The Business, Entrepreneurship & Tax Law Review

Volume 1
Issue 1 *Spring 2017*

Article 9

2017

Netflix and No Chill: The Criminal Ramification of Password Sharing

Benjamin Kweskin

NETFLIX AND NO CHILL: THE CRIMINAL RAMIFICATION OF PASSWORD SHARING

Benjamin Kweskin*

United States v. Nosal

I. INTRODUCTION

If I share my Netflix password, am I breaking the law? An act of Congress, passed in 1984, could be the most important law on the books to help answer that question. Ironically, most major companies that can benefit from the law did not exist at the time of its passage, like Netflix, Spotify, and Facebook. The early 1980s gave techies the floppy diskette,[1] the Apple Macintosh,[2] and the founding of Dell.[3] Today, Netflix exists mostly in the cloud instead of in actual computers at a centralized location,

* B.A. Political Science & Government, Washington University in St. Louis, 2015. J.D. Candidate, University of Missouri School of Law, 2018. Associate Member, Business, Entrepreneurship & Tax Law Review, 2016-2017. Special thanks to Note and Comment Editor; Jennifer E. Bennett, and Professor; Bradley M. Desnoyer for their work on this article. I could not have done it without you two. This article is dedicated to Kilian for her support throughout the writing process.

[1] *R.I.P. Floppy Disc*, BBC NEWS (Apr. 1, 2003), http://news.bbc.co.uk/2/hi/uk_news/2905953.stm.

[2] David Pierce, *The Mac Turns 30: A Visual History* (Jan. 24, 2014), http://www.theverge.com/2014/1/24/5340320/the-mac-turns-30-a-visual-history.

[3] *Our History*, DELL, http://www.dell.com/learn/us/en/ph/our-history (last visited June 19, 2017).

as tech companies did in the 1980s. The changing innovations in computer technology and the usage of computers since the 80s will test the bounds of some United States tech laws.

In July 2016, the Ninth Circuit Court of Appeals ruled on *U.S. v. Nosal*, a case that could open the floodgates for criminalizing password-sharing. Perhaps the Ninth Circuit, more than any other circuit, has a special interest in protecting internet companies from password-sharing. The Court has jurisdiction over California, specifically Silicon Valley, the epicenter of technology and internet innovation. The decision in *Nosal* breaks new ground for internet litigation in Silicon Valley and has the potential to protect internet companies in ways that terms of service agreements cannot. However, in order to make the biggest gains for internet companies, CFAA would have to be amended to exclude the word "computer."

II. BACKGROUND OF THE CFAA

The Computer Fraud and Abuse Act ("CFAA") may see more action over the next decade than it has over the past three as internet companies try to defend themselves against password sharing between members, people who pay for the product, and guests, who obtain

passwords without paying for the product. CFAA presents two issues for future courts to address. The first issue is what does "without authorization"[4] means. The second issue, which will be more important for future courts, is the definition of a computer.[5] Courts have spent a considerable amount of time and resources answering the first question, but there has been little discussion on the second.

The CFAA 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 . . . shall be punished."[6] Put another way, "[t]he CFAA imposes criminal penalties on 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 [from a computer].'"[7]

[4] 18 U.S.C. § 1030 (2012).
[5] *Id.*
[6] Nosal v. U.S., 844 F.3d 1024, 1024 (9th Cir. 2016) (quoting 18 U.S.C. § 1030 (2008).
[7] *Id.* at 1024 (citing 18 U.S.C. § 1030 (2012)) (emphasis original).

Originally, the 1984 CFAA targeted "hackers who accessed computers to steal information or to disrupt or destroy computer functionality."[8] The act was amended in 1986 to deter and protect against certain high-tech crimes or against a scheme to defraud.[9] The act does not define what "without authorization" means.[10] If "without authorization" means "without consent," then criminal liability will expand to anyone who, in any way, exceeds the bounds of their contracted use. If "without authorization" means "a substantial breach of pre-existing authorization," criminal liability will contract.

To respond to the first problem, two questions naturally arise: do members exceed their authorized access by password sharing? Are guests unauthorized? Both of these questions are briefly addressed in the CFAA,[11] but neither the statute nor case law has provided a clear answer. Orin Kerr, perhaps, best summarizes unauthorized access in his 2015 article calling it "norms-driven."[12] He explained that computer laws

[8] *Id.* at 1032 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129(9th Cir. 2009).
[9] *Id.* (quoting S. REP. 99-432 at 4(1986)).
[10] *Id.* at 1033.
[11] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190 (1984).
[12] Orin Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1154 (2016).

should parallel trespass laws in terms of unauthorized access.[13] Since the publication of his article, *U.S. v. Nosal* was decided, which muddied an attempt to clearly define unauthorized access.

