BREAKING INTO AN EMPTY HOUSE: A THEORY OF REMEDIES FOR CFAA UNAUTHORIZED ACCESS TO NON-PROPRIETARY INFORMATION

Omri Rachum-Twaig[*] *& Ohad Somech*[**]

I. INTRODUCTION

In two appeals to the Court of Appeals for the Ninth Circuit,[1] the court was requested to calibrate and clarify the scope of the Computer Fraud and Abuse Act's (CFAA) unauthorized access to computers doctrine.[2] These two cases focus on a recurring set of circumstances that articulates a significant tension between the CFAA unauthorized access doctrine and basic understandings of (lack of) property rights in information.[3] In these types of circumstances, plaintiffs seek to restrict defendants from accessing their computers for the purpose of obtaining non-proprietary information.[4] The reason that the CFAA doctrine is invoked, rather than copyright,

[*] PhD (Law), Buchmann Faculty of Law, Tel Aviv University; Adjunct Professor, Buchmann Faculty of Law, Tel Aviv University.

[**] PhD (Law), Buchmann Faculty of Law, Tel Aviv University; Postdoctoral Fellow, Edmond J. Safra Center for Ethics, Buchmann Faculty of Law, Tel Aviv University. We wish to thank Hanoch Dagan, Omer Pelled and Asaf Wiener for their fruitful comments on an earlier draft of this Article.

[1] *See* Facebook, Inc. v. Power Ventures, Inc., 252 F. Supp. 3d 765, 768 (N.D. Cal. 2017); *rev'd* 844 F.3d 1058, 1062, 1065–66, 1070 (9th Cir. 2016); hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1103 (N.D. Cal. 2017), *appeal docketed,* No. 17-16783 (9th Cir. Sept. 6, 2017).

[2] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012), *amended by* Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168 (2018).

[3] *See Facebook, Inc.*, 252 F. Supp. 3d at 768–69*; hiQ Labs, Inc.*, 273 F. Supp. 3d at 1103.

[4] When we refer to 'computers' in this Article, we mean any type of machine that is used for the storing and processing of electronic information, including, for example, the device on which website pages and databases are stored. The CFAA defines computer as:

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

18 U.S.C. § 1030(e)(1).

trade secrets, or similar property-related doctrines, is that the use or taking of the information, in and of itself, is not legally protected.[5]

This article seeks to explore such tension by reviewing the doctrinal development of both the CFAA's unauthorized access doctrine and the parallel trespass to chattels doctrine, as well as the underlying theoretical justifications for such doctrines. Specifically, we show that much of the tension is manifested in the question of applicable remedies for breach of the CFAA's unauthorized access provisions. This is because some types of remedies may inadvertently create *de facto* property rights in otherwise non-proprietary information.[6] The need to distinguish between remedies for CFAA violations relating to proprietary and non-proprietary information is dictated both by theory and legislative history.[7] The latter specifically mentioned that different types of information require different legal treatment.[8] The above discussion will allow us to highlight some difficulties in current case law and to suggest a taxonomy of the available remedies to plaintiffs in such cases, as well as to offer guidelines for choosing the right remedies model. We believe that such guidelines could be useful in deciding both pending and future cases revolving around such circumstances.

To gain a better understanding of the tension raised in the above circumstances, consider the following typical case: the plaintiff, a major social platform, allows the public to access its computers for the purpose of using the platform.[9] For this purpose, it grants access rights to non-proprietary information stored on these computers.[10] At a certain point, the plaintiff identifies that the defendant, a corporate entity, is accessing the information for the purpose of collecting and then utilizing the information for its own business purposes.[11] In most circumstances, such use of the information is in violation of the plaintiff's terms of use for the platform.[12] Once the plaintiff detects such a violation, it sends the defendant a cease and desist letter or attempts to technologically block the defendant from accessing its computers.[13] If the violation is repeated, the plaintiff

[5] *See* NetApp Inc. v. Nimble Storage Inc., No. 5:13-CV-05058-LHK, 2015 U.S. Dist. LEXIS 11406, at *61 (N.D. Cal. Jan. 29, 2015).
[6] *See hiQ Labs, Inc.*, 273 F. Supp. 3d. at 1116.
[7] *See id.* at 1111.
[8] *See* S. REP. NO. 104-357, at 3–4 (1996).
[9] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1104.
[10] *See id.*
[11] *See id.*
[12] *See id.*
[13] *See id.*

then seeks legal redress.[14] Faced with such cases, the court needs to first decide whether a legal rule was violated, and if so, what the adequate remedy is.[15] If the court decides to grant injunctive relief or disgorgement of profits from the use of such information, this effectively means that a *de facto* property right in the information is granted to the plaintiff, although no such right exists under law.[16] If no remedy is granted at all, however, this effectively undermines the unauthorized access provision with respect to plaintiff's computers.[17]

To properly analyze this tension and suggest valid ways to relieve it, we begin with reviewing existing case law revolving around such circumstances. This review traces back to cases brought not under CFAA doctrine, but rather under the common law trespass to chattels doctrine, which was applied to cyberspace.[18] We show that courts gradually limited this doctrine to a point where it does not provide effective means for plaintiffs to restrict defendants' access to their computers.[19] The case law then progressed to invoking the CFAA unauthorized access doctrine due to the fact that this is a statutory rule tailored to cases of online access to computers.[20]

We show that while the current understanding of what constitutes a violation of the CFAA unauthorized access provision is relatively clear to courts, the question of appropriate remedies for such violations is seldom addressed by courts, and the results are largely inconsistent and varied.[21]

Discussing the underlying theories of such doctrines, we believe, helps to explain both what constitutes violations of the CFAA unauthorized access provision and, more importantly, how the question of remedies should be resolved in various circumstances.

---

[14] *See id.*

[15] *See id.* at 1108.

[16] *See id.* at 1116.

[17] *See id.* at 1113 n.11. ("LinkedIn argues that if it cannot invoke the CFAA to prevent unauthorized access by bots, it may be left open to denial of service attacks.").

[18] *See* Laura Quilter, *Regulating Conduct on the Internet: The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421, 428–430 (2002).

[19] *See* NetApp, Inc. v. Nimble Storage, Inc., No. 5:13-CV-05058-LHK, 2015 U.S. Dist. LEXIS 11406, at *59 (N.D. Cal. Jan. 29, 2015); Quilter, *supra* note 18, at 433.

[20] *See* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 475–76 (2003); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1153 (2016).

[21] *Compare* Facebook, Inc. v. Power Ventures, Inc., 252 F. Supp. 3d 765, 787 (N.D. Cal. 2017) (finding that due to a violation of the CFAA, Facebook is entitled to $79,640.50 in compensatory damages and permanent injunctive relief), *with* Craigslist, Inc. v. RadPad, Inc., No. 3:16-cv-01856-CRB, 2017 U.S. Dist. LEXIS 218351, at *3, *6–7 (N.D. Cal. Apr. 13, 2017) (finding that Radpad had violated the CFAA, yet awarding damages under a different federal statute, copyright infringement, and breach of Craigslist's terms of use).

The crux of the question is the interrelations between rules that protect the property itself and those that protect the boundaries in which property lies. We visit two main theoretical approaches to property in order to extract their application to such rules of boundaries. First, we consider autonomy-based theories that focus on a person's autonomy and ability to exclude others. Second, we discuss economic analysis as a tool to weigh the costs and benefits of boundary rules vis-à-vis the protection of property itself.

Building on these theories, we suggest a novel account of why and how boundaries should be protected regardless of the protection of what lies within them. In this way, we resolve the apparent tension associated with the protection of boundaries even if there is no protected property within them while adding to existing economic literature on the subject and suggesting a new analysis of the matter under autonomy theory.

Using the conclusions from the theoretical discussion, we present a taxonomy of alternative potential remedies for CFAA violations: no remedy for unauthorized access to non-proprietary information, injunctive relief and enforcement costs only, and full restitution and disgorgement of profits. Based on the theoretical conclusions, we suggest guidelines for choosing the right model in different circumstances. We first suggest a novel criterion to distinguish between appropriate remedy models. We believe that the distinction between private and publicly available information has a significant effect on the appropriate model to be chosen, and we explain how this distinction should be understood and applied. The novelty in our formulation of the distinction is that unlike approaches that view the existence of password protection as demonstrating that information is private,[22] we believe that the benchmark for the distinction is whether the access to the information was granted to an indeterminate public or to a pre-defined set of individuals. In other words, it is not the protection measures taken with respect to the non-proprietary information that matter, rather the choice of the computer owner to grant access to such information to the public.

On the basis of the private-public dichotomy, we suggest that

[22] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1109 (N.D. Cal. 2017) (citing *Facebook, Inc.*, 844 F.3d at 1067, 1068; United States v. Nosal, 844 F.3d 1024, 1039 (9th Cir. 2016)) ("[N]one of the data in *Facebook* or *Nosal II* was *public* data. Rather, the defendants in those cases gained access to a computer network (in *Nosal II*) and a portion of a website (in *Power Ventures*) that were protected by a password authentication system. In short, the unauthorized intruders reached into what would fairly be characterized as the private interior of a computer system not visible to the public.").

injunctions and enforcement costs be granted in cases of unauthorized access to private non-proprietary information. When it comes to publicly available non-proprietary information, we believe that the no-remedy model should be applied, in the sense that no injunction should be granted to restrict access in such cases, and we support this claim through the analysis of both theory and positive law relating to injunctive relief in general. However, this is a no-remedy model only to a certain extent. In contrast to other approaches, we believe that some remedial redress is theoretically justified in cases of such violations of the CFAA unauthorized access provision. We use an analogy to the doctrine of easement of necessity with respect to landlocked property to propose a model providing for judicially determined access rights subject to access fees paid to the computer owner. The suggested model is conditional on the defendant securing a court order allowing the access prior to violating the CFAA access provision. In cases where defendants fail to do so, we suggest reverting to the injunction and enforcement costs model.

The remainder of the Article will proceed as follows: Part II will review existing case law on trespass to chattels and the CFAA unauthorized access provision; Part III offers a theoretical analysis of the protection of boundaries, regardless of whether they contain property, based on both autonomy based and economic theories; Part IV outlines a taxonomy of alternative potential remedies for CFAA violations based on the statutory language; Part V provides the guidelines for choosing the appropriate remedies model in various circumstances focusing on our account of the private-public dichotomy; and finally, Part VI concludes.

II. RECENT HISTORY & CURRENT DOCTRINE: FROM TRESPASS TO CHATTELS TO CFAA UNAUTHORIZED ACCESS

In this Part II, we offer a descriptive account of the doctrinal history of two causes of actions used in cases where plaintiffs seek to prevent defendants from accessing their otherwise non-proprietary information. The first wave of cases revolved around the trespass to chattels doctrine, whose applicability courts limited over time to a point where it became almost un-actionable.[23] The second wave of cases, which is currently at its peak, revolves around the CFAA

[23] *See* NetApp, Inc. v. Nimble Storage, Inc., No. 5:13-CV-05058-LHK (HRL), 2015 U.S. Dist. LEXIS 11406, at *61 (N.D. Cal. Jan. 29, 2015); Quilter, *supra* note 18, at 433, 434.

unauthorized access doctrine.[24]

The questions that the two doctrines raise are quite similar, but there is a key difference between the two, namely that while the trespass to chattels doctrine is based on a general common law cause of action,[25] the CFAA access provision is a statutory doctrine specifically tailored to cases involving unauthorized access to computers.[26] In this sense, as we shall see, even though the second wave of CFAA claims was a continuation of the first wave to a great extent, courts found it harder to limit the doctrine and reached to a point where it has substantial applicability, also to cases of access to non-proprietary information.[27]

We now turn to discuss the development of the case law under both doctrines. This discussion will serve as fertile grounds for discussion on the normative bases both of the doctrines and of the doctrinal complexities that arise in the subsequent Parts.

A. Trespass to Chattels

Trespass to chattels is the tort doctrine used to regulate access to electronic information.[28] Unlike the more well-known trespass to land, trespass to chattels was obscure and rarely used up until the late 1990s.[29] Its original purpose was to prohibit the unauthorized use of the personal property of another in a way that harms the owner.[30] This idea is captured in the doctrine's two main requirements: (i) the defendant was in physical contact with the chattel; and (ii) it harmed the owner's right by damaging the chattel, another person, or the property of the owner or by interfering with

[24] *See Facebook, Inc.*, 844 F.3d at 1068; *Nosal*, 844 F.3d at 1028; LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009); Sandvig v. Sessions, 315 F. Supp. 3d 1, 8 (D.D.C. 2018); *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1108; Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 968 (N.D. Cal. 2013).

[25] *See* Quilter, *supra* note 18, at 424.

[26] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(1) (2012); Kerr, *supra* note 20, at 1153.

[27] *See Facebook, Inc.*, 844 F.3d at 1067 (establishing that where a company is accessing another's computers to disseminate messages to the subscribers of the secondary company, this is a violation of the CFAA if the company's authority was rescinded and the company continued to access the computers); *Nosal*, 844 F.3d at 1035 (establishing that where employees who have authorized access to confidential information access this information for another individual who does not have authorization, such as a former employee, this access is no longer permissible under the CFAA).

