THE LAW OF THE ZEBRA

Andrea M. Matwyshyn†

ABSTRACT

At the dawn of internet law, scholars and judges debated whether a "law of the horse"—a set of specific laws addressing technology problems—was ever needed. Time has demonstrated that in some cases, the answer is yes. However, some courts are confused about the appropriate trajectory of contract law in technology contexts. Today, a technology-centric analysis threatens to subvert traditional contract law and the future of entrepreneurship, and circuit splits have emerged in what might be called an undesirable "law of the zebra." Do contracts that involve technology always require exceptional contract rules? In particular, does the use of a computer to breach a contract make the breach inherently worse in law? Using the Computer Fraud and Abuse Act ("CFAA") as a case study, this Article introduces a paradigm of "restrained technology exceptionalism" in contract law, a paradigm predicated on a return to traditional contract law principles and contractual supremacy over technology exceptionalist legal approaches. Applying the restrained technology exceptionalism paradigm to a circuit split concerning the CFAA, this Article then introduces a "privity" model bridging contract law with CFAA analysis, which inverts the traditional legal framing of the CFAA and contract relationship. It argues that where contract formation has occurred, the contract controls the relationship and only contract remedies are appropriate; both criminal and civil CFAA analysis becomes inapposite and should not be considered. Thus, the operative legal question is not whether contract breach revokes authorization in CFAA context. Rather, it is whether contract analysis is possible, thereby rendering the CFAA unnecessary and redundant in contractual contexts.

---

† Andrea M. Matwyshyn is an Assistant Professor of Legal Studies and Business Ethics in the Wharton School at the University of Pennsylvania and an affiliate scholar of the Center for Internet and Society at Stanford Law School. She can be reached at amatwysh@wharton.upenn.edu and wishes to thank the faculty of the Oxford Internet Institute and Notre Dame Law School, where she was a visitor during the writing of this Article. She also wishes to thank Colleen M. Baker, Tricia Bellia, Christina J. DeVries, Margaret F. Brinig, Ian Brown, Erik Goldman, Cathy Kaveny, Orin Kerr, Michael Kirsch, Randy Kozel, Greg Lastowka, Miluska Linares, Brian Martin, Jennifer Mason McAward, Mark McKenna, Jennifer Mueller, John Nagle, Paul Ohm, Frank Pasquale, Jeffrey A. Pojanowski, Marty Redish, John H. Robinson, Stephen F. Smith, David Schwartz, Marcia Tiersky, Julian Velasco, and Kevin Werbach for their helpful commentary and critiques of this Article.

TABLE OF CONTENTS

I. INTRODUCTION

In a seminal debate in the early days of internet law, Professor Lawrence Lessig and Judge Frank Easterbrook exchanged legal barbs over the question of whether the Internet deserves its own regulation. Judge Easterbrook referred to the suggestion of internet-specific approaches as tantamount in irrationality to suggesting a "law of the horse."[1] Professor Lessig, in turn, responded by identifying some spaces where existing legal frameworks fall short and suggesting what this "law of the horse" might look like.[2] Central to Lessig's argument was the primacy of private ordering and contract law.[3]

1. Easterbrook viewed crafting internet-specific laws to be an unnecessary enterprise, asserting that existing legal regimes can adequately accommodate any harms that arise in internet spaces. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208 (1996).

2. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999).

3. *Id.*

Today, almost fifteen years after that seminal debate, there is no doubt as to whether this "law of the horse" exists—it does, without question. In fact, since the Lessig–Easterbrook exchanges, Congress has passed various technology-focused statutory regimes.[4]

However, what has happened in the shadow of the "law of the horse" debates is perhaps partially what concerned Easterbrook at the time of his writing, at least in the context of contract law. Today, courts are derailing traditional contract law approaches with an overzealous focus on the role of technology in disputes. Instead of asking whether a technology-specific "law of the horse" should be crafted to fill gaps in existing law in technology contexts, courts now ask whether technology-specific approaches should usurp the traditional space of contract law. We have arrived at something more exotic and unexpected than the "law of the horse." We have entered the strange and strained realm of what might be dubbed the "law of the zebra."

An aphorism states "when you hear hoofbeats, think horses, not zebras."[5] When we turn to contract law inquiries in technology spaces, courts increasingly look for a metaphorical zebra, rather than a horse or nothing at all. Instead of using contract law in its traditional forms to resolve disputes, and supplementing it with technology-exceptionalist approaches only where true novelty exists, some courts now reach aggressively for technology exceptionalist approaches as a first cut.[6] These courts now seem to ignore the existence of a contract governing the exchange and instead focus on the presence of a computer.[7] At times this approach leads to intrajurisdictional conflict. A particular court may, on the one hand, ignore the novel challenges technology presents to contract formation.[8] But, on the other hand, that court may be quick to point to allegedly unique characteristics of the same technology when analyzing a question of breach.[9] As a result, contract law is becoming progressively more balkanized on technology issues, and, unsurprisingly, circuit splits have emerged. This Article calls for a revitalization of contract discourse around technology questions, and it

4. *See, e.g.*, Controlling the Assault of Non-Solicited Pornography And Marketing Act, 15 U.S.C. §§ 7701–7713 (2011) [hereinafter CAN-SPAM Act]; Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C. § 512 (2011)).