Finally, *LVRC Holdings LLC v. Brekka*[14] outlined the limitations of CFAA in 2009 for the Ninth Circuit. *Brekka* involved a former employee, his wife, and two consulting businesses.[15] Mr. Brekka, Defendant, emailed documents from his work email to his own personal computer, and to his wife's.[16] After his employment terminated, Mr. Brekka was still able to log onto the LVRC website.[17] LVRC sued Mr. Brekka for violating CFAA.[18] In order to violate CFAA, Mr. Brekka must be shown to have,

> (1) accessed a protected computer, (2) without authorization or exceeding such authorization that was granted, (3) knowingly and with intent to defraud, and thereby (4) furthered the intended fraud and obtained anything of value causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value.[19]

[13] *Id.* at 1146-47.
[14] LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).
[15] *Id.* at 1128.
[16] *Id.* at 1129-30.
[17] *Id.* at 1130.
[18] *Id.*
[19] *Id.* at 1132.

The court first addressed what "without authorization" meant.[20] They concluded that, "[n]o language in the CFAA supports LVRC's argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest."[21] In other words, access must be unequivocally revoked in order to meet this element. In *Brekka*, Plaintiff failed to show this element.[22]

The court next addressed the lack of evidence that Mr. Brekka, in fact, logged into LVRC's computer after his employment was terminated.[23] This issue need not be addressed in this paper, as lack of evidence was not an issue discussed in *Nosal*.[24]

III. THE INSTANT DECISION

Nosal extends *Brekka* by defining the boundaries of CFAA with regard to password sharing. In *Nosal*, the court focused heavily on whether this access "exceeds authorization" under CFAA.[25] However, the court neglected to distinguish the legal difference between unauthorized

[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *See generally* U.S. v. Nosal, 844 F.3d 1024 (9th Cir. 2016).
[25] *Id.*

access to a *computer* and unauthorized access to a *website*.[26] This omission will test our legal system as future cases wrestle with the legal limits of password sharing. Until tech companies lobby for an amendment to the CFAA to include the cloud, it will be hard to argue that there is unauthorized access to a *computer*.

IV. FACTS AND HOLDING

In *Nosal*, a former employee of a company accessed that company's computers after his termination.[27] While employed, Defendant was given a password.[28] His credentials, however, were revoked after his termination.[29] The employee disregarded the revocation and accessed the computers through the passwords he had obtained.[30] Beyond the employee's own personal access, he also gave passwords to the company's computers to other non-employees.[31] Those other individuals had been competing for business against LVRC.[32] The non-employees

[26] *Id.*
[27] *Id.* at 1029.
[28] *Id.* at 1031.
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*

then downloaded trade secrets from the computer.[33] A dispute arose over what "without authorization" meant in the confines of CFAA.[34] The Court concluded,"'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected *computer* without permission."[35]

Further, access restrictions and use restrictions are distinct. The court reasoned that the "'exceeds authorized access' prong of § 1030(a)(4) of the CFAA 'does not extend to violations of [a company's] use restrictions.'"[36] In other words, the court distinguished between the amount of information accessed and the amount of information obtained. Once the information is obtained, its use is outside CFAA.[37] [38]

To address some of the criticism from amici briefs of the criminalization of password sharing, the court turns to password sharing. The Court dismissed concerns about password sharing by stating, "this appeal is not about password sharing. Nor is it about violating a company's

[33] *Id.*
[34] *Id.* at at 1033.
[35] *Id.* at 1028 (emphasis added).
[36] *Id.* at 1029 (citing U.S. v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012)).
[37] *Id.*
[38] *Id.* The Court then addressed other counts relating to corporate espionage. Those issues will not be discussed in this article.

internal computer-use policies."[39] The majority criticized dissenting opinions that "spin hypotheticals about the dire consequences of criminalizing password sharing."[40] The majority does not further address the issue of password sharing as it relates to the Defendant's actions.