[28] *See* Quilter, *supra* note 18, at 428–29.

[29] *See* Gregory N. Mandel, *Legal Evolution in Response to Technological Change*, *in* THE OXFORD HANDBOOK OF LAW, REGULATION, AND TECHNOLOGY 225, 232 (Roger Brownsword et al., eds., 2017); Quilter, *supra* note 18, at 424.

[30] *See* Quilter, *supra* note 18, at 424–25.

the owner's right to use the chattel for a substantial period of time.[31]

Since the 1990s, courts have begun to apply the trespass to chattels doctrine to computer-related cases.[32] This transformation, as will be discussed below, often involves two significant changes. The first is eliminating the harm requirement; and the second is stretching the definition of physical contact to include the sending of electronic signals.[33] In doing so, courts have essentially created a "trespass to computers" doctrine, which forbids the "invasion" of another's computer via electronic signals.[34]

The move from trespass to chattels to trespass to computers began with *Thrifty-Tel, Inc. v. Bezenek*.[35] In *Thrifty-Tel,* the defendant had hacked the plaintiff's computer system.[36] Invoking trespass to chattels, the court decided that the electronic signals sent by the defendant were sufficient to meet the doctrine's physical contact requirement.[37]

A year later, in *CompuServe Inc. v. Cyber Promotions, Inc.*,[38] the court enjoined the defendant's spamming scheme, adopting the *Thrifty-Tel* decision concerning electronic signals and determining that the indirect harm caused to the plaintiff (the Internet Service Provider) by the scheme was sufficient to meet the harm requirement.[39] The court further rejected the defendant's claim that because the "plaintiff made the business decision to connect to the Internet . . . it cannot now successfully maintain an action for trespass to chattels."[40]

---

[31] *See* RESTATEMENT (SECOND) OF TORTS §§ 217–218 (AM. LAW INST.1965); RESTATEMENT (SECOND) OF TORTS § 218 (AM. LAW INST.1965); *see also* Kirk v. Gregory, [1876] 1 Exch. Div. 55, 56–58 (Eng.) ("[T]here was no evidence of a conversion; but—the plaintiff's counsel insist[ed] that he was entitled to a verdict on the count of trespass.").

[32] *See e.g.*, Kerr, *supra* note 20, at 1144, 1149 n.23; Mandel, *supra* note 29, at 232; Quilter, *supra* note 18, at 421; Richard Warner, *Border Disputes: Trespass to Chattels on the Internet*, 47 VILL. L. REV. 117, 120 (2002).

[33] *See* Hunter, *supra* note 20, at 478, 482 n.278, 508.

[34] *See id.* at 476, 478.

[35] Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996).

[36] *See id.* at 471.

[37] *See id.* at 472–73.

[38] CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

[39] *See id.* at 1022 (citing *Thrifty-Tel, Inc.*, 54 Cal Rptr. at 473). The court found two distinct types of harm, though neither was physical. The first was harm to plaintiff resources: "To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment . . . the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct." *CompuServe*, 962 F. Supp. at 1022. The second was harm to its reputation: "Defendants' intrusions into CompuServe's computer systems, insofar as they harm plaintiff's business reputation and goodwill with its customers, are actionable under Restatement § 218(d)." *Id.* at 1023.

[40] *CompuServe*, 962 F. Supp. at 1024.

Three decisions, in the early 2000s, further relaxed the harm requirement:[41] in *eBay, Inc. v. Bidder's Edge, Inc.*,[42] the Northern District of California decided that *potential* harm was sufficient;[43] in *Register.com, Inc. v. Verio, Inc.*,[44] the Southern District of New York found that "evidence of a mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels;"[45] and in *Intel Corp. v. Hamidi*,[46] the Third Appellate District of the Court of Appeal of California found that, when the plaintiff is seeking solely injunctive relief, demonstration of harm is not required.[47]

The *Register.com* court also found that the lawsuit itself provides sufficient notice to the defendant that its actions amount to trespass if the plaintiff's terms of use do not prohibit the defendant's actions.[48] Taken together, the new trespass to computer doctrine allows for injunctive relief if notice was given to the defendant, and for damages if mere possessory interference and potential harm can be demonstrated.

Many courts today hold the expansive interpretation outlined above when applying the doctrine to computers.[49] In essence, courts continue to uphold the right of website owners to selectively restrict access to their sites simply by providing notice, and to allow claims based on potential or indirect harm to the plaintiff business or on the costs of preventive measures.[50] Much of the more recent court analysis has been subsumed by the courts' discussion of the CFAA,[51] and therefore we leave the more in-depth analysis to the next Section. Yet, one should not get the impression of a linear expansion of the trespass to chattels doctrine. In parallel to the decision discussed, a very different narrative has also developed. Thus, in the same year

[41] *See* Quilter, *supra* note 18, at 432, 434, 435.

[42] ebay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

[43] *See id.* at 1067.

[44] Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000).

[45] *Id.* at 250.

[46] Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244 (Cal. Ct. App. 2001).

[47] *See id.* at 249.

[48] *See Register.com, Inc.*, 126 F. Supp. 2d at 249.

[49] *See* Quilter, *supra* note 18, at 430.

[50] *See*, *e.g.*, Facebook, Inc. v Power Ventures, Inc., 844 F.3d 1058, 1062 (9th Cir. 2016); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022, 1023 (S.D. Ohio 1997).

[51] Indeed, the CFAA is understood by courts as directly dealing with the issue of computer trespass. *See e.g.*, *Facebook, Inc.*, 844 F.3d at 1065 ("The CFAA prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use."); hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1109 (N.D. Cal. 2017) ("The CFAA was intended instead to deal with 'hacking' or 'trespass' onto private, often password-protected mainframe computers.").

eBay, Inc. was decided, the Central District of California in *TicketMaster Corp. v. Tickets.com, Inc.*[52] refused to enjoin Tickets.com's aggregation of publicly available information on TicketMaster's website, stating that the claim was preempted by copyright law.[53]

The rationale underlying *TicketMaster* survives today, and was recently expanded in *NetApp, Inc. v. Nimble Storage, Inc.* In *NetApp*, the Northern District of California further restricted the application of the doctrine to scraping activity by re-introducing the harm requirement and emphasizing the non-proprietary nature of the information being accessed.[54] The court began by stating that "in order for the taking of information to constitute wrongdoing, the information must be 'property' as defined by some source of positive law."[55] It went on to state that if the information were proprietary, the claim would be preempted, as the proprietary right is likely to be based on either the Uniform Trade Secrets Act or the Copyrights Act.[56] Finally the court rejected other quasi-rights bases for the claim, such as 'deeming' the information *as* property because it is "material that is 'considered' copyright protected"[57] or that is "non-confidential, non-trade secret employee work product."[58]

A similar reasoning can be found in the even more recent, *hiQ Labs, Inc.* v. *LinkedIn Corp.*, which will also be discussed in the context of the CFAA. In this case, the Northern District of California

---

[52] Ticketmaster Corp. v. Tickets.Com, Inc., No. CV99-7654-HLH (BQRx), 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. Aug. 11, 2000).

[53] *See id.* at *14; Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654 HLH (BQRx), 2000 U.S. Dist. LEXIS 4553, at *10–11 (C.D. Cal. Mar. 27, 2000) ("The 6th and 8th claims (misappropriation and trespass) are preempted and the motion is granted as to these claims. The essence of each claim is the invasion and taking of factual information compiled by Ticketmaster. To the extent that state law would allow protection of factual data (not clear at all), this cannot be squared with the Copyright Act.").

[54] *See* NetApp, Inc. v. Nimble Storage, Inc., No. 5:13-CV-05058-LHK (HRL), 2015 U.S. Dist. LEXIS 11406, at *37–38, *46, *59, *60, *61 (N.D. Cal. Jan. 29, 2015).

[55] *Id.* at *59.

[56] *See id.* at *60 ("To the extent that NetApp claims a property right in 'corporate employee work product' because NetApp considers such work product to be proprietary, NetApp's claim would be preempted by CUTSA. . . . If NetApp is claiming that the information is in fact copyrighted, such an allegation would indeed establish a property right. However, NetApp's claim may then be preempted by the Copyright Act.").

[57] *See id.* at *61 ("NetApp cites no source of positive law that grants a property right in material that is 'considered' copyright protected.").

[58] *Id.* at *60 ("Labor Code § 2860 does not grant NetApp a general property right for non-confidential, non-trade secret employee work product."). A similar conclusion was recently reached by The District Court of the District of Columbia in *Sandvig v. Sessions*. Sandvig v. Sessions, 315 F. Supp. 3d 1, 26–27 (D.D.C. 2018) ("Scraping or otherwise recording data from a site that is accessible to the public is merely a particular use of information that plaintiffs are entitled to see.").

reiterated that the doctrine requires that the defendant "intentionally interfered with plaintiff's use or possession of personal property, with resultant injury."[59] The court further questioned whether notice is sufficient to restrict the defendant's right to access as well as to scraping, thereby making such actions trespass to chattels.[60]

Courts offer two opposing narratives about the application of the trespass to chattels doctrine to scraping activities. The first suggests that, simply by providing notice, the "owner" of a server can restrict access to it, deeming any further access a trespass subject to injunction and damages.[61] According to the other approach, emphasizing the harm requirement, the non-proprietary nature of the information accessed and the public availability of the information, severely restrict the application of the doctrine.[62]

In an article discussing trespass in the context of Cyberspace, Richard Epstein argues that the harm requirement exists in chattel but not in land, because only trespass to land claim raises the underlying question of ownership.[63] It is for this reason, Epstein suggests, that "[c]hattels do not give rise to boundary disputes."[64]

In many ways, the two approaches differ on whether legal boundaries can and should be created without addressing the underlying question of ownership.[65] And when it comes to the trespass to chattels doctrine, the recent trend seems to reject the creation of legal borders when there is no legally protected interest lying within them.[66] In the commercial context, plaintiffs disappointed by this trend turn to the CFAA's unauthorized access to computers as a replacement for common law trespass doctrines.[67] In

[59] hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1113 n.11 (N.D. Cal.2017).

[60] *See id.* at 1113, 1113 n.11 ("In sum, viewed in a proper context, the Court has serious doubt whether LinkedIn's revocation of permission to access the public portions of its site renders hiQ's access 'without authorization' within the meaning of the CFAA.").

[61] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067, 1068 (9th Cir. 2015).

[62] *See NetApp, Inc.*, 2015 U.S. Dist. LEXIS 11406, at *37–38, *46, *58–59.

[63] *See* Richard A. Epstein, *Centennial Tribute Essay: Cybertrespass*, 70 U. CHI. L. REV. 73, 78 (2003).

[64] *Id.*

[65] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1112–13 (N.D. Cal. 2017); *NetApp, Inc.*, 2015 U.S. Dist. LEXIS 11406, at *59; Ticketmaster Corp. v. Tickets.Com, Inc., CV99-7654-HLH (BQRx), 2000 U.S. Dist. LEXIS 12987, at *9 (C.D. Cal. Aug. 11, 2000); *see also* Kerr, *supra* note 20, at 1144-45, 1159, 1161 ("On the one hand, protecting online privacy requires recognizing some boundary that individuals cannot cross. On the other hand, preserving the public value of the Internet requires identifying uses that individuals can enjoy without fear of criminal prosecution.").

[66] *See NetApp, Inc.*, 2015 U.S. Dist. LEXIS 11406, at *59.

[67] *See, e.g.*, *id.* at *3, *54–55 (finding against NetApp in their CFAA claim because they should have based their claim on state copyright laws and state common law.); *see* Kerr, *supra*

the next part, we will discuss the development of the CFAA access provision and how it may or may not yield plaintiffs' expected outcomes with respect to trespass to non-protected information. As we shall see, however, turning to the CFAA does not resolve the underlying question: should courts create and defend legal borders when there is nothing within them that is protected by law.

B. Unauthorized Access

The Computer Fraud and Abuse Act (CFAA) prohibits various activities with respect to computers.[68] The main prohibition for the purpose of this Article is the rule brought in Section 1030(a)(2)(C), known as the "access provision," that criminalizes any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[69] The statute also defines "'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."[70] The statute further determines that violations of such prohibitions warrant criminal sanctions, as well as constitute civil wrongs remedied by compensatory damages and injunctive relief.[71]

The access provision has been the basis for extensive debate in the case law in the last decade.[72] The main question, triggering both prosecutors and civil plaintiffs, has been what constitutes "unauthorized" access (or one that exceeds authorization) in a manner that imposes CFAA liability.[73] More specifically, courts focused on whether access to computers that began under permission could constitute CFAA violations at a later stage, and if so, then under what circumstances.[74]

In *LVRC Holdings LLC v. Brekka*, the Ninth Circuit reviewed a civil claim by an employer arguing that an employee accessed the

note 20, at 1144–45.

