software," or malware, which allowed the group to control people's computers from a remote location.[148] The software also allowed the defendant and his co-conspirators to copy "keystrokes," turn on the owner's webcam, and search the computers' files and data.[149] The defendant argued that if any computer with Internet access is considered a "protected computer," then the statute is overly broad and gives Congress the power to limit too many acts.[150] However, the court disagreed in this regard because a "protected computer"

[137] 18 U.S.C. § 1030(e)(2)(B); Jarrett, *supra* note 65, at 94.

[138] 18 U.S.C. § 1030(e)(2)(B); *Auernheimer*, 748 F.3d at 534; *Yücel*, 97 F. Supp. 3d at 419; *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8.

[139] 18 U.S.C. § 1030(a)(5(A) ("knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer"); *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8.

[140] *Fowler*, 2010 U.S. Dist. LEXIS at 4-8.

[141] 18 U.S.C. § 1030(e)(2)(B); *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8.

[142] *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8 (citing United States v. Walters, 182 Fed. App'x 944, 945 (11th Cir. 2006) ("the Internet is an instrumentality of interstate commerce")).

[143] *Id.*

[144] Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241, 271 (1964).

[145] *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8 (citing *Walters*, 182 Fed. App'x At 945; United States v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004)).

[146] 18 U.S.C. § 1030(e)(2)(B); *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8.

[147] *Yücel*, 97 F. Supp. 3d at 419.

[148] *Id.*

[149] *Id.*

[150] *Id.* at 420.

was only one element in the crime, and the government must prove, in the case of *Yücel*, that the defendant breached authorized access and caused damage.[151] The court, after citing several cases from various jurisdictions, ultimately held that "the widespread agreement in the case law on the meaning of 'protected computer,' gives adequate notice to potential wrongdoers of what computers are covered by the statute."[152] In other words, the defendant was no special target under the circumstances of the case, and the standard, as applied, is constitutional.[153]

The concept of the Internet as an instrumentality is best illustrated in *Hornaday*.[154] In this case, the defendant sent an Internet message to an undercover government agent soliciting sex from two minors.[155] The defendant challenged Congress's power to regulate Internet solicitation of minors, but the Eleventh Circuit ultimately held that the Internet was an instrumentality through which the defendant sought "child victims."[156] The court also held that regardless of the Internet's mostly "intrastate" impact, Congress still has the power to regulate such conduct given the potentially massive impact on interstate and foreign commerce.[157]

III. CREATING THE "SUBSTANTIAL FURTHERANCE TEST"

This section will set forth the legal standard and framework for the "Substantial Furtherance Test" that this Note proposes.[158] The need for such a standard is clear based on the overbroad nature of the CFAA, specifically, the felony enhancement for § 1030(a)(2).[159] This test, if adopted by courts or the legislature, would serve as the last element of the CFAA hacking violation felony enhancement analysis.[160] This would serve to eliminate the issue illustrated by the two GPS hypotheticals and the vagueness associated with the act itself.[161]

In order to craft this test, this Note looks to combine the existing standard for the federal attempt law[162] and the mens rea definitions for knowledge requirement as applied in the computer damage statutes of the

[151] *Id.*

[152] *Id.*

[153] *Yücel*, 97 F. Supp. 3d at 420.

[154] *Hornaday*, 392 F.3d at 1311.

[155] *Id.*

[156] *Id.* at 1310-11.

[157] *Hornaday*, 392 F.3d at 1311-12; (citing Heart of Atlanta Motel, Inc., 397 U.S. at 285 (1964) (holding that lodging for intrastate or local use still served an interstate instrumentality purpose and thus could be regulated under the Commerce Clause)).

[158] 18 U.S.C. § 1030(a)(5); *Morris*, 928 F.2d at 509-11; *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

[159] *See generally* Kerr, *supra* note 1, at 1561-67.

[160] 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii).

[161] Kerr, *supra* note 1, at 1561-67.

[162] *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

CFAA.[163] Attempt is defined as taking a "substantial step" towards achieving the goal of completing the crime "beyond mere preparation."[164] This is, in other words, an act that is "strongly corroborative of the actor's criminal purpose."[165]

The second component, knowledge, is derived from the CFAA damage statute § 1030(a)(5), which requires the defendant to "knowingly" cause damage.[166] This standard, as derived from *U.S. v. Morris*, must be an action taken where the result is practically certain.[167] In *Morris*, the defendant was charged § 1030(a)(5)(A) for damaging university and military computers by uploading a virus but argued he never intended to damage the computers, just gain access.[168] The court dismissed the defendant's argument and established the "intended function" test in which the court determined the software's intended function as a virus was to damage computers.[169] The defendant's intent was irrelevant so long as he knew or reasonably should have known the virus could cause damage if uploaded.[170]

The reasoning behind these additions to the standard is to eliminate the possibility of criminal liability for frivolous or insignificant computer use in connection to a crime or tort.[171] To achieve this goal, a line must be drawn between computer use that initiates or aids the attempt or completion of a separate crime or tort, and unauthorized computer use that does not initiate or aid such underlying acts.[172] Therefore, the test must include a significance factor, similar to that of a "substantial step" or "corroborative act," to determine when an individual knowingly makes an effort or makes a significant choice to use the information obtained through unauthorized access to further a crime or tort, and when that person just happens to use technology that is simply related to a crime or tort without significantly impacting the separate violation.[173] The current CFAA language simply states "in furtherance" of a crime or tort, without any requirement as to the significance of the technological contribution.[174] However, with the addition of a "substantial" effort requirement, the new test would significantly decrease the possibility of criminalizing computer use that minimally impacts the completion of the separate crime or tort, while continuing to punish acts that actually impact the attempt or completion of the underlying violation.[175] Additionally, a knowledge requirement would eliminate punishment for incidental computer use in relation to a crime or tort.[176] This new test, in full,

[163] 18 U.S.C. § 1030(a)(5)(A) (requires an individual to "knowingly" cause damage to a protected computer and is a base felony offense).

