A Proposed Amendment to 18 U.S.C. § 1030—The Problem of Employee Theft

*Michael L. Levy**

Abstract

The problem of what constitutes "unauthorized access" and "access in excess of authorization" to a protected computer under 18 U.S.C. § 1030 is proving to be intractable. At the same time, businesses are experiencing significant losses, as disloyal employees, on their way to new employment, take data that they think will be useful in their new jobs. Rather than argue for another meaning for "authorization" either in the courts or Congress, this Article proposes sidestepping the issue and solving the disloyal employee problem with legislation that deals directly with the problem—the employee's access to the employer's computer with the intent to steal information.

Table of Contents

Introduction

Businesses throughout the country are plagued with the problem of disloyal employees, who steal company data from a computer on their way out the door to a new job. Unfortunately, the current statutory scheme for federal prosecutions of computer crimes may present barriers to prosecuting these acts as unauthorized access to a pro-

* Chief of the Computer Crimes Section in the United States Attorney's Office for the Eastern District of Pennsylvania. The ideas, views, and opinions expressed are those of the Author and are not those of the United States Department of Justice.

tected computer, depending upon where the offense occurred. Courts are split on whether § 1030(a)(2) of the Computer Fraud and Abuse Act ("CFAA")[1] covers these data thefts, and, as this Article demonstrates, there may be no federal laws that cover this conduct. This Article posits a typical scenario, reviews the state of the law, and suggests that a combination of statutory drafting problems and a lack of agreement on norms of computer use make this problem one that requires a new statutory solution. Although there have been proposals to amend § 1030 to define "authorization" to cover some of these scenarios, most of the proposals are either inadequate or confusing. This Article proposes to abandon efforts to deal with the authorization question and to focus on what truly concerns the victim—employees accessing computers with the intent to take information that the victim values.

Part I sets forth a common, hypothetical scenario and then shows that courts have applied the CFAA in vastly different ways in similar situations. Part II evaluates the courts' different types of application and then shows that possibilities for reform under currently existing legislation and under currently considered legislation are inadequate. Finally, Part III sets forth a proposed amendment to the CFAA and analyzes how that proposal successfully remedies some of the shortcomings that currently exist and improves the law in this area.

I. The Problem and Court Interpretations

A. Scenario

This scenario illustrates the problem.[2] Assume that you are an attorney in Aiken, South Carolina. One morning you get a call from a business client you have represented for years. She informs you that an employee, who worked for the company for five years, left last month to work for a new business. When she recently checked the website of that new business, she saw a number of things that led her to believe that the former employee had taken proprietary information from her company's computers. She tells you that she had her Information Technology staff review the logs, and they reported to her that in the month before this employee left, he had accessed the network from his home in Augusta, Georgia numerous times at night. A

1 18 U.S.C. § 1030(a)(2) (2012).

2 This scenario is based upon calls the Federal Bureau of Investigation and the Author receive several times per year, reporting employee data theft.

check of the logs showed that he had downloaded a number of critical files containing proprietary information.

You immediately pull the file that you have for this client, and true to your recollection, you had already created a set of policies and announcements to be given to employees. The policies told employees that they were only granted access to the network for the benefit of the employer, that the taking or using of company data for any other purpose was forbidden, that they had no expectation of privacy in anything that they did on the network, and that the company would prosecute those who violated these policies. You call your client back to determine if these notices had been given to the employee in question. About an hour later, your client calls to tell you that the login banner (for both in-office and remote access) informed employees of this policy, and that once each year a paper copy of the policy was given to the employee and he signed a document acknowledging receipt.

Armed with these facts, you call the U.S. Attorney's Office in South Carolina to talk to a prosecutor. Based upon your quick research, it seems to you that the employee has violated the CFAA, 18 U.S.C. § 1030(a)(2). The now-former employee has made unauthorized access to the company's computers and, as a result, has obtained information. After hearing your facts, the Assistant U.S. Attorney informs you that her office cannot prosecute the case, because the law of the Fourth Circuit holds that, if the employee was authorized to access the computer and the information, it does not matter what he did with the information later. Because the person was still employed, he was authorized. The Assistant U.S. Attorney, however, tells you that all is not lost. Because the perpetrator lived in Augusta, Georgia, there is a good chance that the case can be prosecuted there. The Eleventh Circuit has a different view. She gives you the name of an Assistant in the U.S. Attorney's office in Augusta. That Assistant U.S. Attorney, after hearing your facts, says that the case is prosecutable, and opens an investigation.

You are puzzled that a difference of about thirty miles between the business and the residence of the former employee can lead to such a different result for the same federal statute. You are a practicing lawyer and you want favorable results for your clients. Procedure, while interesting, is less important than outcome. If the U.S. Attorney's Office for the Southern District of Georgia can help you, you will take the help.

B. How Did We Get Here?

Congress passed the CFAA in 1984.[3] In its current formulation, 18 U.S.C. § 1030(a)(2) provides:

> Whoever— . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer[ ] [is guilty of an offense].[4]

In our hypothetical scenario, subsection (C) might apply because a "protected computer" is one "which is used in or affecting interstate or foreign commerce or communication."[5] Because the company's computers permitted remote access, they were connected to the internet. As such, they were used "in or affecting interstate or foreign commerce."[6]

The issue in the case turns on the words "unauthorized access" or "exceeds authorized access." Congress did not define "authorized access,"[7] but did define "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[8]

---

3 Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. 98-473, 98 Stat. 2190 (1984) (codified as amended at 18 U.S.C. § 1030 (2012)).

4 18 U.S.C. § 1030(a)(2).

5 *Id.* § 1030(e)(2)(B).

6 *Id.* In its current form, the offense is a misdemeanor. *See* 18 U.S.C. § 1030(c)(2)(A). The offense becomes a felony carrying a term of up to five years imprisonment if the government proves one of the following additional elements:

> (i) the offense was committed for purposes of commercial advantage or private financial gain;
>
> (ii) the offense 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; or
>
> (spn) the value of the information obtained exceeds $5,000.

18 U.S.C. § 1030(c)(2)(B).

7 *See generally* 18 U.S.C. § 1030.

8 *Id.* § 1030(e)(6).

There are seven significant cases in the courts of appeals on this question, five of which involve an in-depth discussion of the issue.[9] These cases turn on whether one interprets authorization based upon the rules of the computer, principles of agency, or the rules of the workplace (which are essentially the terms of a contract), and demonstrate the differing interpretations of this provision in the courts.