[68] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

[69] *Id.* at § 1030(a)(2)C). The term "protected computer" is defined in the CFAA to include practically any computer that is connected to the Internet. *See id.* at § 1030(e)(2)(B); United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012).

[70] *See* 18 U.S.C. § 1030(e)(6).

[71] *Id.* at § 1030(c), (g).

[72] *See* Kelly Singleton, *Federal Judge Allows Researcher's First Amendment Challenge to CFAA's "Access" Provision to Move Forward,* THE WSRG DATA ADVISOR (May 23, 2018), https://www.wsgrdataadvisor.com/2018/05/cfaas-access-provision/.

[73] *See id.*

[74] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1137 (9th Cir. 2009).

work computer, with valid credentials, to email valuable documents to his personal email for use in a future competing business.[75] The court determined that the statutory language is unambiguous in the sense that authorization means "permission or power granted by an authority."[76] It further explained that an access without authorization means that at the time of access, the user has at no point received permission to access the computer for any purpose or that at the time of access the permission had been rescinded by the computer owner.[77] This is the difference between "without authorization" and "exceed[ing] authorized access" the court explained.[78] The court rejected the argument that although the employee received permission to use the computer by the employer, the access was without authorization because the employee was not acting as an agent of the employer at that time.[79] The court explained that its review of the access authorization does not address the relationship between the user and owner at the time of access, rather only the existence of permission to access or the lack thereof.[80]

The *Brekka* decision led to the articulation of a more nuanced question with respect to the access provision—does every violation of use restrictions imposed by the computer owner automatically entail an unauthorized access, even if the access began under authorization?[81] This was more broadly discussed in *United States v. Nosal* (referred to hereinafter as *Nosal I*).[82] In *Nosal I*, the Ninth Circuit reviewed criminal charges against David Nosal for encouraging fellow employees to log into a work computer, download confidential information, and transfer it to a competing business.[83] The employees were authorized to access the information but violated the employer policy by disclosing such information to Nosal.[84] The court clarified that the access provision focuses on "violations of restriction of *access* to information, and not restrictions on its *use*."[85] Although this case focused on employees violating workplace policies, the court predicted the potential collateral outcomes of its decision

[75] *See id.* at 1129–30.
[76] *See id.* at 1132–33.
[77] *See id.* at 1135.
[78] *See id.* at 1133.
[79] *See id.* at 1133–34, 1135.
[80] *See id.* at 1134, 1135.
[81] *See* United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012).
[82] *Id.*
[83] *See id.*
[84] *Id.*
[85] *Id.* at 863–64.

and emphasized that merely violating website terms of service cannot constitute unauthorized access, since "[n]ot only are the terms of service vague and generally unknown . . . but website owners retain the right to change the terms at any time and without notice."[86] *Nosal I* led to a line of decisions determining that the CFAA does not extend to violations of restrictions on use.[87] However, some courts still contend that mere violations of use restrictions may suffice for CFAA violations.[88]

These questions quickly began cropping up in commercial relationships, especially in the context of competing businesses attempting to build on information and databases of leading businesses in the market using various data-mining techniques, including scraping.[89] In *Craigslist Inc. v. 3Taps Inc.*, the court for the Northern District of California examined whether the fact 3Taps aggregated and republished ads published on Craigslist using scraping methods—even after Craigslist sent a cease and desist letter to 3Taps, explicitly revoking its authorization to access its computers, and configured an IP address block addressed at 3Taps—violates the CFAA access provision.[90] While agreeing with 3Taps that the fact that the Craigslist website was open to the general public meant that 3Taps had initial authorization to access its computers, the court found that such preliminary authorization could be revoked by Craigslist.[91] The court determined that while continuing scraping Craigslist data following the explicit rescission of permission to access Craigslist computers, 3Taps was exceeding the authorization that was granted to it.[92]

The Court of Appeals for the Ninth Circuit followed the *Craigslist*

---

[86] *See id.* at 862.

[87] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA."); United States v. Valle, 807 F.3d 508, 523–24, 528 (2d Cir. 2015) (reversing the conviction of a CFAA violation in which the defendant was allowed access to the police database but had used it for non-law enforcement purposes); WEC Carolina Energy Sol.'s LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) (noting that the approach taken in *Nosal* presumes a Congressional intent to criminalize such behavior absent an unequivocal intention to do so'"); Sandvig v. Sessions, 315 F. Supp. 3d 1, 23, 27 (D.D.C. 2018) (accepting the *Nosal* approach).

[88] *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001).

[89] "Scraping" is the recoding of data contained on a computer (e.g. server, website, etc.). *See, e.g.*, Hunter, *supra* note 20, at 478–79, 479 n.254 ("'Scraping' or 'screen scraping' involves the exhaustive traversal and collection of all data on a site.").

[90] *See* Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 966, 967 (N.D. Cal. 2013).

[91] *See id.* at 969–70.

[92] *See id.*

decision and further articulated it in *Facebook Inc. v. Power Ventures Inc.* Power Ventures "operated a social networking website" allowing its users to aggregate their social network account on other platforms.[93] In this context, it allowed its users to view their profiles using its website and launched promotional campaigns utilizing Facebook's platform and the user accounts to extend its reach to more users.[94] When Facebook learned of this practice, it "sent a 'cease and desist' letter to Power [Ventures] instructing [it] to terminate its activities."[95] When Power Ventures refused to sign Facebook's Developer Terms of Use, Facebook created an IP block preventing Power Ventures from accessing its computers.[96] Power Ventures circumvented such block by switching IP addresses.[97] The court, citing *Nosal I* and *Brekka*, reached two main conclusions.

> First, a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. Second, a violation of the terms of use of a website—without more—cannot establish liability under the CFAA.[98]

It then concluded that although Power Ventures did receive the permission of its users to access their Facebook accounts (and by that, indirectly, Facebook's permission too), after Facebook revoked such

---

[93] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062 (9th Cir. 2016).

[94] *See id.* at 1063.

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.* at 1067. In this context, it is important to note the decision in United States v. Nosal, 828 F.3d 865 (9th Cir. 2016) (hereinafter *Nosal II*). There, the Court of Appeals for the Ninth Circuit determined that the same David Nosal violated the CFAA by accessing his employer's computer (after his access permissions had been explicitly revoked) by using the credentials of a fellow employee. *Nosal II*, 828 F.3d at 878. This decision raised some (unsubstantiated) concern in the press that any type of password or credential sharing will constitute a CFAA violation. *See* Liz Calvario, *Yes, Sharing Your Netflix or HBO GO Passwords Is Actually a Federal Crime*, INDIEWIRE (July 12, 2016), https://www.indiewire.co m/2016/07/sharing-netflix-hbo-go-account-federal-crime-1201704820/; Orin Kerr, *Password-Sharing Case Divides Ninth Circuit in Nosal II*, WASH. POST (July 6, 2016), https://www.wash ingtonpost.com/news/volokh-conspiracy/wp/2016/07/06/password-sharing-case-divides-ninth-circuit-in-nosal-ii/?utm_term=.cf5f09dd4079; David Z. Morris, *Sharing Passwords Can Now Be a Federal Crime, Appeals Court Rules*, FORTUNE (July 10, 2016), http://fortune.com/2016/0 7/10/sharing-netflix-password-crime/. This is obviously not the case, since the preliminary conditions in *Nosal II* were that access permissions were first explicitly revoked, before the credential sharing took place. *Nosal II*, 828 F.3d at 875–76.

permission, the permission granted by the users could not suffice, because access must be authorized also by the platform owner.[99]

Two later cases are noteworthy. First, in *Sandvig v. Sessions*, the court for the District of Columbia reviewed a constitutional challenge of the CFAA access provision brought by researchers intending to scrape public websites for research purposes.[100] The researchers argued that the access provision exposes them to risk of criminalization, thus violating the First and Fifth Amendments.[101] To assess the plaintiffs' arguments, the court interpreted the access provision and followed the narrow reading of the Ninth Circuit.[102] In its assessment, however, the court provided two important determinations. First, the scraping of publicly available websites, even if explicitly violating their terms of use, is not a *per se* violation of the access provision.[103] Second, the use of a fictitious account may trigger the access provision since it may grant the user access to pages that are not necessarily open to the general public.[104] This is important because it creates a distinction between public and non-public pages on websites that was not previously adopted by the Court of Appeals for the Ninth Circuit.

Second, in *hiQ Labs, Inc. v. LinkedIn Corp.*, the court for the Northern District of California examined hiQ's request to issue an injunction requiring LinkedIn to remove any technological barriers preventing it from accessing LinkedIn's computers.[105] hiQ, much like 3Taps, scraped LinkedIn's publicly available pages to extract workforce data that it later sold to its clients.[106] LinkedIn, basing its actions on the *Power Ventures* decision, issued cease and desist letters to hiQ and imposed technological barriers preventing it from accessing its website.[107] hiQ, instead of circumventing the barriers, requested that the court issue a preliminary injunction requiring LinkedIn to remove such barriers.[108] Despite the guiding case law of *Nosal I*, *Nosal II*, and *Power Ventures*, the court granted hiQ's motion determining that it did not violate the CFAA access provision.[109] The

---

[99] *See Facebook, Inc.*, 844 F.3d at 1067, 1068.
[100] *See* Sandvig v. Sessions, 315 F. Supp. 3d 1, 10 (D.D.C. 2018).
[101] *See id.*
[102] *See id.* at 23.
[103] *See id.* at 26–27.
[104] *See id.*, at 27.
[105] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1104 (N.D. Cal. 2017).
[106] *See id.*
[107] *See id.*
[108] *See id.*
[109] *See id.* at 1109, 1113, 1120.

court differentiated the prior case law mainly on the fact that both *Nosal II* and *Power Ventures* referred to password protected information, while in hiQ's case, the information was publicly available.[110] The court's reasoning for this decision relied mainly on the underlying normative justifications of the CFAA that will be further discussed below. In short, the court explained that the social norms with respect to publicly open websites and the ability of the public to access such websites, dictates that no website owner could revoke access permissions from a specific user with respect to such public pages, and that such revocation has no valid effects for the CFAA access provision.[111]

Much like with trespass to chattels, courts were not easily inclined to enforce the access provision in cases where the main reason plaintiffs invoked the doctrine was to limit access to unprotected information.[112] This is perhaps one of the reasons for the commonly accepted rule that exceeding use limitations does not trigger unauthorized access. However, in contrast to trespass to chattels, since the CFAA access provision does not require harm to apply, when courts reach the conclusion that explicit access limitations were breached, they reach the inevitable conclusion that the CFAA access provision was violated.[113] The question that follows, on which we will focus later in this Article, is what are the adequate remedies for cases where there is no question as to whether the access provision was violated, but nevertheless no harm was done, for example, when the information (in and of itself) that was accessed, scraped, or otherwise used is unprotected. Before we can discuss the proper remedies for such CFAA violations, we must first revisit the underlying theory and justifications for the CFAA access provision.

III. UNDERLYING THEORY AND JUSTIFICATIONS: WHY DO WE PROTECT COMPUTERS?

Why do we protect computers? Is it because we think there are special features that are inherent to computers and require a *sui generis* protection, or do we protect computers because they are the

[110] *See id.* at 1109.

[111] *See id.* at 1112. The court's decision in *hiQ* also relied on California state constitution and unfair competition law. *See id.* at 1117, 1118. We will discuss the internal logic of the court's decision (and any inconsistencies thereof) below.

[112] *See id.* at 1113.

[113] *See* Reis, Inc. v. Spring11 LLC, No. 15 Civ. 2836 (PGG), 2016 U.S. Dist. LEXIS 131486, at *22 (S.D.N.Y. Sept. 24, 2016).

private property of a person, just like any other type of property? The United States Congress addressed these questions in the Senate Report prior to the enactment of the CFAA.[114] Congress explained that there are two main reasons why a law prohibiting the misuse of computers is required. First, the then current legal framework was ill-equipped to address the misuse of computers, since "the property involved does not fit well into traditional categories of property [targeted by] abuse or theft."[115] Second, the then new trend of hacking into computers needed to be addressed by proper laws governing this type of trespass.[116] In the words of the Report, "[t]he fact is, these young thrill seekers are *trespassers*, just as much as if they broke a window and crawled into a home while the occupants were away."[117]

It is evident that Congress understood computers as property, or a proprietary space, that must be protected just like any other type of property. However, Congress was aware of the difficulty in applying existing property doctrines to the intangible nature of computers as space or property and therefore thought that a *sui generis* protection was required.[118] Indeed, Congress understood computers as proxies for the protection of the property and proprietary transactions that occur through the use of computers.[119] This is evident both in the Senate Report for the enactment of the CFAA, stating that "[a] computer program, for example, may exist only in the form of magnetic impulses and where a program of substantial commercial value is accessed, the information stolen almost always remains in the possession of the original owner."[120] This is particularly evident in the Senate Report on the National Information Infrastructure Protection Act of 1995, amending the CFAA to include the current access provision, stating that

> [t]he proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer. This information, stored electronically, is intangible, and it has been held that the theft of such information cannot be charged under more traditional

[114] *See* S. REP. NO. 104-357, at 12 (1996).
[115] H.R. REP. NO. 99-612, at 5 (1986) (Conf. Rep.).
[116] *See* S. REP. NO. 104-357, at 10.
[117] H.R. REP. NO. 99-612 at 5–6 (emphasis added).
[118] *See* S. REP. NO. 104-357, at 3–4, 5. For further discussion on the idea of cyber as place, see Hunter, *supra* note 20, at 501 n.428.
[119] *See* S. REP. NO. 104-357, at 7.
[120] H.R. Rep. No. 99-612 at 5.