Instead of making password sharing the central issue, "the conduct at issue is that of Nosal and his co-conspirators, which is covered by the plain language of the statute."[41] But the Court defines said conduct as, "conspiring with former [company] employees whose user accounts had been terminated, but who nonetheless accessed . . . a proprietary database through the back door when the front door had been firmly closed."[42] Defendant "blatantly circumvented the affirmative revocation of his computer system access."[43] In other words, because Nosal went so far beyond his access formerly permitted by his employer, there could be no question of exceeding authorized access. The court does not help determine how excessive the violation of authorization was.

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*

At this point, the majority blurs the line between a "database" and a "computer system."[44] The court does not address which moment defined the prohibited conduct in CFAA: accessing the *computer system* or accessing the *database*. In *Nosal*, both issues were created because of password sharing.[45] The difference between a computer system and a database is significant.

When accessing a computer or a computer system, the implication is that there is a physical computer with information stored to it. In 1984 and 1986, there was little question about what constituted a computer. Telephones were not computers. Televisions were not computers. Video-game consoles were not computers. Today, that question is much more confusing, as the technology in an average smartphone contains far-superior computing power than almost any 1986 computer.[46] As this

[44] *Id.*
[45] *See generally id.*
[46] *Compare iPhone Models*, APPLE, http://www.apple.com/iphone/compare/ (last visited June 19, 2017). Today's iPhones have finger print sensors, 2gb of RAM, and a minimum of 16gb of storage. *Product Fact Shee*t, IBM, https://www-03.ibm.com/ibm/history/exhibits/pc25/pc25_fact.html (last visited June 19, 2017). The IBM AT was largely seen as the "best" computer of the early 1980's. Its specs included the inferior 40K ROM (equivalent to today's RAM), and up to 160kb of user storage per disc. It weighed 17 pounds. *Id.*

article will later discuss, the difference is a fact-specific one, the liberalness of construing what a computer is will expand criminal liability.

V. COMMENT

A. *Problems with the Majority Opinion*

The majority too quickly dismisses password sharing. It states that the problem is the *access*, not the fact that passwords were shared.[47] The majority opinion offers no help in describing the role password sharing played in violating CFAA. The court explains that *LVRC Holdings LLC v. Brekka*[48] and *Nosal* are substantially similar.[49] Both cases involved an individual who had gained unauthorized access to a computer.[50] However, *Brekka* did not address password sharing.[51] Had passwords not been shared in *Nosal*, there would have been no unauthorized access gained. The majority wants to distinguish the fact that passwords were shared with the fact that passwords were used.[52]

The majority's argument on this point is purely semantic. If A gives a key to a protected vault to person B, an unauthorized entrant, and

[47] *Nosal*, 844 F.3d at 1029.
[48] LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).
[49] *Nosal*, 844 F.3d at 1029.
[50] *Id.*
[51] *Id.*
[52] *See generally id.*

B gets into the vault, both A and B have committed a crime. A has exceeded his authorized access, by sharing the key, and B has gained unauthorized access, by using the key. The majority argues that simply telling another person your password to an unauthorized computer does not violate CFAA.[53] But the implication behind password sharing is that the password is shared so that it can be used. Sharing the key alone carries no crime, but as soon as the key is used, the access is unauthorized.

The moment CFAA was violated does not change whether *Nosal* has to do with password sharing. In fact, password sharing is at the heart of the case. The majority even recounts that "password sharing was prohibited by a confidentiality agreement that [Company] required each new employee to sign."[54] Still, the Court concluded that *Nosal* is not about password sharing.[55] Thus, the breach of that agreement, or the use of password sharing, set Nosal's criminal liability in motion. In *Nosal*, password sharing and unauthorized access are intimately connected and dismissing them in one sentence does not help outline potential criminal

[53] *Id.*
[54] *Id.* at 1031.
[55] *Id.* at 1029.

liability in password sharing. In fact, the Court opens the door for this issue for future cases.