Of the seven significant circuit cases on "unauthorized access," the earliest decision was *International Airport Centers, L.L.C. v. Citrin*.[10] *Citrin* was a civil case, brought under 18 U.S.C. § 1030(g).[11] Citrin's job was to identify properties for his employer to purchase and to help with any efforts to purchase them.[12] He had the use of a company laptop to record the information he collected.[13] Citrin decided to work for himself.[14] When he returned the laptop, he had deleted all the data he had collected.[15] The employer sued alleging a violation of § 1030(a)(5)(A)(i).[16] Citing the Restatement (Second) of Agency, the Seventh Circuit held that Citrin breached his duty of loyalty when he quit in violation of his contract and deleted files that belonged to the employer.[17] This breach ended his agency relationship and made his access to the computer unauthorized.[18] The court's finding follows the Restatement (Second) of Agency, section 112, which states that "the authority of an agent terminates if . . . he is . . . guilty of a serious breach of loyalty to the principal."[19]

Three years later, the Ninth Circuit faced the issue in the context of a civil case, *LVRC Holdings LLC v. Brekka*.[20] Brekka worked for

---

9 Additional cases in the district courts are not discussed here. These cases largely follow the circuit precedents.

10 Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

11 *See id.* at 419. Although § 1030 is a criminal statute, it has a civil remedy in § 1030(g). *See* 18 U.S.C. § 1030(g).

12 *Citrin*, 440 F.3d at 419.

13 *Id.*

14 *Id.*

15 *Id.*

16 *Id.*

17 *Id.* at 420.

18 *Id.* at 420–21. The case reached the court of appeals after the district court dismissed the complaint. There had been no discovery and, thus, no factual record. It is likely that Citrin kept a copy of the data he had collected and gave a hard drive without the data back to the employer. If those facts had been established, this would be a classic data theft case. Under an agency theory, in accessing the computer to copy the data for his own purposes, Citrin was no longer acting as an agent. Although the case was brought alleging a violation of what was then 18 U.S.C. § 1030(a)(5)(A)(i), which was not an unauthorized access charge, to resolve the case, the court looked to § 1030(a)(5)(A)(ii), which was. *Id.*

19 *See* 1 RESTATEMENT (SECOND) OF AGENCY § 112 (AM. LAW INST. 1958).

20 LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

LVRC and was given administrator privileges, which allowed him access to usage statistics about LVRC's website.[21] He did not have a written contract, and LVRC did not prohibit employees from emailing company documents to their personal computers.[22]

In the course of negotiations to purchase an ownership interest in LVRC, Brekka emailed a number of LVRC documents from his work address to his and his wife's personal email addresses.[23] LVRC sued Brekka alleging that his sending of the documents was both unauthorized access to their computers and exceeding authorized access.[24] The court of appeals held that because Brekka was authorized to access the LVRC computers at the time that he emailed the documents, his access was authorized.[25] It further held that because Brekka was authorized to obtain the documents he emailed, he did not exceed authorized access when he did so.[26]

The court rejected the *Citrin* agency theory, writing:

> The plain language of the statute therefore indicates that "authorization" depends on actions taken by the employer. Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer. If the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA.[27]

The court made a similar holding with respect to exceeding authorized access claim.[28]

The court held that agency law plays no role in interpreting the concept of authorization.[29] The court looks only to what the principal said, not to the agent's motive when she acted.[30] If the agent had the right to access the computer, her access was authorized.[31] If the agent had the right to view or possess the data in question, she did not ex-

---

21 *Id.* at 1129.
22 *Id.*
23 *Id.* at 1129–30.
24 *Id.* at 1131.
25 *Id.* at 1135.
26 *Id.* at 1135–36 n.7.
27 *Id.* at 1135.
28 *Id.* at 1135–36 n.7.
29 *See id.* at 1134–35.
30 *Id.* at 1135.
31 *Id.*

ceed authorized access.[32] The conduct was not a violation of § 1030, regardless of any malicious intent of the agent.[33]

In *United States v. John*,[34] the defendant worked for a bank and gave customer account information to a coconspirator, who used it "to incur fraudulent charges" on these accounts.[35] John was authorized to access the computer for her job and was authorized to view the data.[36] The opinion, therefore, focused on whether she exceeded her authorized access when she took the data.[37]

Company rules prohibited her from removing account information from the office.[38] She had training programs that made clear that company policy prohibited the use of the company's computer system and confidential customer information for anything other than company purposes.[39] The court found two reasons to hold that John's conduct exceeded authorized access.[40] First, the court employed a "norms of the workplace" frame of reference, which it called an "intended-use" rule.[41] It held that the "use of [a bank's] computer system to perpetrate a fraud was not an intended use of that system."[42] Second, the published company policy limited the use of company information.[43] When John knowingly violated the policy, she exceeded authorized access.[44] She was not authorized to obtain access to the data for any purpose, but only for a limited one.[45] Her access outside that limit exceeded her authorization.[46]

The opinion distinguished the Ninth Circuit's concerns expressed in *Brekka* that an employee would not know when he was violating state fiduciary law.[47] Here, the scheme was clearly fraudulent.[48]

---

32 *Id.* at 1135–36 n.7.

33 *Id.* at 1135.

34 United States v. John, 597 F.3d 263 (5th Cir. 2010).

35 *Id.* at 269.

36 *Id.* at 271–72.

37 *Id.*

38 *Id.* at 272.

39 *Id.*

40 *Id.*

41 *Id.* at 271–72.

42 *Id.* at 272.

43 *Id.*

44 *Id.*

45 *Id.*

46 *Id.*

47 *See id.* at 272–73.

48 *See id.* at 273.

In *United States v. Rodriguez*,[49] the defendant Rodriguez worked for the Social Security Administration ("Administration") as a TeleService employee.[50] He was authorized to access account information, which included personal identifying information, such as full names, parents' names, addresses, birth dates, and social security numbers, only to perform his job.[51] The Administration had mandatory training sessions to remind employees that they could access data only in the performance of their duties.[52] The logon screen of Rodriguez's computer reminded him of this rule daily.[53] Employees were asked to sign a form annually, acknowledging that they had been given a written copy of this policy.[54] Rodriguez engaged in a course of conduct that can easily be described as stalking, using information obtained from the database to locate home addresses and other information about women he was interested in dating.[55]

The court held that workplace rules were part of the definition of authorization, and that by breaking the workplace rules and accessing the data for a nonwork-related purpose, Rodriguez had exceeded his authorization.[56] It distinguished this case from *Brekka* because the company in *Brekka* had no policy prohibiting employees from sending company documents to their personal email accounts.[57] Rodriguez argued that he was being punished for improper use of data, and *John* required that the use be criminal.[58] The court declined to even consider this argument, holding that his use was irrelevant to its consideration because he had exceeded authorization when he accessed the data in direct and knowing violation of the workplace rules.[59]

The Ninth Circuit followed *Brekka* with *United States v. Nosal* ("*Nosal I*").[60] David Nosal worked for Korn/Ferry, an executive

---

49 United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

50 *Id.* at 1260.