> criminal statutes . . . . This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected . . . . The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information.[121]

It is apparent that Congress wanted to afford the same level of protection to the cyberspace as there had been to property and proprietary spaces in the physical sphere. But different theories for the protection of private property may lead to different results when applied to the protection of cyber spaces and information.[122] The problem is most evident when, as is often the case, the information itself is not protected by property rights.[123] In such cases, it is crucial to ask what is our theoretical justification for the protection of spaces and boundaries, when these spaces do not include any property at all. In a sense, the physical example for this would be breaking into an empty house, taking no property whatsoever.[124]

We will now turn to discuss this question under two main approaches to the protection of private property—property as the fulfillment of autonomy and personhood, and the economic analysis of property protection. We note that since the main focus of this Article is CFAA remedy regimes in commercial contexts, we will not discuss the criminal aspects of the questions raised above. In addition, since this mainly concerns commercial litigation between corporations, we will not address privacy concerns, which are obviously part of the CFAA framework.

A. Right-Based Approaches to Property: Boundaries as Manifestation of Freedom and Autonomy

Right based theories of private law often rely on Aristotelian corrective justice and Kant's doctrine of right, to explain that private law should be understood as a corrective mechanism for injustice.[125]

---

[121] S. REP. NO. 104-357, at 7–8.

[122] *See* Hunter, *supra* note 20, at 486.

[123] *See id.*

[124] Indeed, the analogy to real property is in itself revealing, as tangible objects would rarely allow for an applicable analogy. *See* Michael De Groote, *Thief in the Night: Stealing in a Digital Age*, DESERET NEWS (Mar. 28, 2014), https://www.deseretnews.com/article/86566282 2/Thief-in-the-night-Stealing-in-a-digital-age.html.

[125] *See* ERNEST J. WEINRIB, CORRECTIVE JUSTICE 2 (2012) [hereinafter WEINRIB, CORRECTIVE JUSTICE]; Ernest J. Weinrib, *Correlativity, Personality, and the Emerging*

This corrective mechanism, however, presupposes correlativity and focuses on the interrelations between the plaintiff and the defendant and the rights and duties they have with respect to one another.[126] In other words, this means that "liability reflects the conclusion that the defendant and the plaintiff have respectively done and suffered the same injustice."[127] Hand-in-hand with the Kantian concept of personality–which treats human beings as purposive entities who are free to act as long as they do not interfere with the rights of others[128]–correlativity serves as the inner, normative justification for legal rights and duties.[129]

The concept of personhood plays a significant role in the corrective justice approach as it is the normative basis for the rights and duties of individuals.[130] It is based on Kant's conception in his doctrine of right, based on which he defined the "right" as follows: "Right is therefore the sum of the conditions under which the choice of one can be united with the choice of another in accordance with a universal law of freedom."[131] Kant's universal-right approach is based on the premise that a right could only exist where it reflects a state in which the free will of every person could exist alongside the free will of any other person.[132]

Kant's universal right focuses on relationships between individuals.[133] To the extent that a person's act that is in line with all others' freedoms – meaning, part of her right – is restricted by the right of another person, the latter wrongs the former.[134] From this premise, Kant derived principles with respect to individuals' rights in external things, such as property.[135] According to Kant, a person can claim that something is hers if she can claim that others' acts

Consensus on Corrective Justice, 2.1 THEORETICAL INQUIRIES L. 107, 111, 112 (2001) [hereinafter Weinrib, *Correlativity*].

[126] *See* Weinrib, *Correlatvity*, *supra* note 125, at 110.

[127] *Id.*

[128] *See id.* at 111. Weinrib explained this framework through the distinction between factual and normative gains and losses. *See* ERNST J. WEINRIB, THE IDEA OF PRIVATE LAW 114–15 (1995).

[129] *See* WEINRIB, CORRECTIVE JUSTICE, *supra* note 125, at 9; Weinrib, *Correlativity*, supra note 125, at 111.

[130] *See* Weinrib, *Correlativity*, supra note 125, at 111.

[131] Immanuel Kant, *The Metaphysics of Morals*, *in* PRACTICAL PHILOSOPHY 387 (Mary J. Gregor trans. & ed., 1996).

[132] *See* Allen Wood, *General Introduction*, *in* PRACTICAL PHILOSOPHY xvi (Mary J. Gregor trans. & ed., 1996). For elaboration on Kant's free will approach, *see* WEINRIB, CORRECTIVE JUSTICE, *supra* note 125, at 87.

[133] *See* Kant, *supra* note 131, at 387.

[134] *See id.* at 387, 401.

[135] *See, e.g.*, *id.* at 413, 414 ("The usual exposition of a *right to a thing* (*ius reale, ius in re*) . . . 'is a right against every possessor of it.'").

with respect to such a thing will limit her freedom that is in line with the freedom of others.[136] Therefore, Kant explained that property is not a right in an external thing, rather the right of a person towards other persons with respect to such a thing.[137]

This right to external things, and thus the right to private property, could only exist in a civil condition according to Kant, as it requires a common will of all people, since a unilateral will cannot restrict other people from acting.[138] The common will guarantees that all people will be entitled to manifest their wills and their ability to have rights with respect to external things, thus fulfilling the universal-right principle.[139] In sum, Kant's doctrine of right (including property rights) is often understood as correlative since it focuses on the existence of a right in a relationship between two (or more) individuals, and universal since it requires that the right of each person conform with the rights of all other persons and the existence of a formal equality with respect to the possibility of acquiring rights.[140]

At first glance, the corrective justice framework easily explains why we protect boundaries. If our normative analysis is premised on the notion that a person has a property right that allows her to exclude others' access to or acquisition of an external thing that is hers, it immediately follows that such person has the right to set boundaries that no other person is allowed to trespass absent her consent.[141] In other words, in order to extend the freedom and autonomy of individuals, property rights should include the right to choose to exclude others.[142] Thus, a common theme in right based theories is the idea that "[y]our right to property is your right to limit the conduct of others in relation to particular things."[143] Therefore, if we understand computers as the property or proprietary spaces of the entity that owns them, it inevitably follows that the owner could set boundaries that prohibit others from using or entering such spaces, regardless of the magnitude of damage that may be caused, if any. To put things differently, the right to exclude when one chooses

[136] *See id.* at 387, 401–02

[137] *See id.* at 401, 414, 419.

[138] *See id.* at 409.

[139] *See id.*

[140] *See id.*

[141] *See* Kenneth A. Stahl, *The Challenge of Inclusion*, 89 TEMP. L. REV. 487, 494 (2017).

[142] *See id.*; Andrea J. Boyack, *Limiting the Collective Right to Exclude*, 44 FORDHAM URB. L.J. 451, 458 (2017).

[143] ARTHUR RIPSTEIN, FORCE AND FREEDOM: KANT'S LEGAL AND POLITICAL PHILOSOPHY 93 (2009).

to do so, is at the heart of one's autonomy.

B. The Economics of Defending Boundaries: Allocating Efficiency vs. Minimizing Social Costs

Turning from autonomy to the maximization of welfare requires translating the legal question of boundaries into economic terms, while keeping it separate from the question of rights in the information within the border.[144] The split between borders is especially troubling in cases of scraping non-proprietary information. This is because such circumstances are grounds for two seemingly contradictory assumptions: first, that there are sound economic reasons to deny rights in whatever is enclosed by borders, and second, that the computer owner should be allowed to use technological means to restrict others from accessing their computer regardless of whether entry is legally prohibited.[145]

To understand why the two assumptions seem contradictory, let us begin with the first assumption—that it is inefficient to grant a legal right in the information.[146] Clearly, if it is efficient that the information would be proprietary, the owner should be allowed to use technological means to prevent others from accessing and using the information.[147] Accordingly, because granting the owner the legal power to control access and use of the information is more efficient

---

[144] *See* Adam J. MacLeod, *Patent Infringement as Trespass*, 69 ALA. L. REV. 723, 726–27, 743 (2018).

[145] *See* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2169–70 (2004); Niva Elkin-Koren, *Copyrights in Cyberspace—Rights Without Laws?*, 73 CHI.-KENT L. REV. 1155, 1159 (1998); Jonathan Klick & Gideon Parchomovsky, *The Value of the Right to Exclude: An Empirical Assessment*, 165 U. PA. L. REV. 917, 920 (2017). To clarify, the distinction here is between whether a person has a legal right to take measures in order to prevent others from entering a certain location, and whether a person can enlist the law (i.e., the state) to prevent such entry. *Cf.* Bellia, *supra*, at 2169 (discussing property rule protection of owner's right to exclude by own means); Elkin-Koren, *supra*, at 1156 (copyright which provides legal force to exclude through court mechanisms). While the two rights often coincide, it is possible for one to exist without the other. *See, e.g.*, Bellia, *supra*, at 2169–70 (discussing possibility of using only liability rule or only property rule protection). Thus, one may have the right to call the police to prevent entry into her property, but be unentitled to self-remedy the violation; conversely, a person may have the right to prevent entry by her own means, but be unentitled to use the state to achieve her ends. *See, e.g.*, Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 753 (1998) (rights to exclude, even on one's own land, are not absolute; some circumstances allow right to use force or call police, others do not). *See also* Nickens v. Mount Vernon Realty Grp., LLC, 54 A.3d 742, 752 (Md. 2012) (right to use reasonable force when excluding trespasser); State v. Quinlan, No. 30860-6-II, 2004 Wash. App. LEXIS 3131, at *18 (Wash. Ct. App. Dec. 28, 2004) (right to call police for trespasser, but not right to use force in these circumstances).

[146] *See* Hunter, *supra* note 20, at 444.

[147] *See* hiQ Labs, Inc. v. LinkedIn Cor., 273 F. Supp. 3d 1099, 1104 (N.D. Cal. 2017).

than having the owner deploying technological means to do so, such right is itself efficient.[148] However, when the law denies the owner the right in the information, it implies that the owner's control in the access and use of the information is also inefficient.[149] Accordingly, it seems that not only should the law not aid the computer owner in restricting access, but it should actively prevent the owner from using technological means to prevent the access and use of the information. Otherwise the law would grant someone control over a public resource solely because that person controls the only access road to it.[150]

The problem, then, is to explain if and why, at least in some circumstances, the owner of the computer storing public information is not legally prohibited from preventing others from accessing the information stored—that is, to explain how it is possible for the two assumptions to co-exist.

Framing the question this way, we can also see that, even when property rights are clear, the law matters because it determines the extent to which one can access and use *common* resources.[151] The standard justification for the existence of legal rules is the existence of transaction costs.[152] In their canonical Cathedral analysis, Calabresi and Melemad suggest that legal rules matter because when transaction costs are high, parties will fail to negotiate for the most efficient outcome.[153] Yet, in practice, negotiations between the parties often took place, suggesting that costs are not prohibitive and

---

[148] *See* Kimberly D. Krawiec, *Fairness, Efficiency, and Insider Trading: Deconstructing the Coin of the Realm in the Information Age*, 95 NW. U. L. REV. 443, 456 (2001).

[149] *See, e.g.*, Gaia Bernstein, *In The Shadow of Innovation*, 31 CARDOZO L. REV. 2257, 2283–84 (2010) (noting courts disfavor information rights because overprotection can stifle innovation); Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 1045–46 (1997) (patent law provides developers rights to incentivize efficient use); Michael Trebilcock & Paul-Erik Veel, *Property Rights and Development: The Contingent Case for Formalization*, 30 U. PA. J. INT'L L. 397, 404 (2008) (property rights are given to efficient uses of resources and goods).

[150] *See* Hunter, *supra* note 20, at 443–44.

[151] This thinking counters the assumption underlying the Coase Theorem. *See* Ronald H. Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1, 2 (1960). Interestingly, one might see Marx's discourse on the law of the forest as somewhat analogical. Though not dealing directly with the issue, Marx discusses the German state's act to deny individuals the right to collect dead wood from the forest, given that the latter (as opposed to live wood) is not considered property. *See* Karl Marx, *Debates on the Law on Thefts of Wood*, RHEINISCHE ZEITUNG, Oct. 25, 1842. One might wonder what would have happened if instead of passing a law criminalizing the collection of dead wood, the state had simply made access to the forest a trespass. That is, as in the case discussed here, what would have resulted from the creation of a border to protect an object which is not protected by a property right.

[152] *See* Guido Calabresi & Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1096 (1972).