[164] *Taylor*, 142 S. Ct. at 2020.

[165] MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

[166] 18 U.S.C. § 1030(a)(5).

[167] *Morris*, 928 F.2d at 509-11.

[168] *Id.*

[169] *Id.*

[170] *Id.*

[171] 18 U.S.C. § 1030(c)(2)(B)(ii).

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *Id.*

[176] *Id.*

would require an individual to knowingly[177] use the information acquired through unauthorized access to a protected computer, in violation of § 1030(a)(2)(C), as "a substantial step . . . beyond mere preparation"[178] to advance the efforts of another crime or tort.[179] This test would allow courts to draw the necessary distinction between the issues illustrated by two GPS scenarios and eliminate the overbroad nature of the statute.[180] The next section focuses on applying this test to the GPS fact patterns.

IV. APPLYING THE CFAA AND *VAN BUREN* TO INCIDENTS INVOLVING MODERN TECHNOLOGY REQUIRES MORE SPECIFICITY

The CFAA and its felony enhancements, as currently understood, can potentially be applied too broadly.[181] After *Van Buren*, physical barriers, when active, can be considered as "gates up" because it expressly signifies the owner does not want strangers to access the device.[182] Subsequently, physical barriers serving as "gates" present the opportunity for § 1030(a)(2)(C) to merge with traditional trespass crimes.[183] Therefore, the "substantial furtherance test" is necessary to determine when that merger point or nexus between committing a physical trespass and a hacking violation[184] should be charged as two separate crimes[185] or when the computer use is insignificant to warrant CFAA violation and punishment.[186] This section will use hypothetical fact patterns to show the value of the Substantial Furtherance Test and its continued importance as technology continues to advance.[187]

[177] 18 U.S.C. § 1030(a)(5); *Morris*, 928 F.2d at 509-11.

[178] *Taylor*, 142 S. Ct. at 2020.

[179] 18 U.S.C. § 1030(c)(2)(B)(ii).

[180] Kerr, *supra* note 1, at 1561-67.

[181] *Id.*

[182] *Van Buren*, 141 S. Ct. at 1658-60.

[183] KERR, *supra* note 29, at 1-5; Van Buren, 141 S. Ct. at 1658-60.

[184] 18 U.S.C. § 1030(a)(2)(C) (gaining unauthorized access to a protected computer).

[185] This incident should be charged as a physical trespass crime and as a Section 1030(a)(2)(C) and 1030(c)(2)(B)(ii) felony enhancement hacking crime.

[186] Griffith, *supra* note 1, at 475-78 (The CFAA was intended to protect private information stored on computers, mostly financial statements and similar documents.); s*ee also* Ric Simmons, *The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime*, 84 GEO. WASH. L REV. 1703, 1706 (2016) (advocating for administrative review of CFAA issues to avoid broad application and unfair punishment for crimes not "deserving" of punishment); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1656, 1660-63 (2003) (Before Van Buren negated the issue, Kerr argued employer agreements serving as barriers for authorized access violated traditional criminal punishment concepts.).

[187] Griffith, *supra* note 1, at 475-78.

A. The Outdated Nature of the CFAA

The 1980s understanding of computer technology and the urgent desire to protect computers from cyber criminals are apparent through the text and background of the Computer Fraud and Abuse Act of 1986.[188] The statute was initially implemented to "criminalize only important federal interest computer crimes" and thus military computers and those of financial institutions were the primary concern.[189] Resultantly, changes throughout the years have focused on narrowing the statute to limit the term "authorized access."[190] However, legal scholar and professor Orin Kerr's fears of "vagueness" in this area are largely corrected by the decision in *Van Buren*.[191] Kerr was worried about the broad application of authorization because he was concerned about who could limit access to computers and who could be punished for it.[192] While the idea of terms of service violations being criminalized is troubling, the Supreme Court held in *Van Buren* that police department policies could not be used to criminalize the defendant's actions, thus correcting Kerr's fear.[193] While access authorization concerns have stabilized, future potential issues with the CFAA could arise as technology begins to merge crimes of the physical and cyber worlds.[194]

B. The "Other Criminal or Tortious Act:" Auto Theft

This Note will examine the need for the "substantial furtherance test" through the lens of car theft as the act of breaching the *Van Buren* "gate."[195] From 2019 to 2020, there was over a ten percent increase in the total number of motor vehicle thefts in the U.S.,[196] and from 2020 to 2021, there was an

[188] Kerr, *supra* note 1, at 1561-67; Griffith, *supra* note 1, at 475-78.

[189] Kerr, *supra* note 1, at 1561-67.

[190] *Id.*

[191] Kerr, *supra* note 1, at 1561-63 (Kerr's main concerns were over two cases in which "the government argued that violations of Terms of Service (TOS) render access to a computer unauthorized" and "an employee who accesses an employer's computer with illicit motives to hurt the employer accesses that computer without authorization," respectively).

[192] *Id.*

[193] *See* Van Buren, 141 S. Ct. at 1660-63.