5. *World Proverbs*, SPECIAL DICTIONARY, http://www.special-dictionary.com/proverbs/keywords/zebra/ (last visited Feb. 28, 2012).

6. *See infra* Section II.A.1.

7. *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

8. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996).

9. *See Citrin*, 440 F.3d at 420.

cautions against crafting a "law of the zebra"—an undesirable body of law where technology exceptionalism triumphs over traditional legal paradigms.

Using judicial interpretation of the Computer Fraud and Abuse Act ("CFAA") as a case study of the looming "law of the zebra," this Article breaks with existing scholarship and advocates a decidedly contractarian analysis: a paradigm of "restrained technology exceptionalism." It also offers one operationalization of this paradigm: a "privity" model to address the circuit split with respect to contract breach and CFAA interpretation. Analysis of CFAA issues in the legal literature to date has primarily come from a criminal or property perspective. This Article adopts a different approach and examines the CFAA through the lens of contract law. It argues that if a contract exists between the parties, a contract inquiry must precede any CFAA analysis. Thus, the goal of this Article is not only to ask what is wrong with the CFAA, in particular. Instead, it asks a broader question: what has gone awry with contract law in technology contexts? Why have we wrongly permitted frameworks such as the CFAA to subvert traditional contract law with overreaching technology exceptionalism?

Part II introduces the current state of balkanization in contract caselaw around technology. Courts sometimes try to duck basic contract queries in technology cases; alternatively, they haphazardly apply technology exceptionalist analysis without a consistent paradigm. For example, courts currently tend to avoid technology exceptionalist analysis in questions of formation, but are sometimes quick to apply an exceptionalist analysis in breach. In fact, the opposite is more appropriate: while contract formation questions frequently warrant technology exceptionalism, a technology exceptionalist analysis is usually misguided in questions of breach. Next, Part II introduces one possible solution to these doctrinal challenges: a paradigm of "restrained technology exceptionalism" in contractual interpretation. This approach turns on traditional contract law concerns: freedom to contract, freedom from contract, damages as the primary remedy for harm, and preservation of private ordering in technology contexts.

Applying the restrained technology exceptionalist paradigm to the case study of the CFAA-contract law circuit split, Part III then asks a superficially simple breach question: should a breach of contract relating to a computer or network automatically provide the basis for a criminal charge of computer intrusion under the CFAA? Introducing four types of "contract hacker" cases, this Part argues that many courts are wrongly viewing contract breaches that involve computers as somehow fundamentally "worse" than or different from other contract breaches. Without any justification as to why contract damages alone are an inadequate remedy, these courts overzealously sanction defendants with CFAA penalties in addition to contract remedies.

Yet, in almost all cases, contract damages sufficiently address the information harms at issue. Hence, we witness the arrival of a "law of the zebra." Part III further argues that this type of "weaponized breach" analysis is highly undesirable as a matter of contract doctrine, contract theory, private ordering, and innovation and entrepreneurship policy. Finally, applying paradigms from developmental and social psychology theory, Part III postulates that courts' tendency to inconsistently exceptionalize breach in technology contexts is likely rooted in essentialism and confirmation bias rather than principle-driven contract law analysis.

Part IV offers a concrete operationalization of a model embodying the paradigm of restrained technology exceptionalism. Applying the principles articulated in Part III, Part IV proposes a "privity" model of contract and the CFAA. The privity model is predicated on a notion of contractual dominance in technology contexts; it provides a means for handling the four "contract hackers" introduced in Part III, while staying true to contract law first principles. When the alleged computer intruder and the information holder stand in contractual privity with each other, and when their agreement directly or indirectly contemplates the information in question, CFAA analysis is inappropriate. The court should only conduct a contract breach analysis. Part V concludes.

II. HORSES AND ZEBRAS: TOWARD RESTRAINED TECHNOLOGY EXCEPTIONALISM IN CONTRACT

In medical contexts, a "zebra" is a slang term used to refer to a surprising and rare diagnosis.[10] As this Part will explain, the way that some courts have addressed technology contracts is indeed both surprising and rare. In instances where applications of traditional contract law will suffice, courts nevertheless increasingly reach for technology-specific paradigms to trump traditional contract law analysis. Courts are hearing and expecting proverbial "zebras" where none actually exist.

In technology contexts, contract law has always been the most prevalent law. End user license agreements have existed almost as long as software, and since the early days of the Internet, terms of use have governed virtual spaces. Yet, in a strange inversion, technology exceptionalism now threatens doctrinal coherence in contract law.