[153] *See id.* at 1120–21.

that access should be protected by a property rule.[154] We will return to this point in Part V. For now, it will suffice to say that the drawback of negotiations is that they are unlikely to center on the 'correct' right.[155] That is, negotiations are likely to turn on the value of the *non-proprietary* information, which is not the computer owner's to sell, rather than on the value of mere access to the information, which is what is actually owned.[156]

Thus, providing legal protection for borders, but not for property, is likely to create a holdout problem. It is obvious that access itself is only desirable for the accessor because of the value of the information, just as the computer owner's willingness to accept would reflect the cost (e.g., diminished profits) that would be incurred from sharing the information.[157] Because holdout problems reflect a transaction cost—one that is likely to prevent the parties from negotiating their actual legal rights—Calabresi and Melemad's Cathedral analysis suggests that, while the owner of the computer should be granted the access right—meaning the right to exclude others—such right should be controlled by a liability rule.[158]

We will discuss the idea of access rights protected by a liability rule further in Part IV. In the remainder of this part, we offer another way to reach a similar conclusion, based on Posner's economic analysis of property rights.[159] Posner's analysis can serve as a reply to the critique on the economic analysis, which argues that the latter justifies so-called "efficient theft" for the same reasons it justifies efficient breach of contracts.[160] The gist of the critique is that, under the economic analysis, individuals should be allowed to take the property of another if they value it more than its current owner.[161] Posner argues that permitting such taking would be inefficient because, rather than fostering allocative efficiency, it would incentivize people to invest more in the protection of their

---

[154] *See id.* at 1108–09.

[155] *See id.* at 1110.

[156] *See id.* at 1092.

[157] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1119 (N.D. Cal. 2017).

[158] *See* Calabresi & Melamed, *supra* note 152, at 1107.

[159] Richard A. Posner, *An Economic Theory of the Criminal Law*, 85 COLUM. L. REV. 1193, 1198 (1985) ("Allowing coercion would create incentives for potential victims to spend heavily on self-protection and for potential aggressors to spend heavily on overcoming the victims' self-protective efforts. All this spending would yield little if any net social product.").

[160] *See* Gil Lahav, *Contract Law: A Principle of Justified Promise-Breaking and Its Application to Contract Law*, 57 N.Y.U. ANN. SURV. AM. L. 163, 182 (2000). To clarify, the critique is that theft—efficient or not—is wrong and that, therefore, any theory that justifies it is also wrong. *See id.*

[161] *See id.* at 182 n.48.

possessions.[162] Because such investment is usually economically wasteful, what is assumed to be efficient theft, in fact, turns out to be inefficient.[163]

The idea above is also applicable to the circumstance addressed in this Article. That is, lacking a legal right to prevent access by others, the owner of a computer on which non-proprietary information is stored would be incentivized to invest in technological barriers to prevent entry, while those who wish to access the information would invest in overcoming these barriers. Assuming that this investment is mostly wasteful,[164] as it is an investment in protecting something to which the computer owner can claim no legal right, it would be better to provide legal protection in order to reduce this investment. Thus, minimizing economic waste serves as an economic justification to protect borders, regardless of what is inside them.[165]

From the discussion thus far, it can be concluded that, when the law allows individuals to prevent access to computers, legal protection of the borders is efficient insofar as it minimizes social costs, but when the law refuses to recognize the validity of the legal border, it should prevent the computer owner from using technological means to protect the content. This line of thought can be observed in the two recent cases of *hiQ Labs Inc. v. LinkedIn Corp* and *Sandvig v. Sessions*. In *Sandvig*, the court determined that access to non-proprietary information, which is not password protected, does not to violate the CFAA access provision.[166] In *hiQ Labs* the court prohibited LinkedIn from using means to restrict access to its non-proprietary information.[167] Thus, when the court allowed the computer owner to protect the non-proprietary information using technological means, it also recognized a legal right to prevent access.[168] When the court refused to recognize the legal validity of the border, it also enjoined the computer owner from using technological means to protect the border.[169]

The alignment between the legal protection of borders and the legal

---

[162] *See* Posner, *supra* note 159, at 1195, 1196.

[163] *See id.* at 1196.

[164] One might argue that such investment could generate a useful byproduct in the form of technological advancement. *See id.* Yet, we believe that the incentives to protect proprietary information—that is to protect an existing legal right—are more than sufficient for such technological advancement to take place.

[165] Epstein, *supra* note 63, at 76.

[166] *See* Sandvig v. Sessions, 315 F. Supp. 3d 1, 30, 34 (D.D.C. 2018).

[167] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1120 (N.D. Cal. 2017).

[168] *See id.*

[169] *See id.*

permissibility of the computer owner's use of technological means to protect borders does not indicate, however, when borders should be legally valid.[170] In *hiQ Labs*, for example, the court seems to draw the line at password-protected information.[171] We believe that, for reasons related to both the economic analysis and autonomy, the line should be drawn elsewhere. We shall return to this issue in Part V. In Part IV, which follows, we begin to address the question of remedies for breaking into a computer protected by a legally valid border.

IV. POTENTIAL REMEDY MODELS FOR UNAUTHORIZED ACCESS

Thus far, we have discussed the available legal doctrines relating to the protection of non-proprietary information based on boundary-protection rules and the underlying theories that justify these rules. Given that, at least with respect to the CFAA access provision, the law effectively grants a cause of action to protect cyber boundaries established through unauthorized access to computers,[172] we believe that applying the theoretical considerations discussed above would be most suitable as part of the remedies models afforded to computer owners whose borders have been illegally crossed.

This Part will attempt to portray the potential alternative remedies models for such cases, discuss their fitness with regards to the underlying theories, and explain their consequences. We identify three common types of remedies models that could be positioned on a spectrum—no remedies for accessing non-proprietary information, injunctive relief and enforcement costs only, and restitution and full disgorgement of profits.

While this Part focuses on remedies, we believe that it has much to do with the overall scope of the CFAA access provision, and even with the substantive question of whether the information itself is protected (as remedies are inseparable from the scope of rights, and to a certain extent, determine whether an effective right exists).[173]

---

[170] *See id.* at 1108, 1109.

[171] *See id.* at 1112.

[172] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018).

[173] *See* Donald H. Zeigler, *Rights, Rights of Action, and Remedies: An Integrated Approach*, 76 WASH. L. REV. 67, 68, 71 (2001); OMRI RACHUM-TWAIG, COPYRIGHT LAW AND DERIVATIVE WORKS: REGULATING CREATIVITY (2019). *See* Bernard Chao, *The Infringement Continuum*, 35 CARDOZO L. REV. 1359 (2014), for a similar argument with respect to patent law. Chao suggests that rights and remedies should be placed on a continuum, which "adjusts the amount of damages by the proximity the infringer's use has to the use envisioned by the inventor." *Id.* 1404–05. *See* Mark A. Lemley & Mark P. McKenna, *Scope*, 57 WM. & MARY L. REV. 2197, 2200 (2016), for a discussion on the many features of a right that determine its overall scope in

This relevance will be especially evident in the discussion on the polar alternatives—no remedy in contrast to full disgorgement of profits—that are essentially equivalent to no CFAA violation as opposed to an indirect protection of non-proprietary information amounting to the treatment of such information *as if* it were property.[174]

We will now turn to discuss each of these potential models. In Part V, we will attempt to suggest a way to choose the right model.

A. No Remedy for Accessing Non-Proprietary Information

The laxest remedy model that could be afforded to computer owners whose boundaries have been crossed, but whose information is not protected as property, is essentially no remedy at all. This is somewhat equivalent to determining that holders of non-proprietary information cannot exclude others from accessing such information, even if it is stored on a protected computer and access rights with respect to such information have been revoked.[175]

This was the case in *hiQ Labs, Inc. v. LinkedIn Corp.* There, a district court in the Ninth Circuit granted hiQ injunctive relief requiring LinkedIn to cease preventing access to non-proprietary information on LinkedIn's servers.[176] It is true that the court did not discuss this as a question of remedies, rather as part of the cause of action, determining that LinkedIn did not have a valid CFAA claim against hiQ.[177] Its decision was based on the premise that when non-proprietary information is publicly available, access rights cannot be later revoked leading to an unauthorized access to such information.[178]

It is difficult to explain, however, why the differentiation between publicly available and password-protected *non-proprietary* information is justified. If we believe that non-proprietary information should not be restricted by legal boundaries—either under an economic analysis explaining that the costs of allowing the

intellectual property law.

[174] *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1063, 1068–70 (9th Cir. 2016) (finding a violation of the CFAA where Power Ventures accessed Facebook through Facebook's users and, in so holding, effectively treated Facebook's users' profiles and personal emails as property); hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1112–14 (N.D. Cal. 2017) (finding no violation of the CFAA where hiQ accessed publicly available information on LinkedIn).

[175] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1112–14.

[176] *See id.* at 1120.

[177] *See id.* at 1114, 1120.

[178] *See id.* at 1113–14.

de facto appropriation of such information are higher than the costs of increased investment in technological fences,[179] or under an autonomy analysis explaining that if we have no right in the information, everyone else's freedom to access such information should be secured[180]—then this should be the conclusion both for publicly available non-proprietary information as well as for non-public, or even password-protected non-proprietary information.

At first glance, this seems to be an extreme position that, while being coherent with the underlying theories for protecting the non-proprietary information itself, is in direct contradiction with the current statutory language and does not take into account the computer owner's interest to prevent access to her computers for other purposes that may lead to damage to or appropriation of proprietary information.[181]

The question is whether the access provision should be contextualized in the sense that an unauthorized access for the purpose of obtaining information would be actionable only if the computer owner (or third parties on his behalf, such as customers or end-users) has a proprietary interest in such information. A more careful look at the legislative history shows that this may be supported by the legislator's original intention.[182] The Senate Report seems to contextualize the use of information by stating that:

> [The access provision] would ensure that the *theft* of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected. . . .
>
> The seriousness of a breach in confidentiality depends, in

---

[179] *Cf*, Richard Posner, J., *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 472–73 (1992) (demonstrating the utility of a cost-benefit analysis in the field of trade secret misappropriation).

[180] *See, e.g.*, Yochai Benkler, *Siren Songs and Amish Children: Autonomy, Information, and Law*, 76 N.Y.U. L. REV. 23, 61–62 (2001) ("[D]espite the limited support autonomy may derive from property rights that individuals have in information products, pervasive recognition of property rights in the information environment imposes an overall cost on autonomy . . . there is one tremendously ubiquitous and useful commons: the public domain in information, wherein all pieces of information, or uses of them, are generally privileged to all."); J.J. Britz, *The Various Ethical Issues Regarding Access to Information*, *in* ETHICS AND ELECTRONIC INFORMATION IN THE TWENTY-FIRST CENTURY 12 (Lester J. Pourciau ed., 1999) ("[I]t is necessary to understand the fundamental relationship between people and information itself. This relationship satisfies a basic human need to give meaning to reality. However, without access to information, it would be impossible. In this regard, information is our lifeblood, the vital core that develops and enhances the quality of life.").

[181] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (a) (2018); Benkler, *supra* note 180, at 61–62; Britz, *supra* note 180, at 12.

[182] *See* S. REP. NO. 104-357, at 7–8 (1996).

> considerable part, on the value of the information *taken*, or on what is planned for the information after it is obtained.[183]

It is therefore evident that the legislator did take the nature of the "taken" information into consideration for the purpose of the access provision.[184] Moreover, by categorizing the action as theft, a presumption about ownership is more than warranted.[185] Therefore, a conclusion that the access provision does not apply when the obtained information is not at all protected, could fit the legislative history and therefore also the statutory language.

B. Injunction and Enforcement Costs Only

The CFAA very clearly affords plaintiffs the option to seek injunctive relief and actual damages for violations.[186] It is rather natural that a plaintiff enforcing a statutory right granted to it will have the option to seek actual damages and potentially injunctive relief to prohibit the defendant from violating its rights again.[187]

It seems very difficult to challenge the justification for granting damages for actual costs and harm resulting from violations of the access provision.[188] After all, if under an applicable doctrine a prohibition was violated, any direct damages (or costs) should generally be paid to the plaintiff.[189] It is therefore unsurprising that courts are willing to grant CFAA plaintiffs actual damages and costs related to the violation. The most basic form for this is the payment of enforcement and restoration costs with respect to the unauthorized access to the plaintiff's computer.[190] This was the case in *Power Ventures*. Where, upon remand, the court granted Facebook the actual costs (to the tune of 79,640.50 dollars) it incurred for monitoring Power Ventures' violations and enforcing its rights.[191]

The more interesting question under this remedies model is whether, in the circumstances discussed in this article, injunctive

---

[183] *Id.* (emphasis added).

[184] *See id.*

[185] *See id.*

[186] *See* 18 U.S.C. § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

[187] *See id.*

[188] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1070 (9th Cir. 2016).

[189] *See id.*; 18 U.S.C. § 1030(c).