[194] Griffith, *supra* note 1, at 472-73 (Griffith notes that the Department of Justice and William G. Petty, "a representative of the National District Attorney's Association," both, "recommended the adoption of fraud language patterned after existing federal mail and wire fraud statutes because such legislation would be flexible enough to withstand advances in technology").

[195] *Van Buren*, 141 S. Ct. at 1658-59.

[196] Maggie Davis, *Vehicle Theft Statistics: Most Stolen Cars & Bikes by State*, VALUEPENGUIN (May 3, 2022 insert timestamp), https://www.valuepenguin.com/motor-vehicle-theft-statistics#:~:text=Since%201991%2C%20the%20overall%20level,1991%20to%20727%2C921%20in%202020 [https://perma.cc/9H9T-JWAJ].

additional six percent increase.[197] The total number of motor vehicle thefts in the U.S. at the end of 2021 was over 930,000.[198]

As motor vehicle thefts continue to rise, technology continues to improve within cars on the road today, but not only are security measures still being circumvented, but accessories inside vehicles are more valuable and useful to those stealing cars.[199] The concept of a "smart car" or a technologically advanced car is becoming more and more affordable at lower price points for consumers.[200] These services include Bluetooth capabilities, satellite radio access, and subscription-based navigation options.[201] As society becomes more reliant on the technology in automobiles, the necessity for their security and thus the security of the owner's personal data becomes increasingly important.[202]

C. Hypotheticals and Fact Pattern

The following hypotheticals illustrate the overbroad nature and potential for misapplication of the felony enhancements for § 1030(a)(2)(C), after the Supreme Court's decision in *Van Buren*.[203] The first hypothetical will illustrate how insignificant use of technology could still be considered a § 1030(a)(2)(C) violation, eligible for felony enhancement, and why the charging decision would be contradictory to the purposes of the CFAA and criminal punishment in general.[204] The second hypothetical will illustrate, using the same base crime of car theft, how the same type of access can be used to significantly further other criminal actions and why it is appropriate to apply the felony enhancements, to preserve the purposes of the CFAA and protect citizen privacy interests, as well as public safety and security of information.[205] These two extremes show how the proposed Substantial

[197] NCIB, *NCIB Report Finds Vehicle Thefts Continue to Skyrocket in Many Areas of U.S.*, NAT'L INS. CRIME BUREAU (Sept. 1, 2022), https://www.nicb.org/news/news-releases/nicb-report-finds-vehicle-thefts-continue-skyrocket-many-areas-us [https://perma.cc/YTN7-UFEY].

[198] *Id.*

[199] Ironpaper, *Smart Car Statistics – The Increasingly Digital Experience of the Connected Vehicle*, IRONPAPER (July 18, 2018), https://www.ironpaper.com/webintel/articles/smart-car-statistics-the-increasingly-digital-experience-of-the-connected-vehicle [https://perma.cc/BV4B-6QRY]; *see also* Montaser N. Ramadan, et. al., *Intelligent Anti-Theft and Tracking System for Automobiles*, 2 INTERNATIONAL JOURNAL OF MACHINE LEARNING AND COMPUTING 88 (2012); FORD MOTOR COMPANY, *The Family of Ford Cars*, (last visited Apr. 9, 2023), https://www.ford.com/new-cars/?gnav=footer-all-vehicles [https://perma.cc/7QQD-ZNUK].

[200] Ironpaper, *supra* note 199.

[201] *Id.* (In 2014, it was estimated by CNBC that eighty-six percent of new cars included Bluetooth capabilities.).

[202] YONG GOO KANG, ET. AL., AUTOMOBILE THEFT DETECTION BY CLUSTERING OWNER DRIVER DATA, 1, 2 (2019).

[203] *Van Buren*, 141 S. Ct. at 1658-59.

[204] *See also* Griffith, *supra* note 1, at 475-78; Simmons, *supra* note 186, at 1716; Kerr, *supra* note 186, at 1656, 1660-63.

[205] *See also* Griffith, *supra* note 1, at 475-78; Simmons, *supra* note 186, at 1716; Kerr, *supra* note 186, at 1656, 1660-63.

Furtherance Test weeds out frivolous prosecution while protecting public safety and privacy.[206]

1. Hypothetical 1: The "Chop Shop"

One morning, in Arlington, Virginia, John Doe spots a late model Ford sedan on the street while walking to work and notes he has never seen the car parked there before.[207] Doe goes to work and leaves, spotting the same car on the street. The next day, he walks past the same car in the same spot and notices the same coffee cup left in the cup holder. This pattern continues for four days until finally, Doe decides the car is abandoned and ripe for taking. During his lunch break, Doe calls a friend who owns an automobile repair shop and is known to accept stolen goods from the street. Doe tells his friend about the car, and the two agree on a price if Doe can get the car to the body shop before it opens the next morning.

Waiting until the dark of night, Doe approaches the car and looks around to see if anyone is watching him. He manages to break into the parked car, surpassing the lock on the car door. Doe then hot-wires the car to start it and drives away. This act is grand larceny, punishable in Virginia by up to twenty years in prison.[208]

Immediately after Doe starts the car, the vehicle's computer system starts, and the dashboard is accessible.[209] On the dashboard, Doe notices a GPS application and decides to use the navigation system to direct him to the body shop,[210] or "chop shop," where the car will be stripped and sold for parts. He knew the address but decided it would be more convenient to use the GPS. He types in the address, and the car's navigation system takes him to the shop.[211] Once at his friend's chop shop, Doe receives his reward and leaves promptly. He is arrested a week later via security camera footage from a nearby convenience store. The chop shop is searched pursuant to a warrant and parts of the car are still found in the shop.