B. *Problems with the Dissent*

The dissent fears the criminalization of "consensual password sharing."[56] In other words, the majority glosses over how it distinguishes *Nosal*'s facts from consensual password sharing.[57] The dissenting justice notes, "[p]eople frequently share their passwords, notwithstanding the fact that websites and employers have policies prohibiting it."[58] He continues by saying that the CFAA does not make the millions of people who password share into federal criminals even though the majority may think so.[59] In the original appeal of Mr. Nosal's conduct, *Nosal I*, the Court had rejected turning the CFAA into a "sweeping Internet-policing mandate" instead of maintaining its "focus on hacking."[60] CFAA was never meant to police the Internet; instead, CFAA was intended to stop hackers from taking information from computers.[61] Both the Second Circuit and the

[56] *Id.* at 1031.
[57] *Id.* at 1049 (Reinhardt, J., dissenting).
[58] *Id.*
[59] *Id.* at 1048 (Reinhardt, J., dissenting).
[60] *Id.*
[61] *Id.*

Fourth Circuit have agreed with the *Nosal* dissent on this point.[62] Extending the CFAA to non-hacking has a major impact, which the dissent rightly fears.[63]

However, the dissent has its shortfall because it misunderstands "authorized access," which implies non-consent. The dissent notes, "The majority does not provide . . . a workable line which separates the consensual password sharing in this case from the consensual password sharing of millions of legitimate account holders, which may also be contrary to the policies of system owners."[64] The dissent focuses on the norms of computer and Internet use.[65] This line of logic does not disprove the majority's point on its own. The court had the power to criminalize Nosal's behavior because his acts were without consent because his credentials had been revoked.[66]

This point is where a company, like Netflix, should be on high alert. Netflix's Terms of Service are unequivocal:

[62] *Id.* at 1048-49. (quoting U.S. v. Valle, 807 F.3d 508, 526–28 (2d Cir. 2015)); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012)).
[63] *Id.* at 1049.
[64] *Id.*
[65] *Id.*
[66] *Id.* at 1038.

> Netflix grants you (which, for purposes of this License Agreement, shall include members of your immediate household for whom you will be responsible hereunder and users of the Netflix ready device with which you are accessing the Netflix service and for whom you will be responsible hereunder) a . . . non-transferable license.[67]

Netflix users who share their password, the dissent would argue, engage in a harmless and ubiquitous act.[68] This harmless and ubiquitous act should not be criminalized simply because millions of people engage in this behavior. The dissenting justice calls this "consensual password sharing."[69] Instead of calling it consensual, I will refer to this password sharing as normal password sharing because consensual cannot be unauthorized by definition. However, normal password sharing could be unauthorized explicitly by contract.

According to the dissent, normal password sharing is not criminalized under the CFAA because society expects it.[70] In this respect, technology law can be similarly viewed with property law. As is the case with implied easements, after a certain amount of time, a normal trespass

[67] NETLIX END USER AGREEMENT, https://help.netflix.com/legal/eula?locale=en (last visited Apr. 11, 2017).
[68] Nosal v. U.S. 844 F.3d 1024, 1048 (9th Cir. 2016).
[69] *Id.* at 1049.
[70] *Id.*

can, and should, become legal.[71] When there is enough password-sharing that a company should be aware of the activity, but does nothing, there should be a pseudo-implied easement.[72] The problem is that none of the facts in *Nosal* suggest that Nosal's access to the computers at his former company was consented to either explicitly or impliedly.

Ultimately, although the dissent is rooted in better logic than the majority, and will eventually be on the right side of history as a matter of policy, it misses the mark in the instant case. The dissent's fears are valid, but the law is clear.

C. *Why the Majority Got It Right for the Wrong Reasons and the Dissent Got It Wrong for the Right Reasons*

In the instant case, Nosal exceeded authorized access to a computer by using and distributing passwords beyond his own eligibility.[73] The majority, seeing the fear that millions of consensual password sharers would have, tried to brush aside password sharing and hastily swept the issue aside.[74] But, whether the majority wants to admit it or not, the instant case revolves around the fact that passwords were

[71] RESTATEMENT (THIRD) OF PROP.: SERVITUDES § 2.1 (AM. L. INST. 2016).
[72] Kerr, *supra* note 13, at 1151-52 (calling this phenomenon an implied license).
[73] *Nosal*, 844 F.3d at 1029.
[74] *See generally id.*

shared which led to unauthorized access to a computer.[75] The password sharing alone was not enough to create criminal liability. The subsequent use of those passwords created criminal liability. Thus, Nosal did violate the CFAA. The majority needs to clarify that password sharing, followed by the *use* of the shared password, is a criminal act in the Ninth Circuit. The majority was quick to dismiss a multitude of amicus briefs,[76] but the court followed the law to its logical conclusion: password sharing can be criminal if the sharer exceeded authorized access.[77]