Although it may have been possible in the past to ignore these doctrinal disagreements, such an approach is no longer sustainable. Circuit splits are

10. *See About Us*, ZEBRAMEDICINE, http://www.zebramedicine.net/about-us.html. (last visited Feb. 28, 2012).

emerging in ways that threaten the core of contract law and the future of the technology marketplace. To date, however, contract scholarship has offered few suggestions for doctrinal paradigms marrying contract law and technology questions successfully. This Part offers one possible solution: by recognizing four fundamental tenets of contract law challenged by technology, we can begin to craft a paradigm of "restrained technology exceptionalism" to guide future contract caselaw in technology contexts.

A. CONTRACTS + TECHNOLOGY = DOCTRINAL CONFUSION

Courts are struggling to understand the implications of technology for contract law. Should courts ignore contracts in some technology contexts in favor of other legal paradigms? Are contracts involving technology inherently special? Do they warrant their own exceptionalist contract law paradigms? Courts disagree on the answers to these questions,[11] and this disagreement now detrimentally affects everyday users of technology.

1. Confusion and Circuit Splits: b0rked Doctrine and Balkanization

Courts seem uncomfortable with contract law in technology contexts. Even the most contract-friendly of circuits now sometimes seem to contort their analysis to avoid conducting technology contract inquiries in technology contexts. For example, the Seventh Circuit—a circuit that has historically tended toward strict enforcement of contract terms even at the expense of equitable concerns[12]—sometimes appears to inexplicably duck contract analysis when technology is involved.[13] For example, *International Airport Center L.L.C. v. Citrin*, a somewhat recent case, should have involved a relatively simple question of breach: an employee failed to perform in accordance with his employment agreement and damaged information on his laptop in the process.[14] While a traditional breach analysis and a damages remedy would have sufficiently compensated the plaintiff for the harms

11. Andrea M. Matwyshyn, *Technology, Commerce, Development, Identity*, 8 MINN. J.L. SCI. & TECH. 515, 520, 523–24 (2007) (discussing how courts and scholars struggle generally to redress technology harms, as opposed to real-space harms).

12. For example, the unconscionability doctrine in the Seventh Circuit is particularly weak, essentially rejecting the role of substantive unconscionability in the analysis. *See, e.g.*, Nw. Nat'l Ins. Co. v. Donovan, 916 F.2d 372, 377 (7th Cir. 1990) (Posner, J.) (calling unconscionability an "umbrella term" for other traditional grounds to invalidate contracts).

13. On at least one occasion, the Seventh Circuit opted in favor of a convoluted agency analysis and invoked technology-specific legislation in lieu of a straightforward contract breach analysis. *See Citrin*, 440 F.3d at 420–21.

14. *Id.* at 420.

incurred,[15] the court instead resorted to a convoluted agency and computer intrusion analysis, ignoring the contract questions entirely.[16]

Meanwhile, when courts do undertake contract analysis in technology contexts, the results seem haphazard and without a consistent paradigm. The Seventh Circuit and the Ninth Circuits in particular have adopted sometimes internally inconsistent positions with respect to technology exceptionalist analysis in contract. These courts have also decided cases with arguably similar facts in significantly different ways, causing a circuit split. On the point of contract formation, the Seventh Circuit has aggressively adopted a pro-drafter, non-exceptionalist position. Following the reasoning of *ProCD v. Zeidenberg*, the Seventh Circuit deems digital contexts and physical space contexts to be essentially equivalent for contract formation purposes: it appears to believe that no unique consumer protection concerns exist,[17]

15. Using the facts of *Citrin*, an expectation damages or a disgorgement-based contract remedy could have been crafted to compensate the employer. For example, the court could have required Citrin to pay out/return a portion of salary proportional to work he destroyed or assessed damages according to the market rate of hiring an employee to recreate the work that Citrin destroyed plus the value of any lost revenue because of the destroyed data. Further, the conduct at issue might provide a basis for an injunction under some employment agreements. The use of computer intrusion law to address this type of situation is, thus, superfluous and duplicative.

16. *Id.* at 420–21.

17. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449, 1451 (7th Cir. 1996). In *ProCD v. Zeidenberg*, the Seventh Circuit assessed whether a plaintiff who had compiled databases from phone directories had a basis for remedy in contract for the breach of a defendant who allegedly violated the contractual restrictions on database reuse. *Id.* at 1449. The defendant argued that the terms were not binding, in part, due to the presentation of the agreement, which involved additional terms not readable by a consumer until the box was opened. *Id.* at 1450–51. The Court held that terms as drafted are binding on a consumer even if the consumer has not had opportunity to read all of the terms before she begins interacting with the product. *Id.* at 1449, 1451. The *ProCD* decision, which many would argue is fatally flawed, is predicated on outdated notions of technology, such as the ability to return software. *See, e.g.*, Wendy J. Gordon, *Intellectual Property as Price Discrimination: Implications for Contract*, 73 CHI.-KENT L. REV. 1367, 1378–86 (1998) (criticizing ProCD for, among other things, comparing price discrimination to monopoly power rather than to a regime that permits free copying); Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CALIF. L. REV. 111, 147–51 (1999) (arguing that ProCD did not consider other relevant preemption doctrines, and that the type of contracts that are enforceable under ProCD can create "rights against the world" that might be contrary to public policy); Yochai Benkler, *Free As the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 432 (1999) ("The practical effect of the decision to enforce mass market information licenses is that more uses of information will be prohibited to more people."); Julie E. Cohen, *Copyright and the Perfect Curve*, 53 VAND. L. REV. 1799, 1812 (2000) (criticizing the price discrimination model because it skews incentives for creation in favor of works that produce large private gains at the expense of works intended primarily to benefit the public); *see also* Randal C. Picker, *Easterbrook on Copyright*, 77 U. CHI. L. REV. 1165,

stating "[s]hrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general."[18]

However, on the point of technology breach, reframing the Seventh Circuit's CFAA analysis in *International Airport Center LLC v. Citrin*[19] as a question of contract law reveals that the court adopted a de facto technology exceptionalist analysis. The court asserted that the mere *intention to* breach a contract terminates contractually granted access[20] to technology: "authorization to access the laptop terminated when, having already . . . decided to quit [his employer] in violation of his employment contract, he resolved to destroy files."[21]

The Ninth Circuit, on the other hand, has split with the Seventh Circuit and adopted a more consumer-friendly exceptionalist posture with respect to contract formation questions. In *Douglas v. United States District Court*,[22] the Ninth Circuit found that modifications to an agreement that were posted on a website were not binding on a consumer, since "a party [would not] know when to check the website for possible changes to the contract terms without being notified that the contract has been changed" or the consumer "would have had to check the contract every day for possible changes. Without notice, an examination would be fairly cumbersome" because the consumer

1178 (2010) ("*ProCD* is the opinion that the copyright casebooks love to hate."). Yet *ProCD* continues to be considered good law and has shaped numerous subsequent decisions. *See, e.g.*, Canal+ Image UK Ltd. v. Lutvak, 773 F. Supp. 2d 419 (S.D.N.Y. 2011); Appliance Zone, LLC v. NexTag, Inc., No. 4:09-cv-0089-SEB-WGH, 2009 WL 5200572, 93 U.S.P.Q.2d 1540 (S.D. Ind. Dec. 22, 2009); Health Grades, Inc. v. Robert Wood Johnson University Hosp., Inc., 634 F. Supp. 2d 1226 (D. Colo. June 19, 2009); Illinois Wholesale Cash Register, Inc. v. PCG Trading, LLC, No. 08 C 363, 2008 WL 4924817, 67 UCC Rep.Serv.2d 291 (N.D. Ill. Nov. 13, 2008); Propet USA, Inc. v. Shugart, No. C06-0186-MAT, 2007 WL 1306540 (W.D. Wash. May 3, 2007).

18. *Id.* at 1449. *But see* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 35 (2d Cir. 2002) (holding that internet customers did not manifest assent to an arbitration clause in a click-through agreement when the clause appeared on a scroll-down screen that did not provide "reasonably conspicuous notice of the existence of contract terms" prior to downloading defendant's software).

19. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

20. It is unlikely that the court would have made this argument about a company car, for example.

21. *Citrin*, 440 F.3d at 420 (holding that an employee was liable under the CFAA and the employee's "authorization to access the [company] laptop terminated when . . . [the employee] resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee").

22. Douglas v. U.S. Dist. Court for the Cent. Dist. of Cal., 495 F.3d 1062 (9th Cir. 2007).

"would have had to compare every word of the posted contract with his existing contract in order to detect whether it had changed."[23]

But, on the point of technology breach analysis, the Ninth Circuit has waffled as to whether it should adopt an exceptionalist position on breach. For example, in *LVRC Holdings v. Brekka*[24] the Ninth Circuit arguably conducted a traditional contract law breach analysis in lieu of a CFAA-focused analysis, stating that "[t]here is no dispute that Brekka was given permission to use LVRC's computer and that he accessed documents or information to which he was entitled by virtue of his employment with LVRC."[25] Yet in *United States v. Nosal* the court initially conducted a CFAA-driven analysis in lieu of merely a traditional contract breach analysis. The court exceptionalized the technology circumstances,[26] asserting "[a]lthough we are mindful of the concerns raised by defense counsel regarding the criminalization of violations of an employer's computer use policy, we are persuaded that [there are adequate protections] against criminal prosecution [of] those employees whose only violation of employer policy is the use of a company computer for personal—but innocuous—reasons."[27] Other circuits are similarly leaning toward a technology exceptionalist analysis in contract law.[28] Further, as the next sections will argue, the deference that many courts pay to technology-specific legislative approaches in lieu of asserting the primacy of a traditional contract analysis is unwarranted, undesirable, and derailing the future of contract law.