51 *Id.*

52 *Id.*

53 *Id.*

54 *Id.* Tellingly, Rodriguez declined to sign for several years. *Id.*

55 *See id.* at 1260–62.

56 *Id.* at 1263.

57 *Id.*

58 *Id.*

59 *See id.* (neglecting to consider whether defendant's conduct violated any state stalking statutes or 18 U.S.C. § 2261A). The holding in *Rodriguez* helps to explain why the Assistant U.S. Attorney in Georgia in the opening hypothetical was willing to open an investigation. *See supra* Section I.A.

60 United States v. Nosal (*Nosal I*), 676 F.3d 854 (9th Cir. 2012) (en banc). *Nosal I* is distinguished from *United States v. Nosal* (*Nosal II*), 828 F.3d 865 (9th Cir. 2016).

search firm.[61] After he left Korn/Ferry to work for a competitor, he persuaded a few of his former colleagues to download information from a confidential database on the Korn/Ferry computers and send it to him.[62] Korn/Ferry authorized the employees to access the database, but had a policy that made it clear that the database was available to them "for work on Korn/Ferry business only."[63] Nosal was charged with aiding and abetting the Korn/Ferry employees with "exceed[ing their] authorized access" to the computers with intent to defraud under 18 U.S.C. § 1030(a)(4).[64]

In *Nosal I*, the company had clearly stated policies that employees were given access to company data only to serve the company.[65] The government argued that these policies distinguished *Brekka*.[66] The opinion is largely a collection of potentially frightening prosecutions if the government's theory of unauthorized access and exceeding authorized access was correct.[67] The court conjured up a series of workplace rules violations that would be prosecutable under the government's view.[68] These included checking weather reports, sending personal emails, doing online puzzles, and tending one's Farmville stable.[69] Although the government attempted to keep the focus on the authorized access issues in the context of the fraud charged under § 1030(a)(4), the court focused on that term as it applied across § 1030, and in particular on § 1030(a)(2), regarding obtaining information.[70] Finding that all of these situations could be prosecuted under

---

61 *Nosal I*, 676 F.3d at 856.

62 *Id.*

63 *Id.* at 856 n.1.

64 *Id.* at 856 (quoting 18 U.S.C. § 1030(a)(4) (2012)). 18 U.S.C. § 1030(a)(4) states:

> Whoever— . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

18 U.S.C. § 1030(a)(4) (2012). While the statute is somewhat different than § 1030(a)(2), the concepts of authorized access and exceeding authorized access are the same, so *Nosal I* is a useful case for this analysis. Indeed, the government argued that the court should apply a different standard for those terms in a § 1030(a)(4) case than it might in a § 1030(a)(2) case. The court firmly declined this invitation to have a term with a single definition have different meanings within the same statute. *Nosal I*, 676 F.3d at 859.

65 *Nosal I*, 676 F.3d at 856 n.1.

66 Reply Brief for the United States at 4, *Nosal I*, 676 F.3d 854 (9th Cir. 2012) (en banc) (No. 10-10038).

67 *Nosal I*, 676 F.3d at 857–62.

68 *Id.*

69 *See id.* at 860 n.7.

70 *Id.* at 859.

§ 1030(a)(2) under the government's theory, the court declined to limit *Brekka* to cases in which there was no company policy.[71]

The Fourth Circuit's decision in *WEC Carolina Energy Solutions LLC v. Miller*[72] is a straightforward adoption of the reasoning of *Nosal I* and a rejection of *Citrin.*[73]

Finally, in *United States v. Valle*,[74] the Second Circuit examined the issue in a case involving a police officer who accessed the National Crime Information Center ("NCIC") database for personal reasons, even though he knew that he could only do so for official business.[75] The Second Circuit examined the cases and the legislative history, and found merit to both sides of this argument.[76] It then concluded that

---

71 *Id.* at 856, 863. With the *Brekka* decision having rejected the agency theory of unauthorized access, there was no need for the *Nosal I* court to do so. *See id.* However, none of the hypothetical examples listed in the opinion would have been unauthorized under the agency theory, for none of them involved "a serious breach of loyalty to the principal" required by the Restatement. 1 RESTATEMENT (SECOND) OF AGENCY § 112 (AM. LAW INST. 1958). They might have been grounds for discipline or even termination, but none of them struck at the heart of the trust required between principal and agent.

Nosal I is also puzzling for a different reason. Nosal was charged with aiding and abetting the Korn/Ferry insiders with violating § 1030. *See Nosal I*, 676 F.3d at 856. 18 U.S.C. § 2(a) makes those who aid or abet others to commit a crime punishable as principals. 18 U.S.C. § 2(a) (2012). Had the government charged him with "willfully caus[ing] an act to be done" under § 2(b), the outcome might have been different for Nosal. *Id.* § 2(b). Under 18 U.S.C. § 2(b), those who willfully cause another to commit a crime are also punishable as principals. 18 U.S.C. § 2(b). While the opinion in *Nosal I* decides that the insiders cannot be convicted of violating § 1030, it did not consider that Nosal was an outsider with no right to be in the system. *See Nosal I*, 676 F.3d at 864. Nosal willfully caused the insiders to obtain access to a computer on his behalf. *See id.* at 856. He was prosecutable for willfully causing them to do so. *See* 18 U.S.C. § 2(b). The law is clear that a person can be convicted under a willful causation theory, even if the person doing the act is immune. United States v. Lee, 602 F.3d 974, 976 (9th Cir. 2010); United States v. Ordner, 554 F.2d 24, 29 (2d Cir. 1977); United States v. Kelner, 534 F.2d 1020, 1022 (2d Cir. 1976); United States v. Valencia, 492 F.2d 1071, 1074 (9th Cir. 1974); *cf.* Standefer v. United States, 447 U.S. 10, 18–19 (1980) (noting that acquittal of the principal does not bar the conviction of an aider and abettor). The fact that the insiders could not be convicted was not a bar to convicting Nosal himself. The court in *Nosal II* did not rely on 18 U.S.C. § 2(b), but it did agree that as an outsider, Nosal could be convicted of unauthorized access for using an insider's username and password. *See infra* note 101.