The majority made the right decision because password sharing is one method of obtaining unauthorized access to a computer. An individual or companies gains information from a computer that they could not have otherwise had through exceeding authorized access or, similarly, through means that were not authorized at all. Nosal did access a computer without authorization, or his authorization had effectively expired, and stole information to the computer owner's detriment.[78] Had the majority stopped here, they probably could have won over the dissent. The majority

[75] *Id.* at 1029.
[76] *Id.*
[77] *Id.*
[78] *Id.* at 1029.

opened the door for new litigation because they stated, "Nosal is charged with unauthorized access—getting into the computer after categorically being barred from entry."[79] However, everyone who does not buy a membership to a website is categorically barred from entry.[80] If they obtain the benefits of membership to the website, they have exceeded authorized access. The court found that Nosal had unauthorized access and proceeded to share that access.[81] Nosal committed a crime on two fronts, under the law.

Yet, even though the dissenting judge comes to the wrong outcome, he does so for a very good reason. The judge is reasonable to fear the criminalization of millions of harmless and ubiquitous acts.[82] However, this concern is not critical to the issue at hand. Nosal stole trade secrets from a company.[83] This type of behavior is exactly what CFAA was trying to protect against.[84] When a person checks their personal email at work, which may technically exceed the granted authorization from a

[79] *Id.* at 1034.
[80] NETFLIX TERMS OF USE (2016) ("[T]he Account Owner should not reveal the password to anyone").
[81] *Nosal*, 844 F.3d at 1036.
[82] *Id.* at 1048-49 (Reinhardt, J. dissenting).
[83] *Id.* at 1029.
[84] *Id.* at 1032.

computer's owner, they are not accessing information specific to the owner.

By looking back at the 1984 legislation, this is a simple logical link as the Internet was in its infant stage. In 1984, computers had files on them that needed to be protected. Today, those files could exist in cyberspace or the cloud. The 1984 Congress, if reexamining the issue today, should have no trouble distinguishing stealing trade secrets from harmlessly checking email. But, even if this logic is unconvincing, the text of CFAA provides the mens rea terms "knowingly and with intent to defraud."[85] A person cannot both ubiquitously share their password yet possess the intent to defraud.[86] The courts could not reasonably interpret the statute as criminalizing an act that countless people engage in.

The mens rea standard in CFAA makes criminalizing password sharing a bit easier to swallow. When a person checks his or her personal email on a work computer, and a company policy forbids it, they do not intend to defraud the company because their behavior is seemingly

[85] 18 U.S.C. § 1030 (2012).

[86] *Fraud*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("A knowing misrepresentation or knowing concealment of a material fact made to induce another to act to his or her detriment. • Fraud is usu[ally] a tort, but in some cases [esp[ecially] when the conduct is willful] it may be a crime").

harmless. Two people, using a single account, do not cause a great deal of harm to a company like Netflix. By contrast, if a person intentionally puts a worm or a virus onto a computer, it can be said that they are defrauding the company by abusing their authorized access.

Further, many of the dissent's concerns could be quelled if sharing a password to a website is probably not covered by CFAA. As previously mentioned, CFAA is explicit in its use of the word computer,[87] which is now antiquated. The dissent is quick to note that point.[88]

"A protected computer is defined as a computer affected by or involved in interstate commerce—effectively all computers with Internet access . . . nearly all desktops, laptops, servers, smart-phones, as well as any iPad, Kindle, Nook, X-box, [and] Blu-Ray player."[89] What a computer means will be addressed in section V. However, it is important to note that CFAA does have its limits. By explicitly stating computer, CFAA might not include servers or other massive data storage systems on its face.

[87] 18 U.S.C. § 1030 (2012).
[88] *Nosal*, 844 F.3d 1024 at 1050.
[89] *Id.* (internal citations omitted).

Specifically, CFAA does not pertain to the cloud[90] on its face. It would seem that password sharing on Netflix[91] is probably not covered by CFAA; however, the framework exists for criminal liability.