Doe decides it is in his best interest to plead guilty, given the overwhelming evidence against him. When entering his confession, Doe spares no details and tells police about the car's dashboard, using the navigation application and driving quickly to the chop shop. Doe is charged with one count of grand larceny with the intent to sell the stolen good(s).[212] This count is punishable by up to twenty years in prison.[213]

In examining the facts more closely, a young prosecutor called Jane Smith, looking at the case holistically, remembers the recent holding in *Van*

[206] Kerr, *supra* note 186, at 1656, 1660-63.

[207] *The Family of Ford Cars*, *supra* note 199.

[208] VA. CODE ANN. § 18.2-95 (LEXIS 2022) (The car is presumably worth more than $2,500, thus satisfying the requirements of the statute.).

[209] *Connected Navigation*, FORD MOTOR COMPANY: TECHNOLOGY (Apr. 2023), https://www.ford.com/technology/connected-navigation/?gnav=footer-connetedNav [https://perma.cc/88MD-KRJF].

[210] *Id.*

[211] *Id.*

[212] VA. CODE ANN. §§ 18.2- 95 and 108.01 (LEXIS 2022).

[213] *Id.*

Buren.[214] She remembers Arlington County's 2021 decrease in motor vehicle-related crimes and the Commonwealth Attorney's desire to continue to be diligent regarding car thefts to avoid Arlington falling in with the rising numbers of the rest of the nation.[215] She decides to reach out to the United States Attorney's Office for the Eastern District of Virginia, to learn more about the issue. The U.S. Attorney's Office decides to take the case on and investigate what charges they can bring.

Examining this situation involves looking at provisions 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii).[216] The first step in the analysis is whether the car or its navigation system is a computer, under the statute.[217] As discussed above, a computer is any machine or device with data processing or data storage capabilities.[218]

In examining the car's dashboard computer functionality,[219] the use of the navigation system is the main concern for the purposes of this Note. Accordingly, onboard subscription-based navigation applications, accessible through the dashboard, are most likely "computers" under § 1030(e)(1) because they process and store location data via a visual display to show the driver maps and step-by-step directions to their desired location.[220] Given the broad holdings of the courts' opinions in *Mitra* and *Kramer*, and that this is the general interpretation of most courts, an onboard GPS meets the definition of a computer.[221]

[214] *Van Buren*, 141 S. Ct. at 1658-63.

[215] Davis, *supra* note 196; Jo DeVoe, *Commonwealth's Attorney Touts Falling Rates of Carjackings, Car Thefts and Homicides in 2021*, ARLNOW (Jan. 6, 2022, 3:55 PM), https://www.arlnow.com/2022/01/06/commonwealths-attorney-touts-falling-rates-of-carjackings-car-thefts-and-homicides-in-2021/ [https://perma.cc/AT3K-842F].

[216] 18 U.S.C. § 1030(a)(2)(C) (A violation of this section requires anyone who breaches authorized access or exceeds authorized access to obtain information from a protected computer.); *see also* 18 U.S.C. 1030(c)(2)(B)(ii) (This provision includes a felony enhancement for violations of (a)(2)(C), the most relevant of which is when the breach of access was in furtherance of another crime or tort.).

[217] 18 U.S.C. § 1030(e)(1).

[218] 18 U.S.C. § 1030(e)(1); *Mitra*, 405 F.3d at 495; *Kramer*, 631 F.3d at 903-05; KERR, *supra* note 29, at 82-83.

[219] It is debatable whether a car is a computer or protected computer in and of itself because it operates as a mechanical apparatus, injecting fuel to function, but as cars become more dependent on Electronic Control Units to operate, they could be considered computers. However, "car hacking" or examining cars as protected computers is outside of the scope of this Note. Rick Cotta, *What Is an ECU?*, CARS.COM (Feb. 27, 2022), https://www.cars.com/articles/what-is-an-ecu-447580/ [https://perma.cc/A7FF-8JNX] (cars operate on Electronic Control Units or Engine Control Units (ECU) which means all of the car's processing functions from the braking, to fuel pumping, to the dashboard computer, are operational once the car's engine is ignited); *see generally* Bryson R. Payne, *Car Hacking: Accessing and Exploiting the CAN Bus Protocol*, 1 J. OF CYBERSECURITY EDUC., RSCH. AND PRAC., 2-5 (2019); *see generally* MARK BACCHUS, ET. AL., THE INSIGHTS INTO CAR HACKING (2014), https://api.semanticscholar.org/CorpusID:18719071 [https://perma.cc/EL7A-HZPJ].

[220] *GPS Applications*, *supra* note 5 (GPS systems are operated by the U.S. government and use satellite data, transmitted to the user to provide location information.).

[221] 18 U.S.C. § 1030(e)(1); *Mitra*, 405 F.3d at 495; *Kramer*, 631 F.3d at 903; KERR, *supra* note 29, at 82-83.