[190] *See, e.g.*, *Facebook, Inc.*, 844 F.3d at 1070 (remanding to the district court to consider injunctive relief and the appropriate calculation of damages).

[191] *See* Facebook, Inc. v. Power Ventures, Inc., 252 F. Supp. 3d 765, 781 (N.D. Cal. 2017).

relief should be granted. Generally, courts have discretion to grant or deny permanent injunctive relief.[192] A party seeking a permanent injunction must fulfill the four-part test showing:

> (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.[193]

But how should these factors be weighed in the context of an access provision violation?

In *Power Ventures*, the district court granted Facebook injunctive relief twice.[194] In the first round, it was mainly due to Power Ventures' CAN-SPAM violations, which are beyond the scope of this article.[195] On appeal, the Court of Appeals vacated the injunction and remanded the case to the district court to discuss the injunction once more due to the fact that the CAN-SPAM violations had, for the most part, been reversed.[196] On remand, the district court dedicated an analysis to Facebook's request for injunctive relief based on the CFAA violation.[197] Assessing the irreparable harm factor, the court's main justification was that Power Ventures "interfered with Facebook's right to control access to its own computers and have acquired data to which Defendants have no lawful right."[198] The second reasoning used by the court is that injunctive relief is required due to the concern from recurring violations by Power Ventures.[199] This reasoning was applied to the other three factors as well, namely, irreparable harm, inadequacy of money damages and balance of hardship.[200]

We will not engage with the court's second reasoning in this Article, although it is questionable whether it could be directly applied to the

---

[192] eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

[193] *Id.*

[194] *See* Facebook, Inc. v. Power Ventures, Inc., No. 08-CV-5780-LHK, 2013 U.S. Dist. LEXIS 137890, at *66 (N.D. Cal. Sept. 25, 2013); Facebook, Inc. v. Power Ventures, Inc., 252 F. Supp. 3d 765, 785 (N.D. Cal. 2017).

[195] *See Facebook, Inc.*, 2013 U.S. Dist. LEXIS 137890, at *24–25, *54, *65–66, *69.

[196] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1058, 1062, 1065 (9th Cir. 2016).

[197] *See Facebook, Inc.*, 252 F. Supp. 3d at 772, 781.

[198] *Id.* at 782.

[199] *See id.*

[200] *See id.* at 782–85.

determination of irreparable harm. But the court's first reasoning is uneasy. Based on the discussion thus far, we can question what exactly is the irreparable harm suffered by plaintiffs in unauthorized access cases, specifically when only non-proprietary information is accessed. The district court in *Power Ventures* relied on the fact that Power Ventures did not have a lawful right to acquire Facebook's data.[201] But is this really the case? If this was merely non-proprietary data, then it was in the public domain and there was no legal restriction on acquiring or using such data.[202] Therefore, the fact that non-proprietary information was used seems like an unpersuasive consideration in the assessment of irreparable harm.

Under the approach suggested in this Article, the violation in cases such as *Power Ventures* entails solely the breaching of a legally recognized border. Accordingly, as noted above, costs incurred in order to protect the legal boundary from the unauthorized breach can be attributed to the violation.[203] However, monetary damages are likely to be adequate to compensate for such harm or that there is a severe imbalance of hardship.[204] Conversely, disadvantages stemming from the use of non-proprietary information are legally irrelevant to the question of remedies, as compensation for these would, in practice if not in theory, create a legal right in the information itself.[205] To return to our empty house analogy, one might be liable for the costs incurred to prevent a trespasser's entry to someone's house, but not for the enjoyment of sunlight or the breathing of air when inside the house.

C. Lost Profits, Restitution, and Full Disgorgement of Profits

At the other far end of the spectrum, we can think of a remedies model that includes not only injunctive relief, but also compensation for lost profits, full restitution, and disgorgement of profits related to

---

[201] *Id.* at 782.

[202] *Compare* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1109, 1113 (N.D. Cal. 2017) (explaining that where access is publicly available courts are hesitant to find access to be "without authorization") *with Facebook*, 252 F. Supp. 3d at 768–69 (describing Facebook's claim that its data and information was proprietary, and therefore, it was not in the public domain and subject to legal restrictions).

[203] *See e.g.*, *Facebook*, 252 F. Supp. 3d at 777–78 (finding that attorneys' fees and investigation costs were compensable under the CFAA claim).

[204] *Cf.* Kholekile L. Gwebu et al., *Understanding the Cost Associated with Data Security Breaches*, PAC. ASIA CONF. ON INFO. SYS. (2014) (concluding that data security breach damages mostly arise from damage compensation and litigation costs).

[205] *Cf.*, *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1109, 1113, 1120 (ordering LinkedIn to remove barriers preventing hiQ from accessing or using public profiles and information designated public on LinkedIn's website).

the unauthorized access.[206] If we take another look at the statutory language of the CFAA, this model could find support. The CFAA provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[207] This means, at least at first glance, that any damage or loss caused by a violation of the CFAA, including a violation of the access provision, entitles the plaintiff to compensation for such damage or loss. Losses could obviously include both actual losses of property or value, but also lost profits.[208]

The question this model raises, much like the other alternative models, is what exactly would be considered a damage or loss. As explained in the second model, it is rather easy to support the compensation for actual damage to the information systems of the plaintiff due to an unauthorized access, including restoration and investigation costs.[209] But can a wider understanding of losses be supported with respect to the access provision? Could restitution and the disgorgement of profits gained by the defendant from use of information obtained by unauthorized access be justified for a CFAA violation? Given that the basis for the profits gained by the defendant and the profits lost by the plaintiff are based solely on the non-proprietary information, it is difficult to support this concept of losses for such unauthorized access.[210]

These questions arise in cases such as the *hiQ Labs* case. It is undisputed that hiQ used LinkedIn's information, obtained by unauthorized scraping of LinkedIn's computers, for the purpose of supporting its business model and potentially making significant gains.[211] Under a very basic understanding of the unjust enrichment doctrine, if the value hiQ gained from using LinkedIn's information is "at the expense" of LinkedIn,[212] then these gains and profits should

---

[206] *See* 18 U.S.C. § 1030(e)(11), (g) (2018) (explaining the circumstances under which a party can claim damages or losses from a data breach under CFAA).

[207] 18 U.S.C. § 1030(g).

[208] *See* 18 U.S.C. § 1030(e)(11).

[209] *See* 18 U.S.C.S § 1030(e)(11); *see also* Facebook, Inc. v. Power Ventures, Inc., 252 F. Supp. 3d 765, 773 (N.D. Cal. 2017) (relying on the CFAA's definition of loss to award damages including investigation and restoration costs).

[210] *See e.g.*, *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1120 (enjoining LinkedIn from preventing hiQ's access to non-proprietary public information).

[211] *See id.* at 1104.

[212] *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 42 cmt. a (AM. LAW INST. 2011) ("Section 42 describes the restitution claim that underlies the recovery of profits or use value following unauthorized interference with . . . rights to control the use of any . . . information . . . protected by local law against misappropriation.").

be returned to LinkedIn.[213]

However, the underlying assumption is that the information obtained from LinkedIn is non-proprietary.[214] That is, that the refusal to grant property in the information was an affirmative decision, as opposed to an oversight or a failure of the law to catch-up with technology. Given this decision, it is difficult to explain, under both common legal theories and the unjust enrichment doctrine, why LinkedIn should be compensated for the use of such information.[215] If the information is non-proprietary, it is difficult to explain the protected interest that LinkedIn has in the information itself, as opposed to its computer systems.[216] Hence, it is also difficult to explain why such gains and profits are made at the expense of LinkedIn.[217] If the information is non-proprietary—say, because it is not protected under copyright, trade secret, or any other intellectual property doctrine—any person who obtains such information is free to use it.[218]

Courts have not yet addressed the option to obtain such extensive remedies for a violation of the CFAA access provision.[219] This is mainly because plaintiffs have not articulated these types of remedies.[220] For example, as discussed above, in the *Power Ventures*

---

[213] *See id.* § 42 cmt. d ("As in every other case of profitable wrongdoing, restitution by the rule of § 42 allows the claimant to recover the benefits derived by the defendant from interference with the claimant's rights. Because a claimant entitled to disgorgement would also be entitled to damages, the practical result is that the claimant may recover either damages or profits, whichever is greater.").

[214] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1106 n.2 ("LinkedIn does not claim a proprietary interest in its users' profiles.").

[215] This much is well reflected in the Restatement's comments. *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 42 cmt. b ("The law of restitution does not define the substantive rules of ownership on which a claim for infringement or misappropriation necessarily rests. The rule of this section depends on a body of law that defines the underlying entitlements, just as the rule of § 40 (describing restitution for trespass or conversion) depends on a body of law that defines ownership rights in tangible property.").

[216] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1107.

[217] *See id.*

[218] *Policies and Procedures—Proprietary vs Non-proprietary Projects*, NAT'L INST. STANDARDS AND TECH. (2016), https://www.nist.gov/cnst/nanofab/policies-and-procedures-proprietary-vs-non-proprietary-projects.

[219] *See* Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 189 (2011) ("[T]he CFAA's complexity makes it a veritable mine-field of procedural and substantive requirements that must be satisfied in order to successfully assert and ultimately prevail on a CFAA claim. To add to its complexity, the CFAA is a relatively new body of law and its jurisprudence is continuing to evolve in a way that often makes its provisions unpredictable from case to case and court to court[.] No one can predict exactly how courts will apply the CFAA to each case, for it is not static.").

[220] *See e.g.* U.S. Gypsum Co. v. Lafarge N. Am., 670 F. Supp. 2d 737, 744 (N.D. Ill. 2009) (finding that Plaintiff did not articulate a sufficient basis for damages suffered outside the scope

case, Facebook sought damages only for actual enforcement expenses (which were ultimately granted to it).[221] However, in *Craigslist, Inc. v. RadPad, Inc.*, which is a continuation of the *3taps* case discussed above, the court granted Craigslist damages for breach of contract (the contract being Craigslist's terms of use) in the amount of $160,000 without accounting for the actual losses caused to Craigslist.[222] The court granted Craigslist compensation "for breach of craigslist's Terms of Use based on collecting personal information ($1 for each email address and $1 for each phone number) from 80,000 emails."[223] The court's willingness to grant Craigslist damages for unauthorized use of information that obviously does not belong to Craigslist is one step closer to the idea of granting full restitution and disgorgement of profits for the obtained information under a CFAA violation.[224]

V. WHAT IS THE RIGHT MODEL?

We can now turn to review the alternative models presented above through a normative lens and outline the right remedies model for violations of the CFAA access provision, in circumstances where no proprietary information was taken. Our analysis will be based on the previously discussed theoretical justifications of the CFAA access provision and of laws protecting boundaries in general.

A. Rejecting the Restitution and Disgorgement of Profits Model

We can begin the review by dismissing one of the models—full restitution and disgorgement of profits. As was already hinted, while this model could potentially be supported by the statutory language of the CFAA, it conflicts with both theory and legislative history in circumstances of unauthorized access absent misappropriation.[225] As

of actual damage or loss).

[221] *See* Facebook, Inc. v. Power Ventures, Inc., 252 F. Supp. 3d 765, 774, 780 (N.D. Cal. 2017).

[222] Craigslist, Inc. v. RadPad, Inc., No. 3:16-cv-01856-CRB, 2017 U.S. Dist. LEXIS 218351, at *7 (N.D. Cal. 2017).

[223] *Id.*

[224] *See id.* Craigslist users' personal information belongs to the users and not to Craigslist. In fact, it is questionable whether Craigslist even had standing with respect to the protection of its users' personal information. In addition, a similar argument was raised by LinkedIn in the *hiQ Labs* case and was rejected by the court. There, the court determined that the actual privacy interests of LinkedIn users in their public data are "uncertain at best." hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1107 (N.D. Cal. 2017). It is interesting to note that Craigslist was awarded over 20 million dollars for copyright infringement, by assigning postings of its users to Craigslist for the purpose of copyright enforcement.

[225] *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 42 cmt. e (2011)

a basic principle, no restitution could be justified if nothing has been taken from the plaintiff.[226] In our case, although information is indeed obtained from the plaintiff's computer, it is not legally "taken" because such information was not the property of the plaintiff to begin with. Under both main theories—economic analysis and autonomy based theory—there should be no remedy for the taking of non-propprietary information. As explained earlier, the cost-benefit analysis that determined that such information should not be legally protected also implies that keeping the information in the public domain is more beneficial than allowing the information to be privately owned.[227]

Under autonomy based theory, if we decide that there are some sorts of information that all people should have the freedom to use as part of their basic freedom to act as purposive human beings, then we cannot justify any compensation to the holder of such information merely for its use by others.[228] As already mentioned, the legislative history supports this stance too.[229] The Senate Report for the legislation of the access provision specifically contextualized this violation depending on the information taken.[230] Therefore, if the information taken is unprotected by the law, the legislative history supports absence of restitution remedies for its taking.