---

23. *Id.* at 1066 n.1 (emphasis omitted).

24. LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009) (holding that because the defendant was authorized under his employment agreement to access documents on his employer's computer and e-mail them to himself, he did not violate the CFAA).

25. *Brekka*, 581 F.3d at 1135. Brekka "would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA." *Id.*

26. United States v. Nosal (*Nosal I*), 642 F.3d 781, 782–89 (9th Cir. 2011) (holding that despite having authorization to access employer's files, defendant employee "exceeded authorized access" and therefore violated the CFAA by exceeding the employer's use restrictions), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012).

27. *Nosal I*, 642 F.3d at 782. En banc, however, the Court rejected the panel's analysis and found that the employee's breach of the employer's use policy does not provide adequate basis for a charge of computer intrusion under the CFAA, which depends on computer access. United States v. Nosal (*Nosal II*), 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

28. *See* United States v. John, 597 F.3d 263, 271–72 (5th Cir. 2010) (holding that an employee's conviction under the CFAA for exceeding authorized access did not constitute a miscarriage of justice where the employee accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud).

It is not entirely clear why contract issues that involve questions of technology prove disconcerting and confusing to courts.[29] It is clear, however, that the result of this confusion is a slow but steady balkanization of contract law. While courts interpret contracts involving goods relatively consistently—even contracts involving noncompetition agreements have evolved to embody some relatively consistent principles in interpretation—contracts involving technology contexts are causing divergence from rather than convergence around shared principles.

We have now arrived at the untenable point where this judicial confusion and contract law balkanization may begin to paralyze consumer behavior in technology contexts. Using a hypothetical about a consumer and her cat, we can start to frame the extent of the problems that this doctrinal uncertainty causes in everyday contracting. In brief, the average consumers can no longer predictably enter into contracts in technology contexts.

2. Hack3r Cat Says "I can haz contract."

Imagine that you have gifted your grandmother an iPad for her birthday. Your Grandma, a woman with a heart of gold, has two great loves in life: her grandchildren and her cat, Dr. Whiskers. As you assist Grandma in unwrapping her shiny new iPad, you explain to her that if she learns to use the iPad and creates a Facebook account, she will be able to see many pictures of her grandchildren and read about what they are doing on a daily basis. Perhaps even more thrillingly, the Internet has many pictures of cats doing funny things,[30] and there are even cat games available for the iPad which Dr. Whiskers might enjoy playing.[31] Grandma is sold.

You pull up the Apple app store. You quickly click "I Agree" on the Apple end user license agreement without reading it and hand the iPad to Grandma to guide her though the registration process. She tells you that she is registering Dr. Whiskers as the primary user of the device; she suspects he will be using the device as much as she will.[32]

Next, you and Grandma log into the Facebook website together. As you start to help Grandma create a Facebook account, the very long terms and

29. Part II, *infra*, will nevertheless offer a hypothesis regarding the drivers of this dynamic.

30. *See, e.g.*, Nadia Heninger, Telex and Ethan Zuckerman's "Cute Cat Theory" of Internet Censorship, FREEDOM TO TINKER (July 22, 2011), https://freedom-to-tinker.com/blog/nadiah/telex-and-ethan-zuckermans-cute-cat-theory-internet-censorship.

31. *See, e.g.*, jashmenn, *iPad Game for Cats: The World's Greatest Video Game (for cats, not humans)*, YOUTUBE (Dec. 15, 2010), http://www.youtube.com/watch?v=XK2dwTVi-aQ.

32. Showing off your contract law knowledge, you tell Grandma that since Dr. Whiskers is nineteen years old, he is over the age of contractual consent in all jurisdictions.

conditions of use appear. Grandma asks you what all these terms mean. She tells you they are very small in size and that she cannot possibly read such small font.[33] Grandma also notes that there are various other documents linked up from this particular contract on Facebook; she asks you what they are and whether she is going to be bound by all of those terms as well. She is concerned that it may not be safe for her to participate in Facebook. You tell her not to worry; even Chief Justice Roberts just clicks yes on these types of terms of use without reading them.[34] Besides, you tell Grandma, companies like Facebook unilaterally change their privacy policies and terms of use so frequently that it is functionally impossible to keep up, and the terms are nonnegotiable anyway. Grandma clicks "yes I agree" on the Facebook terms of use, and she tells you that Dr. Whiskers should be registered as the primary user for this account too. You help Grandma type in Dr. Whiskers' information in the boxes on the Facebook interface, and she uploads a particularly fetching photo of him.[35]

What you may not realize is that you may have just exposed Grandma to possible criminal prosecution for the felony of computer intrusion. As a consequence of your gift of the iPad and your tutelage in creating a Facebook account for Dr. Whiskers, you may have just led Grandma astray into a life of crime as a "hacker," according to some prosecutors.[36] You also may have just participated in a criminal conspiracy with Grandma to commit computer intrusion.