72 WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).

73 *Id.* at 203–06. In this case, a company employee took proprietary information before leaving and used it to help his new employer compete against the old one. *Id.* at 202. The court had one minor quibble with the *Nosal I* court over the construction of the word "so," but it had no impact on the result. *Id.* at 205–06. *WEC* is the reason that the Assistant U.S. Attorney in South Carolina in the hypothetical would not open an investigation. *See supra* Section I.A.

74 United States v. Valle, 807 F.3d 508 (2d Cir. 2015).

75 *Id.* at 512–13.

76 *Id.* at 524–27.

because the proper interpretation of the law was not clear, the rule of lenity compelled it to follow *Nosal I* and *WEC*.[77]

II. The Different Approaches

A. *Case Types*

These cases fit into three categories in defining the term "authorization": agency, rules of the workplace, and rules of the computer. The problem arises because each of these categories constitutes a different lens for viewing the question of unauthorized access. Each one is rational, but they lead to varying results.

The agency cases, of which *Citrin* is our prime example, look to the law of agency to determine authorization. An agent is obligated to act on behalf of her principal.[78] She is not permitted to put her interests before those of her principal and owes a duty of loyalty to the principal.[79] According to the Restatement (Second) of Agency, "[u]nless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[80] Employees who steal their employers' data to use on behalf of themselves or another principal are guilty of a serious breach of loyalty. As soon as an agent accesses the employer's computers with this disloyal purpose, the agent is no longer acting as an agent of the employer.[81] Because the authorization to access the computer is based upon the agency relationship, when the agent accesses the computer to steal the data, she is not accessing the computer with authorization.[82] Thus, in jurisdictions that follow the agency approach, § 1030 provides a reasonable remedy for the disloyal employee's theft of data.

"Employment work place rules" cases, such as *John* and *Rodriguez*, are a subset of the contract cases.[83] Rules created by the employer regarding the purposes for which access can be made can determine whether the access is authorized. If access is limited to furthering the employer's business, access for any other purpose is unau-

---

77 *Id.* at 526–28.

78 *See* 1 Restatement (Second) of Agency § 112 cmt. b (Am. Law Inst. 1958); *see also id.* § 1.

79 *Id.* § 112 cmt. b.

80 *Id.* § 112.

81 *See id.*

82 *See id.*

83 *See supra* notes 34–59 and accompanying text. The only contract case in the court of appeals, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 579–80 (1st Cir. 2001), does not involve an insider, so it is not discussed here.

thorized. This can provide clarity, but as *Nosal I* noted, it also carries risks.

The final group is the "rules of the computer" cases. *Brekka*, *Nosal I*, and *WEC* can be considered in this category.[84] In the "rules of the computer cases," courts only look to the rules written into the computer itself. If the person has not bypassed the rules programmed into the computer rules for access, it does not matter what he was thinking, or what the employer told him. If the computer says "yes," the case is over. If the person has to bypass software or hardware safeguards to access the computer, then the access is not authorized.

In contrast to the "rules of the computer" standard, the "rules of the workplace" cases and the agency cases step back from the computer itself and look to the relationship between the employer and the employee. They ask if there were clear rules about computer use (in language that humans use to communicate with each other, not computer code).

The concerns about workplace rules and contracts are those expressed in *Nosal I*: who decides which breaches of workplace rule and contract terms warrant prosecution?[85] Can an employer or a website make "silly" rules that criminalize behavior?[86] Because no one reads website terms of service, the risk of unfair prosecutions could be high.[87] The risk is a decisionmaking process so lacking in standards, that it becomes a due process violation.[88]

Although this might be remedied by relying upon an agency theory and limiting cases to those involving a serious breach of the duty of loyalty, the Supreme Court decision in *Skilling v. United States*[89] casts serious doubt upon the feasibility of this idea. The "honest services" theory of mail fraud, 18 U.S.C. § 1346,[90] had been used to charge serious breaches of the agency relationship and conflicts of interest,[91] but *Skilling* has eliminated this theory, requiring that "honest services" fraud involve the payment of money for disloyalty, because

---

84 *See supra* notes 20–33, 60–73 and accompanying text.

85 *Nosal I*, 676 F.3d 854, 860 (9th Cir. 2012) (en banc).

86 *Id.*

87 *Id.* at 861–62.

88 This was the concern in *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), which influenced the decision in *Nosal I*. *See Nosal I*, 676 F.3d at 862.

89 Skilling v. United States, 561 U.S. 358 (2010).

90 18 U.S.C. § 1346 (2012).

91 *See, e.g.*, United States v. DeVegter, 198 F.3d 1324, 1328–29 (11th Cir. 1999) ("[T]he breach of loyalty by a private sector defendant must in each case contravene—by inherently harming—the purpose of the parties' relationship.").

any other standard ran the risk of being unconstitutionally vague.[92] The reasoning of *Skilling* is most likely applicable to any similar interpretation of § 1030. Under the agency theory as expressed in *Citrin*,[93] it is not the taking of a bribe or kickback, but the breach of a fiduciary duty that forms the basis of criminal liability. It is very likely that a proper reading of *Skilling* would find that such an interpretation of the CFAA would also be void for vagueness.

The flaw in the "rules of the computer" cases is that, while the theory is frequently promoted as a "code-based" rule,[94] it really is not. Consider the person who uses another's username and password to access a computer. This is considered a classic unauthorized access.[95] If we only look at the rules coded into the computer, this is an authorized access, however. The computer compares the username and password, sees that they match, and allows access. To make this access unauthorized, we need to move back from the computer, and look to who set the rules and what they meant. There we run into ambiguity.

Suppose Alex is out of the office and needs certain information, so he asks coworker Mary to log into his workplace computer, using his credentials, to get the information for him. Is Mary's access authorized? From the point of view of the rules programmed into the computer, it is—she typed in the correct username and password. From Alex's point of view, it is. The access may not be authorized from the point of view of the employer, however. The employer may have a policy that allows this, or the employer may consider this to be a serious breach of workplace security. To the computer, all these situations look the same. The point here is that the rules programmed into the computer do not provide us with the answer to the question: was Mary's access authorized? The answer will turn on the employer's rules and policies, written in English, not in computer code.

The same is true if Mary, without Alex's permission, guesses Alex's username and password. Again, the rules of the computer tell us that this access is authorized. However, the person who set the rules meant that if Alex had a particular username and password, Mary could not use it without permission, even if Mary knew it and

---

92 *Skilling*, 561 U.S. at 408–09.

93 Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

94 *See, e.g.*, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1644–46 (2003).