Rejecting disgorgement of profits as a potential remedy also follows directly from the above reasoning. If we believe that nothing has been legally taken as part of an unauthorized access, then, if the defendant used the obtained non-proprietary information for profit, such profit is legally unrelated to the unauthorized access and to the plaintiff's rights with respect to its computers.[231] We believe, therefore, that neither restitution nor disgorgement of profits for non-proprietary information obtained as part of an unauthorized access should be available for the plaintiff as a valid remedy.

B. The Private-Public Dichotomy

Before reviewing the other two models—no remedies and

(explaining that misappropriation is a requirement in determining remedy); *see also* S. REP. NO 104-357, at 8 (1996) (noting that the procurement of information minimal in value is merely a misdemeanor).

[226] *See* Harker Heights v. Sun Meadows Land, Ltd., 830 S.W.2d 313, 317 (Tex. App. 1992) ("Restitution involves restoring property or money taken from the plaintiff.").

[227] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1113, 1120; Hunter, *supra* note 20, at 443–44.

[228] *See, e.g.*, Benkler, *supra* 193, at 61–62; Britz, *supra* note 180, at 12.

[229] *See* S. REP. NO 104-357, at 8 (1996).

[230] *Id.*

[231] *See id.*

injunction and enforcement costs—which we believe may be applicable to a certain extent, we suggest a distinction that could help assess different circumstances under the underlying theories and that would perhaps lead to different conclusions. The distinction is between access to publicly available non-proprietary information and access to private, non-public, non-proprietary information.[232] At first glance, this distinction may seem irrelevant. In both cases, only non-proprietary information is obtained.[233] However, since the subject matter of the CFAA, and the access provision specifically, is the unauthorized access to computers,[234] we believe that the private-public dichotomy, if calibrated properly, could be helpful in tracing protected interests in the computers (or boundaries) themselves, regardless of the type of information contained in them.

The private-public dichotomy was suggested by the court in *hiQ Labs* for the purpose of differentiating the case from the previous *Power Ventures* case, and thus justifying the result that differed from the court of appeals' guiding decision.[235] The court in *hiQ Labs* suggested that in the case before it, the information obtained from LinkedIn was publicly available even before it was obtained by hiQ.[236] In contrast, in the *Power Ventures* case, Facebook's information was password protected, in the sense that one had to create a user account to get access to such information.[237] While we believe that the standard that the *hiQ Labs* court suggested to distinguish between private and public information is wrong, we think that there is merit in making this type of distinction. For the purposes of this Part, when we refer to private information, we mean information that was not communicated, or intended to be communicated, to an indeterminate public by the holder of that information. An example would be a corporation that holds a database of non-proprietary information and wants to share such information with two specific other businesses via a secure connection. In contrast, we believe that offering to communicate

---

[232] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1109, 1113 (N.D. Cal. 2017).

[233] *See id.* at 1109.

[234] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) (2012).

[235] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1109–10, 1113.

[236] *See id.* at 1112–13.

[237] *See* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1062–63 (9th Cir. 2016); *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1109 ("[N]one of the data in *Facebook* or *Nosal II* was *public* data. Rather, the defendants in those cases gained access to a computer network (in *Nosal II*) and a portion of a website (in *Power Ventures*) that were protected by a password authentication system. In short, the unauthorized intruders reached into what would fairly be characterized as the private interior of a computer system not visible to the public."); Kerr, *supra* note 20, at 1171.

certain information to an indeterminate public makes such information publicly available, regardless of whether the information is password protected. Therefore, for example, allowing any person to create a password protected account and obtain access to non-proprietary information will be considered offering an indeterminate public access to such information.[238] Password protection itself (or any other protective measures for this purpose) does not make the information private.

C. Appropriate Remedies for Unauthorized Access to Private Non-Proprietary Information

Moving on with our review of the alternative models, we believe that the injunction and enforcement costs model may be applicable, specifically in cases of unauthorized access to private non-proprietary information.

Autonomy based theory leads to the intuitive understanding that unauthorized uses of computers should be prevented.[239] After all, if I choose not to allow anyone to access something that is mine (my computer), I should be allowed to prevent others from doing so as part of exercising my freedom.[240] In the case of private non-proprietary information, the owner of the computer storing such information allows only selected and identified people to access her computer.[241] In doing so, she manifests her will to restrict the access to such computer only to these people and no one else.[242] Such choice demonstrates the computer owner's explicit concern with access to her computer by others not previously approved by her.[243] This justifies, in the most basic way, granting a preventive remedy such as injunction.

From an economic perspective, the private-public dichotomy serves as a proxy to predict the level of certainty regarding the type of information contained in computers.[244] If a computer (or a segment thereof) is made publicly available, we can determine whether the information disseminated to the public is proprietary or not, and, as

---

[238] *See id.* at 1172–73 (noting that Facebook and similar websites require authentication for access); *cf.* Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (U.S. 2017) (noting that social media websites like Facebook are quintessential public fora akin to public streets or parks).

[239] *See* Kant, *supra* note 131, at 403.

[240] *See id.* at 409.

[241] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1109 (N.D. Cal. 2017).

[242] *See id.*

[243] *See id.*

[244] *See, e.g.*, United States v. Nosal, 844 F.3d 1024, 1030–31 (9th Cir. 2015).

a result, whether or not it could be freely taken or used.[245] However, if the computer is kept private, we have no way of determining, *ex ante*, whether the contained information is proprietary or not.[246] In fact, we can assume, with a rather high level of certainty, that at least some information in such computer is proprietary (or protected by other interests, such as privacy).[247] Therefore, allowing access to private computers poses a much greater risk of obtaining proprietary information through unauthorized access (thus, leading to actual harm and loss under the CFAA). This difference in expected harm justifies different remedies, and in the case of private computers, injunctive relief.

This analysis is in line with the four-factor analysis for injunctive relief under *eBay Inc. v. MercExchange, L.L.C.*[248] With respect to the irreparable harm factor, given that the protected interest is the choice of the computer owner not to share access to the computer with the public, the fact that an unauthorized person gained access to the computer violated such choice in an irreparable manner.[249] Respectively, as this protected interest is highly subjective, it may not be possible to compensate for such violation in monetary damages.[250] Considering the balance of hardship, given that the computer is private and the accessor cannot rely on its contents to develop any type of protected interest, and that, on the other hand, absent an injunction, the entire right of the computer owner will be violated, this weighs in favor of the computer owner.[251] As for the public interest factor, we believe that the ability to keep computers private, should one want to, on the one hand, and dis-incentivizing random unauthorized access to computers, on the other, are both in the public's interest.

---

[245] *See Policies and Procedures—Proprietary vs Non-proprietary Projects*, *supra* note 218.

[246] *See id.*

[247] *See id.*; Andrew T. Winkler, *Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era*, 39 RUTGERS COMPUTER & TECH. L.J. 194, 194 (2013).

[248] eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

[249] *See* Facebook, Inc. v. Power Ventures, Inc., 252 F. Supp. 3d 765, 782 (N.D. Cal. 2017); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1067–68 (N.D. Cal. 2000).

[250] *See Facebook, Inc.*, 252 F. Supp. 3d at 783; *eBay, Inc.*, 100 F. Supp. 2d at 1066.

[251] *See Facebook, Inc.*, 252 F. Supp. 3d at 784, 785; *eBay, Inc.*, 100 F. Supp. 2d at 1069, 1070; FXDirectDealer, LLC v. Abadi, No. 12 Civ. 1796 (CM), 2012 U.S. Dist. LEXIS 49588, at *19 (S.D.N.Y. Apr. 5, 2012).

D. Appropriate Remedies for Unauthorized Access to Publicly Available Non-Proprietary Information

In contrast to private non-proprietary information, we believe that in the case of publicly available non-proprietary information, the no-remedy model prevails. This is because the concerns that justify certain remedies in cases of private computers do not exist once the computer owner grants the public access to the computer.[252]

Under autonomy based theory, the choice to grant an indeterminate public access to a computer demonstrates that the computer owner's autonomy is not violated merely by the public's access to the computer.[253] This also means that once access has been granted to the public, the autonomy concern cannot be reinstated simply because of the access of a specific individual to the computer.[254] The fact that one or more individuals access a computer, while it is available to the entire public, does not raise autonomy concerns in itself.[255] The autonomy concern could be reinstated if a legitimate reason exists.[256] This could be, for example, illegal behavior of a certain individual while accessing the computer.[257] However, in the case of non-proprietary information, the use of such information could not serve as a valid reason to revoke access.[258]

From an economic perspective, when a computer is made publicly available, we can determine, *ex ante*, whether the information disseminated is proprietary or not.[259] Thus, if we are certain that the potential unauthorized access is only to non-proprietary information, the cost-benefit analysis conducted above justifies granting access to the information in order to minimize protection costs, thus, maximizing social benefits by utilizing the non-proprietary

---

[252] *See* hiQ Labs, Inc. v. LindkedIn Corp., 273 F. Supp. 3d 1099, 1109, 1113 (N.D. Cal. 2017); Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 649 (E.D. Pa. 2007) (collecting cases).

[253] *See* Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) (citing Int'l Airport Ctrs. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006)); *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1110–11.

[254] *See, e.g.*, *Plute Homes, Inc.*, 648 F.3d at 304 (citing *Citrin*, 440 F.3d at 420); *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1110–11.

[255] *See Plute Homes, Inc.*, 648 F.3d at 304 (citing *Citrin*, 440 F.3d at 420); *hiQ Labs, Inc.*, 273 F. Supp. 3d at 1110–11.

[256] *See* Sandvig v. Sessions, 315 F. Supp. 3d 1, 26–27 (D.D.C. 2018).

[257] *See id.*

[258] *See* Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 649 (E.D. Pa. 2007) (collecting cases); *Policies and Procedures – Proprietary vs Non-proprietary Projects*, *supra* note 218.

[259] *See Policies and Procedures – Proprietary vs Non-proprietary Projects*, *supra* note 218.

information efficiently.[260]

The same conclusion could be reached by weighing the four factors of the injunctive relief test.[261] In the case that the computer was already made publicly available, it is difficult to explain why the access of one individual or another causes irreparable harm (absent a legitimate reason to revoke access, as explained above).[262] Remember that the use of the non-proprietary information by itself cannot be considered harm at all, as it is not protected under any legal right.[263] It also follows that the question of available monetary damages is irrelevant as well, as no actual damage occurred, and even if it did, it could be easily remedied by compensation.[264] With respect to the balance of hardships, in contrast to the discussion on private computers, here, the computer owner has no identifiable protected interest with respect to specific access to the computer, whereas the accessor, if prevented from such access, loses the possibility to realize any interests it developed in reliance on access to the non-proprietary information, including goodwill and reputation losses.[265] In this case, the public interest also supports no injunctions, as it is in the public interest that non-proprietary information be freely accessed by all, and since such information was already made publicly available, there is little interest in preventing a specific access to the computer.[266]

We should further note that, because the computer owner has no right to prevent access to the publicly available non-proprietary information, naturally there is no justification to afford her any monetary damages for the technological means acquired to monitor and prevent the unauthorized access.[267]

The above analysis may lead to the conclusion that in cases of unauthorized access to publicly available non-proprietary information, the access provision itself is not violated, and that there is no right to restrict access to begin with. This is due to the basic understanding that no right could exist without remedy.[268] We do

---

[260] *See* Calabresi & Melamed, *supra* note 152, at 1092.

[261] *See* eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

[262] *See* hiQ Labs, Inc. v. Linkedin Corp., 273 F. Supp. 3d 1099, 1112–13 (N.D. Cal. 2017) (citing Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016)).

[263] *Cf.* Facebook, Inc. v. Power Ventures, Inc., 252 F Supp. 3d 765, 782 (N.D. Cal. 2017).

[264] *See id.* at 765, 773.

[265] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1106, 1107, 1109.

[266] *See* U.S. Golf Ass'n v. St. Andrews Sys., 749 F.2d 1028, 1035 (3d Cir. 1984); *hiQ Labs Inc.*, 273 F. Supp. 3d at 1105, 1113.

[267] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1112–13; *Facebook, Inc.*, 252 F. Supp. 3d at 773.

[268] *See* Marbury v. Madison, 5 U.S. 137, 163 (1803).

not believe, however, that the right to restrict access could be so easily dismissed.

We suggest that the right to prevent access under the CFAA access provision could be fulfilled by a different intermediate remedies model allowing courts to determine fees for accessing the computer. In economic terms, this means that while the computer owner has a right to exclude access, this right is protected solely by a liability rule.