How could Grandma possibly be deemed a felon for her conduct? The legal argument goes as follows: When Grandma clicked "yes" on the terms of use (that she could not read), she, in theory, agreed to all terms in the agreement, including a provision that stipulated that all users must sign up for accounts in their real names. As Dr. Whiskers is not the (human) user connected to the account, by typing in his information rather than her own, Grandma has already breached a term of the contract. According to some courts, in that magic moment when Grandma breached the agreement, Facebook revoked her authorization to use the website, even in the absence

33. You show Grandma how to make things bigger on the iPad, but she tells you it is too hard for her to make that gesture with her arthritis constantly acting up.

34. Mike Masnick, *Supreme Court Chief Justice Admits He Doesn't Read Online EULAs Or Other 'Fine Print,'* TECHDIRT (Oct. 22, 2010 9:48 AM), http://www.techdirt.com/articles/20101021/02145811519/supreme-court-chief-justice-admits-he-doesn-t-read-online-eulas-or-other-fine-print.shtml.

35. You also help Grandma post the first status update, which says "Dr. Whiskers is purrfect in every way," and you help Grandma friend you and the rest of her grandchildren.

36. *See* Indictment, United States v. Drew (C.D. Cal. Feb. 2008), *available at* http://www.citmedialaw.org/sites/citmedialaw.org/files/2008-05-15-Drew%20Indictment.pdf.

of notice to her of her breach. From that moment she entered Dr. Whiskers' information, she was no longer authorized to use the website.[37] Since she continued to use the website following her breach, her actions may be construed by some courts as "unauthorized access" constituting computer intrusion.

Although this hypothetical may seem far-fetched, a variant of the question presented in this hypothetical—whether a mere breach of contract can provide the basis for a criminal conviction for computer intrusion—has already caused a real-life circuit split in the courts.[38] Further, a case similar to the facts of the hypothetical, one where a consumer violated the terms of use of a social networking website and was prosecuted as a "hacker," resulted in a jury convicting the defendant in question on criminal computer intrusion charges.[39]

Perhaps even more troubling than Grandma's possible "hacker" prosecution is the fact that the same courts that might have been quick to convict Grandma—arguing that technology contexts present unique harms with respect to breach—might instead refuse to acknowledge that Grandma faced any novel consumer protection concerns when she was entering into the contracts. In other words, the same court that, on the one hand, argues

---

37. *Id.*

38. *Compare* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006) (finding civil liability under the CFAA using an exceptionalist approach), United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010) (following *Citrin* to find CFAA liability), WEC Carolina Energy Solutions v. Miller, 687 F.3d 199 (4th Cir. 2012) (same), and United States v. John, 597 F.3d 263 (5th Cir. 2010) (same), *with* LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009) (declining to follow *Citrin*), and *Nosal II*, 676 F.3d 854 (9th Cir. 2012) (en banc) (same).

39. *See* United States v. Drew, 259 F.R.D. 449, 452–53 (C.D. Cal. 2009) (setting aside jury's verdict finding the defendant guilty of a misdemeanor CFAA violation for "accessing a computer involved in interstate or foreign communications without authorization or in excess of authorization to obtain information," based on user's violation of the MySpace Terms of Service). *Drew* highlights the complexity and confusion that pervades questions of contracts in technology contexts. The District Court ultimately decided to grant defendant's motion to set aside the guilty verdict under the "void for vagueness" doctrine because the judge was troubled by the outcome:

> Treating a violation of a website's terms of service, without more, to be sufficient to constitute [a CFAA violation] would result in transforming Section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeant criminals. . . . [And would afford] too much discretion to the police and too little notice to citizens who wish to use the Internet.

Id. at 466–68 (citing City of Chi. v. Morales, 527 U.S. 41, 64 (1999)). However, despite setting aside the verdict, the judge seemed to indicate that a mere breach of contract might indeed support a prosecution for computer intrusion. *See id.* at 452–53.

that contracts involving technology contexts are inherently special in breach may, on the other hand, be completely unwilling to adopt the same technology exceptionalist stance in contract formation questions.

As the discussion in Section II.A.1, *supra*, illustrated, case law on both formation and breach questions lacks a consistent theoretical paradigm to determine whether technology contexts merit a special analysis. The next section will highlight four traditional contract law principles that offer a starting point for determining whether technology exceptionalist analysis is warranted in a particular contract case: freedom to contract, freedom from contract, the primacy of damages,[40] and preserving private ordering.[41] This paradigm of "restrained technology exceptionalism" can assist courts in crafting a minimally disruptive and more predictable approach to contract and technology questions.