The next step in the process is that the government must show that the GPS is a protected computer.[222] The most critical factor for a car's GPS to be a "protected computer" is that the system relies on the global transmission of data.[223] According to GPS.gov, a U.S. government website run by the U.S. Space Force, GPS systems are connected to an international network "like the Internet" and "[are] an essential element of the global information infrastructure."[224] Subsequently, a GPS connecting to an international data network likely yields a similar result, in terms of connection to interstate commerce, that a laptop connecting to the Internet does, as per the reasoning in *Fowler, Yücel*, and *Hornaday*.[225] Thus, if GPS devices function like other computers, and their network impacts interstate commerce, they are likely to meet the low bar for a "protected computer."[226] Therefore, the last step is connecting a GPS device to interstate commerce or communication.[227] While the Supreme Court has not directly examined this issue, courts at the appellate and district level have found GPS devices to be included as instrumentalities of interstate commerce, specifically within the context of kidnapping statutes.[228] Additionally, GPS connects automobiles to a network that extends through state and national borders, thus heavily suggesting regulation under interstate commerce.[229]

After establishing the car's GPS as a protected computer, the government would next be required to prove that Doe breached authorized access or, in the eyes of the Court in *Van Buren*, breached clear gates that were up to prevent Doe from accessing the device.[230] After surpassing the car's locked doors and hot wiring the engine, Doe can then access whatever information is available on the dashboard.[231] The owner, through locking the car, clearly indicated they did not want another person to drive it or presumably use any of the car's applications or accessories.[232] This indication would likely satisfy the *Van Buren* standard because the owner established a physical barrier and their desire to not have others use their vehicle.[233]

Doe then continued to breach the security of the GPS or "protected computer" by starting the ignition.[234] The car's dashboard computer, with

[222] 18 U.S.C. § 1030(a)(2)(C) and (e)(2)(A-B).

[223] *GPS Applications*, *supra* note 5.

[224] *Id.*

[225] *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8 (citing *Walters*, 182 Fed. App'x at 945; *Hornaday*, 392 F.3d at 1311; *Yücel*, 97 F. Supp. 3d at 419).

[226] 18 U.S.C. § 1030(e)(2)(B).

[227] *Id.*

[228] 18 U.S.C.S. § 1201(a)(1); United States v. Morgan, 748 F.3d 1024, 1032 (10th Cir. 2014); United States v. Muller, No. 2:15-cr-0205, 2018 U.S. Dist. LEXIS 120186, (E.D. Cal. July 18, 2018).

[229] *Fowler*, 2010 U.S. Dist. LEXIS at *4-*8; (citing *Walters*, 182 Fed. App'x at 945; *Hornaday*, 392 F.3d at 1311); *see also Yücel*, 97 F. Supp. 3d at 419.

[230] *Van Buren*, 141 S. Ct. at 1658-60.

[231] 18 U.S.C. § 1030(a)(2)(C) (the statute requires the violator to "[obtain] information from any protected computer" and in this case, the information Doe obtained was the directions to the "chop shop" after plugging in the address).

[232] *Van Buren*, 141 S. Ct. at 1660-63.

[233] *Id.*

[234] *Id.*

access to several applications, starts when the engine is ignited.[235] With the ignition of the car directly causing the activation of the computer, the criminal trespass now merges with the barrier standard of *Van Buren*.[236] By breaking the locks on the car doors and starting the car's ignition, Doe breached authorized access to a protected computer.[237] Ultimately, Doe breached two gates: the door locks and protections against the ignition sequence.[238]

Lastly, to activate the felony enhancements under § 1030(c)(2)(B)(ii), the government must prove Doe furthered an underlying crime or tort.[239] As in *Steele*, where the defendant used his former employer's computers to steal valuable government contract information, thus committing grand larceny,[240] in this case, Doe used the GPS computer to pull up turn-by-turn directions to the "chop shop" and sell the stolen car, thus using a protected computer in "furtherance" of committing grand larceny with intent to sell.[241] Therefore, Doe's actions meet all the requirements of a § 1030(a)(2)(C) violation, with a felony enhancement under § 1030(c)(2)(B)(ii).[242]

The problem this hypothetical creates for society is that Doe can now be punished for frivolous use of technology and for an act that simply should not be considered illegal.[243] Substantively, Doe did not do anything more than he otherwise would have if he did not have a navigation system. Doe knew the address but simply decided it would be faster to plug in the address and get directions. If he simply drove to the shop or used his own smartphone for directions, he would not face an additional five years in prison for using a car GPS.[244] Additionally, in *Van Buren*, the Supreme Court refused to accept prosecutorial discretion as the only safeguard against frivolous or overbroad charging of the statute and chose to clarify the statute and legal standard through its holding.[245]

The potential for this charge to occur is unjust. The CFAA was intended to protect financial records and has since been developed to protect the broad privacy interest of citizens.[246] Additionally, almost twenty years before the issue was decided in *Van Buren*, Orin Kerr warned of the overbroad nature of § 1030(a)(2) leading to written agreements serving as barriers to authorized access and for individuals to be criminally liable for essentially breaching

[235] FORD, *supra* note 209.

[236] Van Buren, 141 S. Ct. at 1660-63.

[237] *Id.*

[238] *Id.*

[239] *Steele*, 595 F. App'x at 216.

[240] VA. CODE ANN. §§ 18.2- 95 AND 108.01 (LEXIS 2022); Steele, 595 F. App'x, at 216.

[241] 18 U.S.C. § 1030(c)(2)(B)(ii).

[242] *See* H. MARSHALL JARRETT ET. AL, PROSECUTING COMPUTER CRIMES 20 (Office of Legal Education Executive Office for United States Attorneys: Computer Crime and Intellectual Property Section Criminal Division 2017).

[243] Doe is being punished for violation of 18 U.S.C. § 1030(a)(2)(C), but common knowledge suggests it is not illegal to use a GPS as an isolated incident.

[244] 18 U.S.C. § 1030(c)(2)(B)(ii).

[245] *Van Buren*, 141 S. Ct. at 1662 (The Court declared the need for statutory clarity through legislative action or jurisprudence by stating, "[t]he Government's approach would inject arbitrariness into the assessment of criminal liability.").