95 Theofel v. Farey-Jones, 359 F.3d 1066, 1074 (9th Cir. 2004) (quoting United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991)).

could convince the computer that she was Alex. In short, we do not want to limit an unauthorized access statute to deal only with the hacker whose computing skills overwhelm the defenses of a computer.

Finally, as evidence that courts are concerned with the rules of the workplace and not just those inside the computer, consider *United States v. Steele*[96] and *United States v. Shahulameed*,[97] in which the defendants continued to log into the computers of their former employers after they had left their jobs. The defendants argued that because the company had not disabled the accounts, their accesses were authorized.[98] Both courts rejected the arguments.[99] The court in *Steele* characterized its rejection of the argument as "common sense."[100]

In *United States v. Nosal* ("*Nosal II*"),[101] the Ninth Circuit recognized the validity of this proposition. In *Nosal II*, the government prosecuted the defendants for acts they committed after all of them had left Korn/Ferry's employment.[102] The trial record showed that Nosal and his coconspirators got a username and password from a current employee and accessed Korn/Ferry's computers.[103] The court noted that under company policy the current employee "had no authority from Korn/Ferry to provide her password to former employees whose computer access had been revoked."[104] Although the current employee "might have been wrangled into giving out her password, she and the others knew that she had no authority to control system access."[105]

If password guessing and misuse of passwords is unauthorized access, which everyone agrees it should be, then the basis for the rules of authorization lies outside the computer. Yet, once we look to what the employer intended, it is hard to distinguish the password misuse cases from *John* and *Rodriguez*.

---

96 United States v. Steele, 595 F. App'x 208 (4th Cir. 2014).

97 United States v. Shahulhameed, 629 F. App'x 685 (6th Cir. 2015).

98 *Id.* at 688; *Steele*, 595 F. App'x at 210–11.

99 *Shahulhameed*, 629 F. App'x at 688; *Steele*, 595 F. App'x at 211.

100 *Steele*, 595 F. App'x at 211.

101 United States v. Nosal (*Nosal II*), 828 F.3d 865 (9th Cir. 2016).

102 Thus, *Nosal II* is not a case that involves a disloyal, current employee and is outside the scope of our problem.

103 *Id.* at 871.

104 *Id.* at 870.

105 *Id.* at 875 n.7.

B. *Statutory Drafting and Internet Norms*

All of these cases present issues of the norms for computer use along with issues of proper statutory construction. They involve restricted computer systems containing data that was not available to the public.[106] *Citrin*, *Nosal I*, *WEC*, *Rodriguez*, *John*, and *Valle* involved a disloyal employee—one who used his or her insider status to obtain confidential information and then used that information against the employer's interest.[107] The courts have either decided that the statute reaches this conduct because it is so clearly wrong that it is in excess of authorized access, or they have employed a strict construction of the law, and held that the statute does not cover the conduct because the employee was allowed access to the computer and to the data, regardless of what he or she did thereafter.[108] The problem, however one chooses to construe the statute, is real.

The meaning of the terms chosen by Congress, "authorized access" and "exceeds authorized access,"[109] are vague[110] partly because we have no consensus on what is permissible conduct on computers. The personal computer is less than forty years old and large-scale adoption of desktop computers by businesses is less than thirty years old.[111] Societal norms take a long time to develop and there has not

---

106 United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010); United States v. John, 597 F.3d 263, 269 (5th Cir. 2010).

107 United States v. Valle, 807 F.3d 508, 512–13 (2d Cir. 2015); *Nosal I*, 676 F.3d 854, 856 (9th Cir. 2012) (en banc); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 202 (4th Cir. 2012); *Rodriguez*, 628 F.3d at 1260; *John*, 597 F.3d at 269; Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

108 *See supra* note 107.

109 18 U.S.C. § 1030(a)(2) (2012).

110 In *Nosal II*, however, the Ninth Circuit found that the term

> "without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission. This definition has a simple corollary: once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party. Unequivocal revocation of computer access closes both the front door and the back door.

Nosal II, 828 F.3d at 868–69. However, *Nosal II* does not deal with the disloyal employee problem. It addresses the former employee. Our problem is access by a current employee. *Nosal I* governs our issue.

111 9 David Wright, America in the 20th Century 1249 (2d ed. 2003). There were almost no personal computers in business use in 1980. By 1990, it is estimated that there were about twenty-five million in use by businesses. *Id.* One estimate put the total number of devices connected to the internet in excess of eight billion in 2012. Rob Soderbery, *How Many Things Are Currently Connected to the "Internet of Things" (IoT)?*, Forbes (Jan 7, 2013, 1:26 PM), http://www.forbes.com/sites#/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/ [https://perma.cc/MX6D-QV7A].

been enough time for a consensus to form.[112] In addition, today, we have laws being written by legislators and interpreted by judges with a wide variety of computer savvy. Over the next twenty to thirty years that will change as a generation that grew up with computers takes over. It will take time to form a consensus about the kinds of actions that are permissible on a work computer. The problem of the disloyal employee, however, is here today and is not going away. Businesses cannot wait another twenty years for a consensus to form.

C. Alternative Statutes for Prosecution

Before adding to existing laws, it is fair to ask if there are alternative ways to prosecute this conduct. The answer is that sometimes there are. The wire fraud statute[113] can be a powerful tool if the government can show fraud. Not all stealing is fraudulent, however. Fraud requires either an intentional material misrepresentation or the deliberate withholding of a material fact.[114] The employees and former employee in *Nosal I* and the employees in *WEC* and *John* did not lie or withhold information.[115] They stole the data fair and square—no lying involved.[116]

The Theft of Trade Secrets Act[117] can also prove useful sometimes, but not everything stolen is a trade secret.[118] Consider a cus-

---

112 *See generally* Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM L. REV. 1143, 1153–61 (2016).

113 18 U.S.C. § 1343 (2012). The statute provides, in pertinent part:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

Id.

114 *See* Neder v. United States, 527 U.S. 1, 25 (1999); United States v. Pearlstein, 576 F.2d 531, 535 (3d Cir. 1978) ("The scheme need not be fraudulent on its face, but must involve some sort of fraudulent misrepresentations or omissions reasonably calculated to deceive persons of ordinary prudence and comprehension." (citation omitted)).

115 *See Nosal I*, 676 F.3d 854, 854 (9th Cir. 2012) (en banc); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 199 (4th Cir. 2012); United States v. John, 597 F.3d 263, 263 (5th Cir. 2010).