B. THE PARADIGM OF "RESTRAINED TECHNOLOGY EXCEPTIONALISM"

As Section I.A, *supra*, explained, courts are increasingly adopting inconsistent—sometimes even internally inconsistent—approaches to analyzing the role of technology in contract law. However, as our society becomes more technology-reliant, progressively greater numbers of contracts will eventually include a technology component. This slippery slope eventually leads us into a world where substantially all contracts will implicate technology in some manner. As such, finding doctrinal coherence and a theoretically logical approach to questions of technology exceptionalism in contract law becomes essential. Without doctrinal consistency, we risk inverting the traditional relationship between contracts and technology.

Current doctrinal tensions in contract law implicating technology exceptionalism have weakened traditional contract analysis at a core level. This Section argues that these tensions are leading contract law dangerously astray, losing touch with foundational principles and crafting the aberrational and undesirable "law of the zebra" described in the Introduction. By identifying strategic contract behaviors in technology contexts, we can then map them onto traditional contract law first principles. In this way, we can

40. Primacy of damages refers to the idea that the primary remedy for a contract breach should be monetary compensation, regardless of which measure of contract damages is used. For a discussion of contract damages as the primary remedy for contract breach, see *Introductory Note*, RESTATEMENT (SECOND) OF CONTRACTS, 16 (1981); CORBIN ON CONTRACTS § 55.3 (Joseph M. Perillo ed., 2005).

41. "Private ordering" refers to the ability of individuals to enter into mutually consensual economic relationships. For a discussion of private ordering, see, e.g., Tehila Sagy, *What's So Private About Private Ordering?*, 45 LAW & SOC'Y REV. 923 (2011).

arrive at an emergent yet minimally disruptive contract approach to technology.

Four foundational principles dictate that courts should adopt a type of "restrained technology exceptionalism" that privileges contract law analysis over exceptionalized approaches to technology. Viewing technology as "special" in contract law analysis is only appropriate when it furthers and buttresses the foundational principles of traditional contract law: freedom to contract, freedom from contract, damages primacy in breach, and private ordering. In other instances, technology exceptionalism in contract law is unjustified and must be avoided. Further, technology exceptionalist legal regimes should be used to supplement, not supplant, traditional contract analysis. Stated another way, the law of the horse may be necessary sometimes; the law of the zebra is never necessary. While new technology continues to meaningfully change our world, it does not necessarily need to dramatically change our contract doctrine; both overcorrecting and undercorrecting for technology in contract disputes will be equally destructive in the long term. Viewing technology as special is appropriate only when it furthers foundational principles of contract law and helps to maintain the doctrinal status quo in light of innovation.

This approach, which determines the appropriateness of technology exceptionalism in contract law by seeking to maintain the status quo of human relations crafted by traditional contract principles—and not by looking at a particular technology itself—might be termed a paradigm of "restrained technology exceptionalism." Particular technologies should not be determinative of contract law; however, tweaks in contract law may be necessary when the changing behaviors of contracting parties and their jockeying for power with respect to each other (which may involve use of a particular technology) threaten traditional contract law principles. Thus, the concern is actually a human and relational one,[42] not a technological one.[43]

Four existing principals of contract law will serve to guide courts well in avoiding overzealous (or underzealous) technology exceptionalism. First, courts should seek to preserve freedom of contract; they should be conscious of new shifts in bargaining power and obstacles to meaningful consent that are byproducts of particular technology. Second, courts must preserve freedom from contract. They must remain vigilant in situations where

42. *See* Stewart Macaulay, *Relational Contracts Floating on a Sea of Custom? Thoughts about the Ideas of Ian MacNeil and Lisa Bernstein*, 94 NW. U. L. REV. 775, 782 (2000) (explaining that a relational approach avoids the oversimplification of contract law).

43. This distinction will be elaborated upon using the context of contract breach and computer intrusion in Part II, *infra*.

technology creates incentives and opportunities for one party to violate duties of good faith in performance and enforcement. This gaming creates novel types of contractual instability and threatens contractual liberty with respect to enforcement, exit, and redress. Further, courts should seek to preserve traditional contract remedies and the primacy of monetary damages as a remedy for contract harms. Finally, as a corollary fourth principle, courts should seek to preserve private ordering, supplementing but never supplanting contract's role in the innovation ecosystem.

1. Principle 1—Freedom to Contract: Equalizing Bargaining Power and Making Consent Meaningful in Formation

As I have demonstrated empirically in other work, contract drafting norms in technology contexts are a moving target.[44] They have shifted over time,[45] and contracts have become progressively more aggressive in the rights they reserve to the drafter.[46] Similarly, as I have argued elsewhere,[47] as technology evolves, new types of possible harms arrive, as well as new interfaces and devices for contract formation.[48] However, it is impractical to wait for contract law to fight out every incarnation of the technology contract battles with each particular product or interface. The law will never be able to anticipate the evolution of technology. Yet, simultaneously, technology evolves less efficiently when its creators cannot reasonably anticipate legal outcomes—a seeming conundrum.