VI. Redefining and Changing Essential Terms in CFAA

The courts cannot get around the fact that the law says "computers."[92] A narrow interpretation of computer would suggest that this means a physical, technological device, the primary function of which is to keep and store digital data. A broader view could make the argument for other devices to count as computers. Tablets could certainly qualify as a computer because of their computational power as well as functionality. However, courts cannot evade the fact that a computer is a physical device. Thus, a website is not a computer. An issue arises below the surface. Although websites are not themselves computers, they are backed by computers on the ground. Because of the nature of the cloud, an

[90] The Cloud is a series of interconnected servers that hold digital data which can be accessed wirelessly. Jess Fee, *The Beginner's Guide to the Cloud*, MASHABLE, (Aug. 26, 2013), http://mashable.com/2013/08/26/what-is-the-cloud/#lyMN6qjsvkqA.
[91] Whose movies stream from the cloud.
[92] *Nosal*, 844 F.3d at 1033-34.

interconnected system of computers, once information is accessed on a website, access to its storage system is also gained.[93]

Thus, a website can be so closely tied to database, that they can be seen as one and the same. If access to information is like entering a house,[94] the website is the front door. A website allows the individual to access stored information too great for the website alone to handle. Thus, websites necessarily link back to other computers that actually store the data.

Additionally, the cloud makes it fairly easy to view websites as databases. Dropbox,[95] Spotify,[96] and Netflix[97] are all databases. Dropbox holds digital data. Spotify is a database for music. Netflix is a database for movies. Thus, the distinction between computer systems and databases may seem unimportant when regulating rudimentary access to websites, but can be the difference between criminality and contract liability in

[93] Jess Fee, *The Beginner's Guide to the Cloud*, MASHABLE (Aug. 26, 2013), http://mashable.com/2013/08/26/what-is-the-cloud/#lyMN6qjsvkqA.
[94] Kerr, *supra* note 13, at 1148.
[95] *What's Dropbox?*, DROPBOX, https://www.dropbox.com/tour/1 (last visited June 19, 2017).
[96] John Pullen, *Everything You Need to Know About Spotify*, TIME (June 3, 2015), http://time.com/3906839/spotify-tips/.
[97] Andrew Lampitt, *Big Movies, Big Data: Netflix Embraces NoSQL in the Cloud*, INFOWORLD: BIG DATA (May, 2, 2015), http://www.infoworld.com/article/2614318/big-data/big-movies--big-data--netflix-embraces-nosql-in-the-cloud.html.

password sharing for websites. Contract liability will be discussed more fully in the conclusion. For now, it is important to note that violating a contract, by exceeding its terms, can lead to liability.

If the courts automatically interpret unauthorized access to a website to mean unauthorized access to a database, there are serious ramifications for Netflix and its users. A website alone is not a database, but it is connected to one. Thus, in order to gain "anything of value,"[98] the final element of the CFAA necessitates access to a database, thus computers. Tricking a website into giving access to a database would create liability under CFAA. Before any cases can move forward, Congress should seriously consider the definition of a computer, what unauthorized access means, and what "anything of value" means.

Redefining computer so that it best fits for the modern age is important, but not essential for violations under the CFAA. As it sits, the CFAA could easily be construed to mean that every time a person accesses a website to view a file, listen to music, or watch a movie without authorization, they have committed a federal crime no matter what the

[98] 18 U.S.C. § 1030 (2012).

medium. Hackers can target cell phones, Xboxes, and even thermostats.[99] Accessing a video game system and accessing a corporate computer should not be treated as equals under criminal law. Accessing a video game in order to play it for free carries a minimal impact when compared to accessing a corporation's secret files. By outlining the parameters of a computer, exactly what kind of unauthorized access is worthy of criminal liability will become clear.

The best approach would be abandoning CFAA because its original intent has been lost. Instead of hacking, any kind of intended unauthorized access to a database exposes criminal liability. In 1984, the only way to hack digital information was through a physical computer, and all computers were fundamentally similar.[100] Obviously, the damage that a hacker can do to a digital thermostat is different than the damage they can do by hacking a corporate computer. On the one hand, the hacker can gain sensitive information about individuals and corporate secrets, while on the other, he or she can ruin an electric bill. Further, access to a

[99] *Id.*
[100] By comparison to a cellphone, a video game console, a laptop, and a thermostat in 2016.

website[101] can lead to unauthorized access to movies or music, which have a relatively small devastating effect on society. It would be prudent for Congress to give a clearer meaning to, or change, the phrase "anything of value" as it is used in CFAA. Redefining "anything of value" would help ease the dissent's concerns in *Nosal* because Congress could be explicit in prohibiting the societally harmful behaviors associated with hacking. Netflix has made "anything of value" more tangible under the CFAA. In November 2016, Netflix announced that it would allow members to download movies.[102] Being able to download movies will make a more tangible economic harm to tie liability to.