[246] Griffith, *supra* note 1, at 475-78 (The CFAA has since developed into protecting more privacy interests than just financial documents.).

company policies.[247] Kerr argued that such a policy contradicted Congress's purpose to "limit the scope of criminal liability to conduct that satisfies both utilitarian and retributive goals."[248] Such goals "include deterrence, rehabilitation, and incapacitation."[249] Similarly, if unchecked, another overbroad provision within the CFAA could lead to punishment that contradicts the purposes of the act altogether, as outlined by Kerr.[250] The frivolous use of technology during a crime, such as typing a known address into a dashboard GPS, is not one society should be looking to deter with a potential five-year prison sentence.[251] In fact, GPS use is becoming more and more prevalent, so it seems absurd to criminalize such insignificant use during the theft.[252] Furthermore, the use of a GPS computer does not warrant rehabilitation because it is a legal act, if isolated, and a necessity in many occupations.[253] Doe's need for rehabilitation in this instance stems solely from the auto theft.[254] For that same reason, incarceration is unnecessary because the use of GPS harms no one.[255]

The possibility of charging Doe with a felony hacking violation for this GPS use illustrates the larger problem that these CFAA felony enhancements are much too broad.[256] The possibility of being charged for insignificant use of technology during a crime or tort must be eliminated by revising the statute to only apply to the knowing use of information acquired from a "protected computer" that substantially excels another criminal or tortious act.[257] Under the "Substantial Furtherance Test," the federal government would be unable to charge Doe with a § 1030(a)(2)(C) felony violation because Doe did not use the GPS navigation information to take a significant effort or "substantial step" to completing his sale of stolen goods.[258] He knew the "chop shop" and knew where it was. The GPS did not aid him in selling the car in any significant way; therefore, his use of the computer was not a knowing[259] act in "[substantial][260] furtherance of any criminal or tortious act."[261]

2. Hypothetical 2: "Closer to Home"

While the substantial furtherance test absolves Doe of felony liability for his actions in the first hypothetical, it does not absolve him from using the same device to attempt or commit a crime he otherwise would not have been

[247] Kerr, *supra* note 186, at 1656, 1660-63.
[248] *Id.* at 1656.
[249] *Id.* at 1656, 1660-63.
[250] *Id.*
[251] *Id.*
[252] Kerr, *supra* note 186 at 1656, 1660-63; *GPS Applications*, *supra* note 5.
[253] Kerr, *supra* note 186 at 1656, 1660-63.
[254] *Id.*
[255] *Id.*
[256] 18 U.S.C. § 1030(c)(2)(B)(ii).
[257] 18 U.S.C. § 1030(a)(2)(C); *Morris*, 928 F.2d at 509-11; *Taylor*, 142 S. Ct. at 2020.
[258] 18 U.S.C. § 1030(c)(2)(B)(ii).
[259] 18 U.S.C. § 1030(a)(5)(A); *Morris*, 928 F. 2d at 509-11.
[260] *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).
[261] 18 U.S.C. § 1030(c)(2)(B)(ii).

able to do without the information obtained from the GPS. In this second hypothetical, assume the same individual (John Doe) breaks into the same car under the same circumstances. However, this time, the car is a recently-made Ford model with a "Connected Navigation" subscription, and Doe notices a preset saved location in the owner's navigation app.[262] Doe then clicks on the location, believing it to be the owner's home, and drives to the house to see if there might be some added value to his escapade.[263] Doe assumes that since the car was relatively nice, the house is worth exploring as well. He uses the navigation to get back to the owner's house and sees no signs of alarms, dogs, or advanced home security.[264] From this point, Doe could cause considerable damage. He could break in and steal items or, far worse, if any individual is inside the house. For the sake of clarity, assume Doe breaks into the house, steals anything he can grab quickly, and then gets back in the car, selling his stolen goods to the chop shop owner, along with the car.

A week later, Doe is caught under the same circumstances as in the first hypothetical. He is charged this time with two counts of grand larceny with the intent to sell the stolen good(s) for the stolen car and the items he stole from the owner's house.[265] Both of these counts are punishable by up to twenty years in prison.[266] This time, the Commonwealth's Attorney is disturbed by the access to private information and that information led John Doe to the home of a family, who happened to be out of town.[267] Doe may or may not have been violent in that situation, but the potential is concerning, nonetheless. ACA Smith takes the same procedural path to the U.S. Attorney's Office, which once again decides to take the case on and investigate what charges they can bring.

Under the same analysis as the first hypothetical, the car's navigation system is a protected computer. Doe breached authorized access, and he obtained information to advance another crime or tort.[268] However, Doe's actions regarding the house appear to be much more extreme whether he intended to break into the car to obtain the physical address or not.[269] Under the proposed Substantial Furtherance Test, the government is required to prove that Doe used the information he obtained from the car's navigation computer[270] to knowingly[271] and substantially[272] "[further] any criminal or

[262] FORD, *supra* note 209.

[263] *Id.*

[264] *Id.*

[265] VA. CODE ANN. §§ 18.2- 95 and 108.01 (LEXIS 2022).

[266] *Id.*

[267] *Commonwealth Attorney Parisa Dehghani-Tafti*, ARLINGTON COUNTY VIRGINIA (2023), https://www.arlingtonva.us/Government/Departments/Courts/Commonwealth-Attorney/Meet-Parisa [https://perma.cc/9K8T-SVNT].