116 *See supra* note 115*; see also* Skilling v. United States, 561 U.S. 358, 365 (2010) (finding that proof of honest services fraud requires proof of a bribe or gratuity to take the data).

117 18 U.S.C. § 1832 (2012).

118 "Trade secret" is defined in 18 U.S.C. § 1839. *See* 18 U.S.C. § 1839 (2012). The definition is similar to that in the Uniform Trade Secrets Act. *See* Uniform Trade Secrets Act § 1(4) (1986). Section 1832, however, contains an additional definitional element: the secret must be "related to a product or service used in or intended for use in interstate or foreign commerce,"

tomer list with notations of a customer's particular preferences for goods, shipping, times to call, and spouse's and children's names. All of this information would be useful to a competitor wishing to steal the business. The document, however, is not a prosecutable trade secret. Neither was the data taken by Rodriguez and John, although apparently the data taken by Nosal was, because the government charged him with violating that act and his conviction was affirmed.[119] The Trade Secret Act can be a useful tool, but it will not cover all data theft by employees.

Some may ask why a federal prosecution is necessary. My answer is both practical and theoretical. There are few nonfederal law enforcement agencies and prosecution offices with the time or the expertise to investigate and prosecute these cases. Most law enforcement officers are peace officers.[120] Detectives follow up on the work of the peace officers, but most of the crime that is of their concern is either violent crime, drug crime, or the types of crimes that make a municipality unlivable. If a business complains about a computer data theft, these agencies usually do not have the capacity to help. If there is to be a prosecution at all, it will have to come from the federal government. From a theoretical viewpoint, these thefts interfere with the proper flow of interstate and foreign commerce, and are a proper subject for federal attention.

D. The Current Proposed Solution

In July 2015, Senators Graham and Whitehouse released a discussion draft of legislation that would replace the language of § 1030(a)(2) with the following:

> "(2)(A) intentionally accesses a protected computer without authorization and thereby obtains information from or causes damage to any such protected computer;
>
> "(B) accesses a protected computer with authorization and thereby knowingly obtains information from such computer that the accessor is not entitled to obtain, or knowingly obtains any information from such computer for a purpose

---

which means that not everything which a business keeps secret and which is not readily ascertainable is a prosecutable trade secret. 18 U.S.C. § 1832.

119 *Nosal I*, 676 F.3d at 859; *Nosal II*, 828 F.3d 865, 880–84 (9th Cir. 2016).

120 *See* BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, FEDERAL LAW ENFORCEMENT OFFICERS, 2008, at 1 (June 2012), http://www.bjs.gov/content/pub/pdf/fleo08.pdf; BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, CENSUS OF STATE AND LOCAL LAW ENFORCEMENT AGENCIES, 2008 1–2 (July 2011), http://www.bjs.gov/content/pub/pdf/csllea08.pdf.

> that the accessor knows is prohibited by the computer owner, if—
>
> "(i) the value of the information obtained exceeds [$10,000];
>
> "(ii) [the conduct was undertaken in furtherance of any felony violation of the laws of the United States or of any State, unless an element of such violation would require proof that the information was obtained without authorization or in excess of authorization;] or
>
> "(iii) the protected computer is owned or operated by or on behalf of a State or local governmental entity responsible for the administration of justice, public health, or safety, or of the United States Government; and
>
> "(C) the limitation on access to or use of the information is not based solely on the terms of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, between a provider of online service and a customer or subscriber thereof."[121]

Will this help us with the hypothetical data theft presented at the beginning of this Article? The answer is sometimes it will, but often it will not. First, subsection (iii) is of no help because, in the scenario presented above, our client is not a government entity. Subsection (i) can present problems because of the difficulty in valuing data. In some cases, it is not hard to place a number on it, but often, the task is nearly impossible. Consider the customer list mentioned above, with notations of a customer's particular preferences for goods, shipping, times to call, and spouse's and children's names.[122] Putting a value on that list is probably not feasible. There is some caselaw on valuation that permits the cost of assembling the information.[123] That is not always an easy thing to calculate. Although lawyers keep time sheets, few businesses do. Although many federal statutes have a jurisdic-

---

121 *See* Senate Legislative Counsel, International Cybercrime Prevention Act of 2015, https://cdt.org/files/2015/07/Graham-Whitehouse-Discussion-Draft.pdf; *see also* Harley Geiger, *Graham/Whitehouse Draft Bill Would Make CFAA Worse*, CTR. DEMOCRACY & TECH. (July 17, 2015), https://cdt.org/blog/grahamwhitehouse-draft-bill-would-make-cfaa-worse/.

122 *See supra* Section II.B.

123 *See* United States v. Batti, 631 F.3d 371, 377–78 (6th Cir. 2011) (deciding under 18 U.S.C. § 1030(a)(2) and citing cases decided under 18 U.S.C. § 2314 for support); United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988) (deciding under 18 U.S.C. § 2314); United States v. Drebin, 557 F.2d 1316, 1328 (9th Cir. 1977) (same).

tional dollar limit, these are frequently tied to the value of commodities[124] or to a determinable expense.[125]

There is a similar problem with subsection (ii). The taking of this property has to be a felony. While the Interstate Transportation of Stolen Property Act ("ITSP")[126] would seem to be an obvious solution, it has significant limits. First, although the title of the statute uses the term "property," the text limits the "property" to "goods, wares, merchandise, securities or money, of the value of $5,000 or more."[127] Much of what employees take on their way out is not "goods, wares, merchandise, securities, or money." Second, there is a significant body of law holding that digital materials are not "goods, wares, and merchandise" under ITSP.[128] By the very nature of the crime, what will be taken will be digital in nature. Yet, there may be no federal crime that fits. The application of the federal statute will thus turn on whether individual states recognize the stealing of digital property as theft.

Although subsection (C) is probably meant to insure that violations of terms of service of websites are not a basis for criminal prosecution, it is written in a way that might bar prosecution of the employee in our problem. The defendants in *Rodriguez* and *Valle* violated a contractual obligation between themselves and the government, which was part of their employment agreement.[129] If Rodriguez

---

124 *See, e.g.*, 18 U.S.C. § 2314 (2012) (pertaining to stolen goods that have a value of more than $5000); 18 U.S.C. § 2319 (2012) (pertaining to reproduction of copyrighted works that have a value of more than $2500).

125 *See, e.g.*, 18 U.S.C. § 1030(c)(4)(A)(i)(I) (pertaining to loss to victims of at least $5000).

126 18 U.S.C. § 2314 (2012). This section is a subsection of the National Stolen Property Act, §§ 2311, 2314–2315.