The unauthorized access issue is still a problem, but changing what a computer means as well as rephrasing "anything of value" would help future courts understand the bounds of unauthorized access. Congress could simply clarify that unauthorized access" means access that either exceeds express or implied authorization to satisfy the concerns of normal password sharing the dissent focused on.

[101] And, necessarily, a computer or database.
[102] Chris Welch, *Netflix Finally Lets You Download Shows and Movies to Watch Offline*, THE VERGE (Nov. 30, 2016), http://www.theverge.com/2016/11/30/13792376/netflix-offline-downloads-now-available.

VII. FUTURE PROBLEMS WITH PASSWORD SHARING

There still may be one issue in CFAA that will prevent liability. CFAA includes a mens rea element. Neither the majority nor the dissent in *Nosal* brought up the mens rea issue. As Orin Kerr correctly observed, "computer trespass statutes generally require that the user commit an intentional or knowing unauthorized access."[103] Criminal liability under CFAA requires a hacker "intentionally access a computer without authorization" or intentionally "exceeding authorized access."[104] As it is the government's job to prove mens rea, this is a serious limitation to actual convictions.

The mens rea requirement, with respect to lack of authorization, could mean the intent to access the computer or the intent to access the information creates criminal liability. This difference is important, but still remains an unanswered question through *Nosal*. If the element of exceeding authorized access is met simply at the moment the computer was logged into, then the first element is automatic. It is impossible to gain information from a computer without accessing it. If the second

[103] Kerr, *supra* note 13, at 1180.
[104] 18 U.S.C. § 1030 (2012).

interpretation is true, that the element is met when the hacker obtains the data, the flow of logic is more clear. The elements could be sorted as follows: (1) an unauthorized person; (2) intentionally; (3) gains access to anything of value; (4) on a targeted computer.

By organizing the elements in this way, courts have a clearer understanding of what constitutes a crime under CFAA. The *Nosal* majority focused heavily on the fact that a computer was accessed without authorization at the initial login.[105] This is a problem because the element is automatic, and the authors of the CFAA probably did not intend such an interpretation because their focus was on hacking.[106] The fact that a computer was accessed is not the problem. The information accessed is the problem. The fact that the information was on a computer should be an additional step. This step is important when two actors are in play.

Password sharing is a unique issue because it requires two actors: the person who accesses the information, and the sharer. Sharing your password and logging on could easily be seen as trespassing on Netflix's website to provide you with content you should have otherwise paid for,

[105] Nosal v. U.S., 844 F.3d 1024, 1038 (9th Cir. 2016).
[106] *Id.* at 1049.

thus it has value. All other elements aside, the question of whether or not the sharer of information could be criminally liable remains unanswered. Under *Nosal*, there is strong evidence to suggest liability. It is clear that the person who accesses this information is liable, but what about the password sharer?

The *Nosal* majority's focus was on the fact that Nosal himself exceeded his authorized access to a computer.[107] But if Nosal had not accessed the computer personally, and had only given the information to other people, the current holding may create criminal liability. If I were a prosecutor, and Nosal had not personally accessed the information, I would argue that Nosal is still liable under the theory that "exceeds authorized access" means that Nosal simply had to go beyond the limits of his authority in the process of accessing a computer's valuable information. Nosal's agents accessed the information.[108] He did that by handing over passwords to other people, enabling their unauthorized access, and exceeding his own authorized access.[109] Nosal does not personally have to gain the access to the computer itself under this theory,

[107] *Id.* at 1032.
[108] *Id.* at 1034.
[109] *Id.* at 1037.

just the data. As I noted above, the real crime cannot come at the moment that the computer itself was breached, it has to come once the valuable information was obtained. Thus, Nosal, a person who exceeded his authority, and thus is unauthorized, intentionally gained access to information that was contained on a computer.

Now, the dissent's concerns should be ringing out. If all password sharing is criminalized, then millions of people who share their passwords are criminally liable.[110] At face value, this is true. When a Netflix password is shared to a person that does not live in the same household as the member, he or she is a criminal under CFAA. The hacker has knowingly taken unauthorized access to something of value, such as movie rentals, from a computer, through Netflix's website, and thus the servers it runs on, which are computers. Further, as explained previously, the sharer of the password is also criminally liable. So, sharing a password to a website can trigger criminal liability under CFAA. Opponents to *Nosal*'s interpretation of CFAA would most likely prefer that the act clarify that the accessed computer was targeted. Thus, someone specifically gained unauthorized access to a single computer that

[110] *Id.* at 1048 (Reinhardt, J., dissenting).

contained information of value because that targeted computer contained something of value. But even with this change, "something of value" is so vague that virtually any access to any one computer could be seen as valuable, which millions of people do.