[268] *Van Buren*, 141 S. Ct. at 1658-60; 18 U.S.C. § 1030(c)(2)(B)(ii).

[269] 18 U.S.C. § 1030(a)(2); *Morris*, 928 F.2d at 506 (This case mostly deals with issues involving 1030(a)(5) issues with intent to cause damage, but it does clarify that the offender must "intentionally" breach access to the computer.).

[270] 18 U.S.C. § 1030(a)(2)(C).

[271] 18 U.S.C. § 1030(a)(5)(A); *Morris*, 928 F.2d at 509-11.

[272] *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

tortious act."[273] In this case, the information Doe received from the GPS was the car owner's home address. He would not have known that address without gaining access to the GPS by breaking through the car's locked doors and hot-wiring the ignition. He then used the information he obtained to go to the owner's home and burglarize or commit other heinous crimes. Doe knew, or reasonably should have known,[274] that an address labeled "Home" would be the owner's home address. He then used the information he received from the GPS to complete a "substantial step" in contributing to his intended crime of burglary by using the directions to go to the owner's house.[275] Therefore, under the Substantial Furtherance Test, and prior understandings of § 1030(a)(2)(C)'s felony enhancements, Doe could be charged and convicted of a hacking felony under the CFAA.[276]

Doe's violative use of technology to commit crimes of the physical world is exactly the type of act Congress was concerned with regulating when drafting began for the CFAA in the early 1980s because it violates someone else's privacy interests and puts personal data at risk.[277] It, therefore, satisfies the needs for "deterrence, rehabilitation, and incapacitation.[278] The critical difference between the two hypotheticals is that in the second one, Doe used someone else's computer to obtain information about them and then used that information to commit another crime.[279] In other words, Doe would not have gotten the owner's address without breaking into the car and gaining access to the GPS.[280] He then used that access to complete a crime he could have never even attempted without seeing the home address of the car owner saved in the GPS computer.[281] Conversely, in the first hypothetical, Doe knew about the chop shop already, and he knew the address. Even if the facts changed and he did not know the chop shop address, he already had a deal in place to sell the car and could presumably contact the buyer at any point. Despite the GPS making the process more convenient, Doe's attempted or completed effort to sell stolen goods is not initiated by the information displayed through the car's GPS, and the GPS use is frivolous in helping the process of furthering the separate crime.[282] In summary, the main difference is Doe obtained new and vital information from his breach of authorized access in the second hypothetical by finding someone's address.[283] He then used that new and vital

[273] 18 U.S.C. § 1030(c)(2)(B)(ii).

[274] 18 U.S.C § 1030(a)(5)(A); *Morris*, 928 F.2d at 509-11 (implied from the intended functionality of saved GPS locations labeled home).

[275] *Taylor*, 142 S. Ct. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

[276] 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii).

[277] Jarrett, *supra* note 242, at 19-20; s*ee generally* STEPHANIE RICKER SCHULTE, "THE WARGAMES SCENARIO" REGULATING TEENAGERS AND TEENAGED TECHNOLOGY 1-5 (1980–1984) (2008).

[278] Kerr, *supra* note 186, at 1656, 1660-63.

[279] *See* 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii); *Van Buren*, 141 S. Ct. at 1660-1663 (2021).

[280] FORD, *supra* note 209.

[281] *Id.*

[282] *See* 18 U.S.C. § 1030(a)(2)(C), § 1030(c)(2)(B)(ii); VA. CODE ANN. § 18.2-91 (LEXIS 2022); *Van Buren*, 141 S. Ct. at 1658-59.

[283] *See* 18 U.S.C. § 1030(a)(2)(C); Jarrett, *supra* note 242, at 19-20; s*ee generally* SCHULTE, *supra* note 277, at 1-5.

information to complete another crime.[284] Society does not want individuals thinking they can break into cars, start them, and obtain personal information or location information to then break into someone's home, steal property, or cause physical injury.[285] Simply put, in the first hypothetical, Doe is not abusing the GPS, but in the second hypothetical, he is because he knowingly violated public trust.[286] The Substantial Furtherance Test still satisfies the goals of criminal punishment in the context of the CFAA because it limits punishment to acts that abuse technology or critical information obtained via unauthorized use while excluding the use of technology that is trivial in relation to a separate crime or tort.[287] Lastly, the test ensures the CFAA can more accurately regulate the potentially serious and dangerous offenses described in the second hypothetical, while not punishing simplistic uses of technology that do not aid in additional crimes as described in the first hypothetical.[288]

D. Looking Beyond the Limited Lens of GPS Devices

Simplistic GPS computers are much rarer today as people rely more and more on their smartphones for navigation.[289] Furthermore, most new cars, including newer Ford models, as well as Tesla cars, include a tablet-like device on the dashboard that is connected to the Internet and allows the driver to use various applications, similar to a smartphone.[290] These devices are connected to the Internet, and process and store data, thus making them protected computers.[291] Take the same facts as above, but imagine all of the personal identifying information contained on a smartphone or in a car's tablet.[292] The violations of privacy and potential "[furthered] criminal or tortious acts"[293] become much more vast. This dilemma that advancing technology creates increases the need for the Substantial Furtherance Test because the CFAA must be narrowed to accurately regulate computer crimes

[284] *See Van Buren*, 141 S. Ct. at 1658-59.

[285] *Id.*

[286] Kerr, *supra* note 186, at 1660-63.

[287] 18 U.S.C. § 1030(c)(2)(B)(ii); Griffith, *supra* note 186, at 476; Simmons, *supra* note 185, at 1716; Kerr, *supra* note 186, at 1656, 1660-63.