127 *Id.*

128 *See, e.g.*, United States v. Aleynikov, 676 F.3d 71, 77 (2d Cir. 2012); United States v. Stafford, 136 F.3d 1109, 1114–15 (7th Cir. 1998); United States v. Brown, 925 F.2d 1301, 1307–08 (10th Cir. 1991). In my view these cases are wrong. Amazon, Google, Microsoft, Apple, and Symantec would probably be surprised to learn that the software, books, and music that they offer for downloading are not "goods, wares, or merchandise." The absurdity of the result is best illustrated by comparing *Aleynikov* and *United States v. Agrawal*, 726 F.3d 235 (2d Cir. 2013). Both Aleynikov and Agrawal worked for investment banks. *Agrawal*, 726 F.3d at 237; *Aleynikov*, 676 F.3d at 73. Both stole the source code for the bank's high frequency trading system. *Agrawal*, 726 F.3d at 237; *Aleynikov*, 676 F.3d at 74. Aleynikov did so by uploading the code to a storage server in Europe and then downloading it at home. *Aleynikov*, 676 F.3d at 74. Agrawal used the low-tech method of printing out the software code and carrying out the paper on which he had printed the source code. *Agrawal*, 726 F.3d at 237. The decisions were that Aleynikov had not taken "goods, wares, or merchandise," while Agrawal had. *Agrawal*, 726 F.3d at 242–44; *Aleynikov*, 676 F.3d at 76–79.

129 *See generally* United States v. Valle, 807 F.3d 508 (2d Cir. 2015); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

or Valle worked for a private business and if we could not find other crimes committed by them, they may not be prosecutable under this proposed statute. While the terms of use in *Rodriguez* and *Valle* were not between a provider of online service and a customer or subscriber, those statutory terms are words of example and not of restriction. Because this is a criminal statute, the rule of lenity may result in a court holding that any violation of workplace rules, which is not otherwise a crime, is excluded from coverage. The same concern about delegating the power to employers to choose what conduct is criminal, which bothered the court in *Nosal I*, lurks here.

A narrow interpretation, however, means that the hypothetical problem remains unsolved. Of the cases discussed, probably only the defendants in *Rodriguez* (the Social Security Administration employee who accessed a government computer)[130] and *Valle* (the police officer who accessed the NCIC computer)[131] will be covered. For the defendants in *Citrin*, *Nosal I*, and *John*, it will depend upon the value of the information, or if the government can find a felony that this data theft assisted.

III. Access with Intent to Steal

A. The Proposal

The current state of the law is such that the venue of the act may determine whether or not it was criminal.[132] The draft legislation in Congress tries to fix issues of authorization, but does not deal directly with the problem of the disloyal employee.[133] This Article proposes instead that to solve this prevalent problem, we abandon the focus on whether the access was authorized and focus on the intent of the person when he or she was making the access. If the purpose was to steal information, we should criminalize it. Here is my proposed statute:

> 18 U.S.C. § 1030(a)(8)
> (A) Whoever intentionally, and with intent to steal information, accesses a protected computer of another and appropriates, takes, carries away, copies, duplicates, downloads, uploads, replicates, transmits, delivers, sends, mails, communicates, conveys, or otherwise steals any information of another shall be punished as provided in subsection (c) of this section.

---

130 *Rodriguez*, 628 F.3d at 1260.

131 *Valle*, 807 F.3d at 512–13.

132 *See supra* Section II.A.

133 *See supra* Section II.D.

(B) The owner of the information must have taken reasonable steps to keep the information from the public, and either
  (i) the information taken must either:
    (a) have a value of $5000 or more; or
    (b) be sensitive, nonpublic business information; or
  (ii) the offense was committed for commercial advantage or private financial gain.
(C) "Value" means the face, par, or market value, whichever is the greatest, and the aggregate value of information referred to in a single indictment shall constitute the value thereof.[134]

The proposal requires an intentional access, as do most of the other access sections of § 1030. It is similar to § 1030(a)(4) in requiring a mental state when making access. I have made the mental state "intentionally," rather than "knowingly." It appears to be a slightly higher standard, but under these circumstances, the intent to steal will certainly provide the evidence of intentional access. I chose the word "steal" to use the word as the Supreme Court construed it in the National Stolen Property Act.[135] It is also a term used in the Theft of Trade Secrets Act.

This proposal incorporates the asportation verbs from the Theft of Trade Secrets Act. In this regard, the statute is different from the unauthorized access prohibition of § 1030(a)(2). That section does not require asportation.[136] The proposed law does require the carry-

134 The definition of "value" parallels that in the National Stolen Property Act. 18 U.S.C. § 2311 (2012). An attempt to violate this section would be covered by the general attempt and conspiracy language of § 1030(b). While problems of proof make it unlikely that a prosecutor would charge an attempt (how do we know what the person's intent was), there may be cases in which this will be a useful tool.

135 18 U.S.C. §§ 2311, 2314–2315. *See* United States v. Turley, 352 U.S. 407, 417 (1957) ("We conclude that the Act requires an interpretation of 'stolen' which does not limit it to situations which at common law would be considered larceny. The refinements of that crime are not related to the primary congressional purpose of eliminating the interstate traffic in unlawfully obtained motor vehicles. The Government's interpretation is neither unclear nor vague. 'Stolen' as used in 18 U.S.C. § 2312 includes all felonious takings of motor vehicles with intent to deprive the owner of the rights and benefits of ownership, regardless of whether or not the theft constitutes common-law larceny."). It is worth noting that "steal" is a word that has been commonly understood at least since Biblical times (or more accurately, the early seventeenth century). *Deuteronomy* 5:19 (King James); *Exodus* 20:15.

136 *See* S. REP. NO. 99-432, at 6–7 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2484. The Senate Report states:

> The Department of Justice has expressed concerns that the term "obtains information" in 18 U.S.C. § 1030(a)(2) makes that subsection more than an unauthorized access offense, i.e., that it might require the prosecution to prove asportation of the data in question. Because the premise of this subsection is privacy protection, the

ing away of the data (or at least an attempt to do so). This is not an "access" statute; it is a "taking" statute. For those who suggest that copying is not stealing, the law has already said that it is with respect to the photocopier.[137] There is no reason not to apply this concept to digital copying.

The law only makes it a crime to take information. The government cannot use this statute to prosecute an employee who takes time and money from his employer by working on things other than his job, because that employee takes no information.