Societal norms must be taken into consideration when evaluating criminal liability under CFAA. The dissent correctly notes that in the past, the Ninth Circuit "emphatically refused to turn violations of use restrictions imposed by employers or websites into crimes under the CFAA, declining to put so many citizens at the mercy of [their] local prosecutor."[111] It is inarguable that many people share passwords regularly. The concerns an employer has in protecting its websites are serious, and some acts can trigger criminal liability under CFAA. However, not all unauthorized access *should* trigger should liability. The dissent notes that these cases would cause the public to be at the mercy of their prosecutor.[112] Even the Huffington Post commented on *Nosal*'s effect on sharing passwords.[113] Ultimately, the article concluded that it would be

[111] *Id.* (internal citations omitted).
[112] *Id.*
[113] David Moye, *It's Probably OK To Share Netflix Passwords (For Now)*, HUFFINGTON POST (July 11, 2016), http://www.huffingtonpost.com/entry/share-netflix-

unreasonable for Netflix or similar carriers to seek criminal action against users who share their passwords.[114] Punishment for such a crime would be arbitrarily given.

The immediate decision does not take into consideration societal norms. Although there are no estimates as to how many people actually share their passwords and account information, an outbreak exists. The dissent suggests that "millions"[115] of people share passwords, which is a safe estimate. Assuming that estimate is accurate, it seems implausible for a company to not know that password sharing exists. In January 2016, the CEO of Netflix went so far as to say he had no problem with password sharing.[116] When the CEO admits that he sees no problem, the password sharing is normal because it happens so frequently. Netflix's stock has been soaring over the last five years. Shares of Netflix stock closed 2011 at $9.90.[117] On October 28th, 2016, the stock opened just shy of $127.[118] If

password_us_57842235e4b0e05f05232f67.
[114] *Id*.
[115] *Nosal*, 844 F.3d at 1048 (Reinhardt, J., dissenting).
[116] Moye, *supra* note 113.
[117] *Netflix, Inc. (NFLX)*, YAHOO FINANCE (Nov.16, 2016), http://finance.yahoo.com/quote/NFLX?p=NFLX.
[118] *Id*.

password sharing is hurting Netflix, the stock price certainly does not reflect the pain.

But even if password sharing is stunting Netflix's growth, the act should not be criminal for efficiency purposes. Password sharing should be viewed in light of a contract dispute, not as criminal liability. This is because a contract dispute resolves in putting the injured party in the position they would be if the contract had been fully performed or had the contract never been entered into.[119] When a member of Netflix goes beyond her license, she is in breach. Netflix can seek remedies that would compensate for its economic loss. Contract law would increase efficiency for Netflix in this case.

By contrast, criminal law seeks to punish wrongdoers, thus decreasing utility for both parties. Netflix does not benefit from putting its customers in jail. I can't imagine that inmates are allowed their own Netflix accounts. Netflix could lose customers and would create a public relations nightmare. The company could not defend seeking criminal charges against a high volume of customers. Unlike contract, criminal

[119] RESTATEMENT (SECOND) CONTRACTS § 347 (1979).

liability decreases efficiency across the board. From an efficient market prospective, contract remedies make the most sense.

VIII. CONCLUSION

Although the facts in *Nosal* were substantially dissimilar to normal password sharing, the Ninth Circuit will continue to be challenged by cases that inch closer to normal password sharing. The majority was correct in the instant case, but their correct decision rightfully creates worry and shows a deeper problem in the congressional act. There could be millions of criminals at large for engaging in a ubiquitous activity. Further, contract law solves the problem more efficiently than criminal law. Criminal liability turns on what a company authorizes to its members. Thus, activity on one website (with a well crafted Terms of Service Agreement) could create criminal liability, where another website (with a poorly crafter Terms of Service Agreement) would not. There is no universal standard for criminal liability. As the elements sit from the *Nosal* decision, it is hard to believe that password sharing escapes criminal liability under CFAA at face value limited only by arbitrary distinctions between Terms of Service Agreements.