In Part III we suggested that Calabresi and Melamed's Cathedral analysis justifies protecting the right of the computer owner to restrict access to the computer through a liability rule.[269] The reason for this was that if we leave it to the parties' own negotiations, a holdup problem is likely to occur, which is likely to prevent the execution of many efficient transactions.[270]

A useful analogy is easement of necessity. In general, an owner of a landlocked parcel of land—land without access to public roads—will be granted an easement allowing for reasonable access.[271] The granting of the easement may be based on either contractual or statutory grounds, and it is the latter that we shall focus upon.[272] Statutory easements of necessity "vary in several particulars, but each requires the claimant to establish present necessity and to compensate the owner of the servient estate."[273]

---

[269] As a side note, it might be useful to briefly note why the Cathedral's fourth rule is inapplicable to this case. That is, if the law grants a right of access to the computer on which the information is stored, the computer owner would be unable to negotiate the purchasing of a right to exclude, as separate from the right to use the information. *See* Calabresi & Melamed, *supra* note 152, at 1116–17. Thus, *prima facia*, it seems that an inverse holdout problem occurs when the law provides for a right to access, and there the right to access information should also be protected by a liability rule. *Id.* That is, the 'owner' of the cyberspace in which information is stored should be able to exclude others and pay a judicially determined fee. *Id.* The reason that this inverse scenario is not symmetrical is that here, there is no good reason to separate exclusion from use. *Id.* That is, in the above scenario, the public holds both the right to access the cyberspace and the right to use the non-propitiatory information stored in it. Accordingly, by selling the right to access, the seller also effectively sells his right to use the information and it stands to reason that this too should be reflected in the negotiated price.

[270] *See id*. at 1116; Saul Levmore, *Takings, Torts, and Special Interests*, 77 VA. L. REV. 1333, 1338–39, 1139 n.8 (1991).

[271] *See* JOSEPH W. SINGER, PROPERTY LAW: RULES POLICIES, AND PRACTICES 387 (3d ed. 2002); *see, e.g.*, Yun-chien Chang, *Hybrid Rule: Hidden Entitlement Protection Rule in Access to Landlocked Land Doctrine*, 91 TUL. L. REV. 217, 230 (2016).

[272] *See e.g.,* Chang, *supra* note 271, 230–32 (2016) (discussing both types of easements and suggesting that statutes allowing for easement of necessity exist in 22 states). Although the Section of the Restatement on servitudes deals with the assertion that "servitudes by necessity are acquired in land once held in a common ownership without payment of additional compensation," it recognizes that statutes "in a number of states provide a broader solution by permitting the owners of landlocked property to purchase necessary access rights regardless of the manner in which the landlocking occurred." RESTATEMENT (THIRD) OF PROPERTY (SERVITUDES) § 2.15 cmt. a (2000).

[273] JON W. BRUCE & JAMES W. ELY, JR., THE LAW OF EASEMENTS AND LICENSES IN LAND §

The rationale for granting an easement of necessity is one of public policy.[274] One way to explain the easement is that because the value of a landlocked land without a right of access is severely diminished, easement of necessity could be thought of as a way to prevent economic waste.[275] However, this argument in itself does not explain why the Coase theorem would not apply.[276] That is, why would the parties be unable to negotiate about the granting or restriction of the right to access, regardless of the legal rule? Easement of necessity is therefore better and more commonly understood as a liability rule created to resolve a holdout problem.[277]

In the terms discussed above, because the locked land is worthless without the ability to access it, rather than negotiating about the right to access, the parties would negotiate about the value of the land itself.[278] In practice, this is equivalent to giving the owner of the property surrounding the landlocked land rights in the landlocked land itself.[279] As one can observe, this is precisely the situation when it comes to the ownership of a computer that essentially 'landlocks' non-propriety information. Here, it is the non-propriety information that is cut-off from the 'information high-way' by the computer on which it is stored.

The similarities between the two situations suggest that the same legal solution would be applicable to both. As we mentioned, owners of landlocked land are likely to be granted a court-ordered easement of necessity.[280] Such easement is usually limited to reasonable access and may be subject to compensation to the owner for the land

4.02[4] (1995). *See also* SINGER, *supra* note 271, at 389 ("Some states have enacted statutes empowering the owner of a landlocked parcel to obtain an easement over neighboring land for access to a public road by application to a public official and payment of compensation to the landowner whose property is burdened by the easement.") For state examples, *see* ALA. CODE § 18-3-1 (1982); ARK. CODE ANN. § 27-66-401 (1987); MASS. GEN. LAWS ch. 82 § 24 (1986); MO. REV. STAT. § 228.342 (1993); OR. REV. STAT. § 376.150-200 (2009); WASH. REV. CODE § 8.24.010 (1913).

[274] *See* SINGER, *supra* note 271, at 387–88.

[275] *See id.* at 388–89.

[276] *See* Coase, *supra* note 151, at 43, 44.

[277] *See* RESTATEMENT (THIRD) OF PROPERTY (SERVITUDES) § 2.15 cmt. a ("Public policy also justifies the rule because it avoids the costs involved if the property is deprived of rights necessary to make it useable, whether the result is that it remains unused, or that the owner incurs the costs of acquiring rights from landowners who are in a position to demand an extortionate price because of their monopolistic position."); Henry E. Smith, *Property and Property Rules*, 79 N.Y.U. L. Rev. 1719, 1737–38 (2004) (discussing easement of necessity); Stewart E. Sterk, *Neighbors in American Land Law*, 87 COLUM. L. REV. 55, 76 (1987) (discussing easement of necessity rules as a solution for bilateral monopoly).

[278] Ernest J. Weinrib, *Private Law and Public Right*, 61 U. TORONTO L.J. 191, 207–08 (2011).

[279] *See id.*

[280] *See* Levmore, *supra* note 270, at 1339 n.8.

deprived.[281] Applying this solution to access to publicly available non-propriety information, we find that access should be granted by a court order, which would allow for reasonable access, and should perhaps be subject to a fee.

Under the model we propose, any person would have the right to receive a court order allowing her to gain reasonable access to the public non-proprietary information, if such person can demonstrate that access would be used only for that purpose, and subject to the payment of an access fee. As with landlocked property, this solution is economically justified as it resolves the hold-out problem discussed above, while compensating the owner of the computer for its loss.[282] The remainder of this Part we therefore expend on the idea of 'reasonable' access and the determination of access fees, as well explain the model from the perspective of autonomy based theory.

First, the right to receive a court order allowing access to a computer containing public, non-proprietary information is justified from an autonomy perspective for the reasons discussed above in relation to the no-remedy model.[283] That is, given that the computer owner allowed access to the public, restriction of access has to be grounded on legitimate reasons that go beyond the mere access of a certain person.[284] Unless such reasons exist, courts should grant an order allowing access to the computer.

Turning to the reasonableness of access, we note that a complete economic analysis of the scope of reasonable access is beyond the scope of this Article. Nevertheless, at least intuitively, it seems to us that reasonable access would entail access *only* to the non-propriety information, but *also* for commercial use. Any less would mean that the legal rule provides the computer owner an unjustified advantage in the use of the information, given that the information is non-proprietary.[285] Any more might create an undue burden on the

[281] *See* F. T. Chen, annotation, *Extent and Reasonableness of Use of Private Way in Exercise of Easement Granted in General Terms*, 3 A.L.R.3d 1256, at 2a; Weinrib, *supra* note 278, at 207–08.

[282] *See* Levmore, *supra* note 270, at 1339 n.8; Weinrib, *supra* note 278, at 207–08.

[283] *See*, Benkler, *supra* 193 at 61–62; Gregory S. Alexander, *Property's Ends: The Publicness of Private Law Values*, 99 IOWA L. REV. 1257, 1286–87 (2014).

[284] *See*, Benkler, *supra* 193, at 61–62.

[285] *See* hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1109, 1113 (N.D. Cal. 2017) (finding that hiQ Labs could permissibly use the public information provided on LinkedIn's site for commercial purposes without being in violation of the CFAA). This is the case even when the accessor and the owner of the site is not using the information in the same manner, which is beneficial as it does not allow the owner of the site to dictate the possible usages of the information. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1060–61, 1067 (N.D. Cal. 2000).

computer owner.

To clarify, while access should be tailored to the requirements for reasonable commercial use, the use of information itself should not be restricted. To give a real property example, if reasonable commercial use requires a twelve-foot-wide road, then the easement should reflect as much, but use of the road should be allowed regardless of its purpose.[286]

Moreover, because the access required for reasonable commercial use will be granted, the threat of holdout would be diminished, and negotiations concerning access rights that exceed the needs of reasonable commercial use would be much more likely to succeed.[287] Accordingly, protecting the right to prevent excessive access by a property rule should not raise concerns.

The formula for determining adequate compensation follows the same lines. The compensation should reflect the expropriation of the access control to the computer and certain potential uses of it. In economic terms this compensation guarantees that the easement would not leave the property owner worse off.[288] From an autonomy perspective, compensating the computer owner for part of the land expropriated is justified, because it ensures that the freedom of the public is guaranteed by inflicting the minimum amount of harm to others.[289] No less important is the notion that compensation should not depend on the economic value of the use of the information—including any indirect economic effects such as loss of reputation or of consumer good will—as considering these will again grant the computer owner rights in the information itself.[290]

To complete our model, in circumstances in which a person was given notice by a computer owner denying him authorization to access the computer containing publicly available non-proprietary information, and such person chooses to nevertheless access the

---

[286] *See* Chen, *supra* note 281, at 2a, 11. Naturally, then, what amounts to reasonable commercial use and the scope of access required for it may change overtime. *See* Kerr, *supra* note 20, at 1147.

[287] *See* Chang, *supra* note 271, at 235–36.

[288] *See id.* at 240. Note that access would deny the owner the economic benefits of having sole access to the information, but because the owner of the computer had no right to these benefits to begin with, denying him such benefits does not harm him in the normative-legal sense.

[289] *See* Weinrib, *supra* note 278, at 207–08. Applying the idea of proportionality, Weinrib suggests that private necessity would allow only for the minimum interference with another's property to alleviate the state of the necessity, as well as a duty, to compensate for any harm such intervention caused. *See id.* at 206–10. This idea, as the above discussion shows, is indeed what our model suggests and is reflected in the way in which the easement of necessity doctrine is fashioned.

[290] *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1105–07, 1109.

computer without first securing a court order allowing him to do so, an easement of necessity would no longer be available for such person.[291] We believe that in such circumstances, courts should revert to the injunction and enforcement cost model presented above. This is because, as discussed, the judicial process is meant to ensure that access is requested only for the use of publicly available non-proprietary information in the computer and that there are no legitimate reasons to restrict it.[292] Thus, when a person fails to undergo such process, there is reason to assume that this may not actually be the case. Moreover, sanctioning those who fail to secure a court order will provide the incentives to secure one, rather than attempting to first access the computer without authorization.[293] And, while there are economic and autonomy based justifications to granting a right of access, these do not justify eliminating the ownership rights in the computer itself. Doctrinal support for this idea can be found in the application of easement of necessity as an equitable remedy.[294] Accordingly, requesting the affirmative injunction only after the attempts to illegally access the computer have failed suggest that it should not be granted.[295]

VI. CONCLUSION

This Article addressed the tension between the boundary protection that the CFAA access provision affords to privately owned computers and the public decision that some of the information contained in such computers is in the public domain and cannot be legally protected. We reviewed the doctrinal development of both common law's trespass to chattels and the CFAA access provision, and explained that while courts have a rather consistent account of what constitutes violations of the CFAA access provision, the discussion on the appropriate remedies is missing and the respective results are inconsistent. To address this gap, we suggested a novel basis for discussion of the theoretical justifications for protecting

---

[291] *See* Chang, *supra* note 271, at 220; eBay, Inc. v. Bidder's Edge Inc., 100 F. Supp. 2d 1058, 1062–63, 1068 (N.D. Cal. 2000).

[292] *See Policies and Procedures – Proprietary vs Non-proprietary Projects*, *supra* note 218.

[293] This reflects, to a certain extent, the course of events in the *hiQ Labs* case. There, after being revoked of its access to LinkedIn's computers, hiQ actively sought injunctive relief from the court asking to prevent LinkedIn from blocking its access to LinkedIn's computers. *See hiQ Labs, Inc.*, 273 F. Supp. 3d at 1103. While we believe that the court's justifications in *hiQ Labs* are at times imperfect and at times flawed, the result could be supported by the model suggested here.

[294] *See eBay, Inc.*, 100 F. Supp. 2d at 1067.

[295] *See id.* at 1062, 1068.

boundaries, regardless of whether they contain legally protected property, using both right-based and economic analysis as theoretical approaches.

Harnessing the conclusions from the theoretical discussion, we outlined a taxonomy of alternative remedies models for CFAA violations—no-remedies, injunctive relief and enforcement costs only, and full restitution and disgorgement of profits—we ruled out the restitution and disgorgement of profits model, as it contradicts the normative underpinnings of the CFAA. We then suggested the private-public dichotomy as a tool to choose between the remaining models in different circumstances. We argued that if the access to a computer is kept private, meaning that access is not granted to an indeterminate public, unauthorized access to such computer justifies injunctive relief and enforcement costs. However, if a computer is made accessible to an indeterminate public, no remedies should be granted for unauthorized access whose purpose was to obtain non-proprietary information. In addition, we explained that this rule should be subject to both the pre-obtaining of a judicial order granting such access and the payment of adequate access fees. Failing to meet these criteria, we argued, would result in reverting to the injunctive relief and enforcement costs model.