[288] Kerr, *supra* note 186, at 1662.

[289] *See* Amy He, *People Continue to Rely on Maps and Navigational Apps,* INSIDER INTEL. (July 18, 2019), https://www.insiderintelligence.com/content/people-continue-to-rely-on-maps-and-navigational-apps-emarketer-forecasts-show [https://perma.cc/Z4HY-SVD2].

[290] FORD, *supra* note 209; *Dashcam, Sentry, and Security*, TESLA https://www.tesla.com/ownersmanual/models/en_us/GUID-49096E34-97D2-4182-9414-2F7F4E88EE79.html [https://perma.cc/36NC-78RE] (last visited Month Day, 2023).

[291] FORD, *supra* note 209; *Dashcam, Sentry, and Security*, TESLA, *supra* note 290, (2023) https://www.tesla.com/ownersmanual/models/en_us/GUID-49096E34-97D2-4182-9414-2F7F4E88EE79.html [https://perma.cc/36NC-78RE]; *see Fordpass,* FORD MOTOR CO., https://www.ford.com/support/category/fordpass/fordpass-connect-wifi-hotspot/#:~:text=Download%20the%20FordPass%20App%20d,find%20the%20Vehicle%20Hotspot%20icon. [https://perma.cc/2Y22-KXLH] (last visited Nov. 6, 2023).

[292] *See Connect iPhone to CarPlay*, APPLE, https://support.apple.com/guide/iphone/connect-to-carplay-iph6860e6b53/ios [https://perma.cc/XR4Z-ZDD3] (last visited Nov. 22, 2022).

[293] 18 U.S.C. § 1030(c)(2)(B)(ii).

as they continue to merge with traditional crimes of the physical world.[294] The Test limits the felony enhancement to the use of information obtained from a protected computer[295] to knowingly[296] and substantially[297] "[further] any criminal or tortious act,"[298] thus not criminalizing computer use that is trivial to the separate crime or tort while continuing to punish violations of privacy and use of technology that directly aid the attempt or completion of the separate crime or tort,[299] in accordance with Congress's original intentions for the CFAA.[300]

V. CONCLUSION

The CFAA of 1986 was an admirable attempt at predicting and regulating the unimaginable modern world of technology based on the knowledge and understanding of the time period.[301] Through the benefit of hindsight however, it is clear Congress did not account for more complicated hacking issues such as GPS systems in cars to be potentially interpreted as computers, for the Supreme Court to simplify the language of § 1030(a)(2)(C) to the point of establishing a barrier for access to protected computers, and for the connection between a car door lock and the ignition system powering on a computer to merge a traditional crime of the physical world with federally regulated cybercrimes.[302] The decision in *Van Buren* brings with it the potential for abuse of prosecutorial discretion without focusing on protecting specific cyberspace targets, such as automobiles, especially as cars become more technologically advanced and integrated into society.[303]

This Note shows the necessity for modernizing the felony enhancement requirements for § 1030(a)(2)(C) violations to ensure individuals are not arbitrarily charged and punished for acts not otherwise deemed criminal while establishing a precedent for future protections of technologically advanced cars and the personal data they store.[304] The statutory language must be targeted at computer use that substantially furthers or is a critical component of an underlying crime or tort or when the personal information obtained from the protected computer is used directly to advance that criminal or tortious

[294] Kerr, *supra* note 186, at 1656, 1660-63.

[295] 18 U.S.C. § 1030(a)(2)(C).

[296] 18 U.S.C. § 1030(a)(5)(A); *Morris*, 928 F.2d at 509-11.

[297] *Taylor*, 142 S. Ct,. at 2020; *see also Resendiz-Ponce*, 549 U.S. at 107; MODEL PENAL CODE § 5.01 CRIMINAL ATTEMPT (AM. L. INST. 2023).

[298] 18 U.S.C. § 1030(c)(2)(B)(ii).

[299] *Id.*

[300] *See* Kerr, *supra* note 186, at 1656, 1660-63.

[301] *See generally* Kerr, *supra* note 1 *see also* Griffith, *supra* note 1.

[302] 18 U.S.C. § 1030(a)(2)(C); *Van Buren*, 141 S. Ct. at 1658-1662; KERR, *supra* note 29.

[303] *Van Buren*, 141 S. Ct. at 1658-59; Ironpaper, *supra* note 198, (July 18, 2018), https://www.ironpaper.com/webintel/articles/smart-car-statistics-the-increasingly-digital-experience-of-the-connected-vehicle [https://perma.cc/BV4B-6QRY]; s*ee generally* Kerr, *supra* note 1, at 1561-67.

[304] *Van Buren*, 141 S. Ct. at 1658-59; Ironpaper, *supra* note 198, (July 18, 2018), https://www.ironpaper.com/webintel/articles/smart-car-statistics-the-increasingly-digital-experience-of-the-connected-vehicle [https://perma.cc/BV4B-6QRY]; s*ee generally* Kerr, *supra* note 1, at 1561-67.

end.[305] In other words, simple access in the process of committing a crime or tort, such as John Doe using the navigation system to get to the chop shop, should not be a federal felony punishable by up to five years, even if Doe stole the car.[306] However, using personal information stored on that navigation system, such as a physical address, for criminal gain should be deterred, and such punishment aligns with the original purpose of the CFAA.[307]

[305] 18 U.S.C. §§1030(a)(2)(C) and (c)(2)(B)(ii).

[306] *See generally* Kerr, *supra* note 1, at 1561-67.

[307] *Id.*