The proposal limits the information taken to the types of information that are taken from businesses, but there are alternative standards to deal with the problems here. First, the business must have made efforts to keep the information out of public hands. Data placed on a publicly accessible website is not covered.[138]

Second, the proposal also addresses the idea that the information should have some value. As a first option, there is a dollar value for the data stolen. As discussed above, it is frequently difficult to impossible to do this.[139] However, where it is possible, it provides a ready measure of the importance of the information.[140] The definition of "value" in the proposal is from 18 U.S.C. § 2311, so the law is clear how the valuation should be done. Where it is not realistic to place a dollar value on the data, the statute will require that the data be sensitive, nonpublic information of a business. In the alternative, if the motive was commercial advantage or private financial gain, the proposal uses the language from 18 U.S.C. § 1030(c)(2)(B) and the Copyright Act.[141]

> Committee wishes to make clear that "obtaining information" in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.

Id. (footnote omitted).

137 United States v. Bottone, 365 F.2d 389, 393–94 (2d Cir. 1966); United States v. Lester, 282 F.2d 750, 754–55 (3d Cir. 1960).

138 This eliminates the possibility of a prosecution of someone "scraping" a public website for data. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579–80 (1st Cir. 2001).

139 *See supra* Section II.D.

140 In the context of a prosecution under 18 U.S.C. § 2314, courts have held that the value can be that in a "thieves' market." United States v. Weinstein, 834 F.2d 1454, 1463 (9th Cir. 1988); United States v. Moore, 571 F.2d 154, 157–58 (3d Cir. 1978); *Bottone*, 365 F.2d at 393. If the prosecution thus can prove that the thief sold the data for $5000 or more, or sought to extort $5000 or more from the owner to return the data, the dollar amount will be satisfied.

141 17 U.S.C. § 506(a)(1)(A) (2012).

The proposed statute is not intended to apply only to profit-making organizations and thus avoids the word "commercial" in describing the information taken. It can therefore cover records of a nonprofit as well as sensitive customer or patient information.

B. Application of the Proposed Statute

How would our previous cases fare under this proposal? The defendant in *Citrin* might be convicted if the prosecution could prove that, in addition to deleting the data he had collected on the hard drive that he returned, Citrin also kept a copy for himself.[142] That is certainly a likely scenario. By keeping the information, thereby depriving his former employer of it, he gave himself a jump on properties to consider. The information had clear value, and Citrin's reason for taking it was for his own financial gain at the expense of his former employer.[143] It is unclear how the *Brekka* case would come out based upon what is known.[144] What was Brekka's purpose when he emailed the information to his personal email account? If it was to continue working for the benefit of his principal, there is no crime under this statute. If, however, his purpose was to get a negotiating advantage in his attempt to buy an interest in the company, or a competitive advantage if he were planning to leave, the statute would cover his conduct. The result in *John* would be the same. John was convicted under the current statute.[145] John was stealing the data, not using it for any company purpose. He would be convicted under this proposal for stealing the data for private financial gain.[146] The defendants in *Rodriguez* and *Valle* might not be prosecutable under this law.[147] It is not clear that their purpose was to steal the information.[148] If they were not carrying the information away, but using it to harass women (*Rodriguez*), or to

142 *Cf.* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006) (describing Citrin deleting the laptop's data).

143 *Id.*

144 *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129–30, 1132–33 (9th Cir. 2009).

145 *See* United States v. John, 597 F.3d 263, 281 (5th Cir. 2010).

146 *Id.* at 272.

147 *See* United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

148 For federal government employees, 26 U.S.C. § 7213(a)(1) (2012) makes it criminal to disclose tax returns and tax return information, which includes the "taxpayer's identity" as well as information about "the nature, source, or amount of . . . income." 26 U.S.C. § 6103(b)(2)(A) (2012). Federal employees are also subject to criminal prosecution for disclosing the social security number of anyone. 42 U.S.C. § 408(a)(8) (2012). Finally, 26 U.S.C. § 7213A(a)(1) (2012) makes it a crime for any government employee to inspect any tax return or tax return information outside the scope of his or her duties. Disclosure is not an element of this last crime. *Id.*

engage in flights of fantasy (*Valle*), they might not be prosecutable, even if the information stolen is sensitive, nonpublic business information. The result for all defendants in *Nosal I* would be different.[149] They planned and executed a scheme to steal information from Korn/Ferry.[150] The information has value and their purpose was their own financial gain.[151] They therefore could be prosecuted under this proposal.

There are, of course, difficulties with this statute. Proving intent to steal may not always be easy. However, proving intent is what prosecutors do regularly. It is something we ask a jury to infer from the surrounding circumstances. If a person is caught inside a closed office building at 1:00 AM with gloves, a flashlight, screw drivers, and lock picks, a prosecutor will be able to convict the intruder of burglary, even if he had not yet succeeded in taking anything. Unlike the interrupted burglar case, for prosecutions under this statute, the government will be able to prove that the data have been moved. The hard factual question will come in cases such as *Brekka*, *Rodriguez*, and *Valle* regarding their purpose in accessing and removing the data.

The hypothetical marchers in the "parade of horribles" in *Nosal I* could not be charged. Playing online games, chatting online, checking the weather, or tending one's Farmville stable do not involve stealing information.[152] None of them would be in danger if this law were adopted.

Conclusion

The statute has the benefit of bringing our moral common sense to bear on these situations. John and Nosal ought to be convicted of stealing. We all know that stealing is wrong. There is nothing about it that is esoteric or dependent upon knowledge of computers or of the law of agency. The proposal goes back to physical world concepts that many have employed for centuries—stealing (removing) information. True, the idea of information being subject to theft may be relatively new, but it is an easy concept to understand.

---

149 *Cf. Nosal I*, 676 F.3d 854, 863–64 (9th Cir. 2012) (en banc).

150 *Id.* at 856.

151 *Id.*

152 Of course, none of these hypotheticals ever resulted in a real prosecution. The only case that comes close is *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). *Drew* involved a woman who used a false MySpace account to drive a teenage girl to suicide. *Id.* at 452. There was no other statute with which she could be charged, so the prosecutors brought this unsuccessful case. In the absence of this once-in-a-century type of fact pattern, however, prosecutors do not bring "silly" cases.

In addition to clarity, the proposed statute has a clear intent requirement. It requires the prosecution prove a malicious intent beyond a reasonable doubt. This protects employees against employers seeking a vengeful way to get rid of an employee whose conduct was not done with any criminal intent.

There may come a time when the country has a consensus about fair use of business computers and business data. Until then, however, important, confidential business data needs to be protected. This proposal will do that.[153]

153 It will also serve as a statement of positive law on the norms of the internet, advancing the development of this new area of the law.