However, hope is not lost: what law can anticipate reasonably successfully is strategic human behavior. In particular, we know from contract law scholarship that contract drafters will tend to act in their own self-interest, and they are likely to leverage new technologies and the contracts that accompany them to maximize their own benefit.[49] Second, we

---

44. *See* Andrea M. Matwyshyn, *Mutually Assured Protection: Toward Development of Relational Internet Data Security and Privacy Contracting Norms*, *in* SECURING PRIVACY IN THE INTERNET AGE 73–75 (Anupam Chander et al. eds., 2008).

45. *Id.* at 75.

46. *Id.*

47. *See* Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529, 538–40 (2007) (explaining that the recent use of hacker coding tactics in digital rights management technology has led to increased vulnerability of computer systems worldwide).

48. *See* Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 125 (2009) (explaining that gaps in technology regulation have necessitated looking to other areas of law for guidance).

49. *See* Melvin A. Eisenberg, *Why There Is No Law of Relational Contracts*, 94 NW. U. L. REV. 805, 808 (2000). Eisenberg states:

> [C]lassical contract law was based on a rational-actor model of psychology, under which actors who make decisions in the face of

know that when possible, drafters employ unnegotiated form contracts, which will be likely to disadvantage the party who lacks bargaining power.[50] Third, we know that aggressive contract enforcement in an adversarial system, if judicially unchecked, is likely to continue to push the limits of the law in favor of the better-resourced litigant in perpetuity.

A foundational principle that has been prominent in contract law relates to fairness in formation: equalizing bargaining power between differently sophisticated parties and ensuring that both parties' consent is meaningful.[51] As I have argued elsewhere, significant concerns exist with current contract law in the context of formation of agreements involving technology.[52] Two types of new strategic formation behaviors now exist, which take advantage of this doctrinal inadequacy. First, the drafter of the agreement tries to game the presentation of the agreement for competitive advantage over the other party.[53] Second, the drafter tries to game the content of the agreement to preserve maximum flexibility and leverage in enforcement, such as limiting the other party's ability to meaningfully consent.[54] In these scenarios, technology exceptionalist approaches to contract formation are warranted.

a) Gaming in Presentation and Content

The use of digital media for contract presentation introduces new opportunities for strategic gaming. In the technology contexts, the drafter gains additional leverage in contract formation. For example, digital contracts frequently incorporate various other documents by reference—if the user is on a mobile device, reviewing these incorporated documents simultaneously

---

> uncertainty rationally maximize their subjective expected utility, with all future benefits and costs discounted to present value. In particular, the rules of classical contract law were implicitly based on the assumptions that actors are fully knowledgeable, know the law, and act rationally to further their economic self-interest.

Id.

50. *See, e.g.*, Mark R. Patterson, *Standardization of Standard-Form Contracts: Competition and Contract Implications*, 52 WM. & MARY L. REV. 327, 331–33 (2010) (analyzing standard form contracts with a focus on the balance of bargaining power between the parties).

51. *See* 8 WILLISTON ON CONTRACTS § 18:9 (4th ed. 2012).

52. *See, e.g.*, Matwyshyn, *Technoconsen(t)sus*, *supra* note 47, at 533, 550–55 (explaining that contract doctrine surrounding digital agreement formation focuses only on procedural unconscionability and ignores substantive unconscionability entirely); Matwyshyn, *supra* note 44, at 73–75 (explaining the progression of terms of use in a draconian direction and explaining formation challenges therein); Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1635–39 (2011) (explaining how website presentation can be used to obscure consumer ability to meaningfully understand end user license agreements).

53. Matwyshyn, *Technoconsen(t)sus*, *supra* note 47, at 551–52.

54. *Id.* at 554–56.

becomes functionally difficult if not impossible.[55] Many users may not even understand the concept of incorporation by reference or realize that they are in essence agreeing not only to the agreement that is visible to them on the screen before them, but also to a series of additional agreements that exist elsewhere on the Internet.

The hypothetical with Grandma and Dr. Whiskers demonstrates some of the common problems that users experience when attempting to read and understand contracts in technology contexts. Fonts used in these contracts tend to be very small on a screen, and the presentation of contracts can appear in different sizes on different screens.[56] Particularly in the context of mobile devices, the ability of an average user to comfortably read these agreements is dubious. Even when the agreement initially appears in a pop-up, links to the agreement may be hidden in obscure locations on the user interface, limiting the user's ability to navigate to and subsequently review terms after initial "consent."[57]

Apart from gaming in the presentation of contracts, technology also allows for gaming with respect to content and meaningful contractual consent. Many contracts involving technology are either entirely unnegotiable, such as terms of use, or functionally unnegotiable, such as a workplace technology permissible use contract or employee handbook. Take-it-or-leave-it transactions have always been a concern of contract law.[58] However, in physical space, consumers are capable of crossing out and modifying provisions with which they do not agree, and these customizations generally control.[59] In digital spaces this ability to cross out and modify form contracts does not exist for the consumer.

---

55. *See, e.g.*, *Terms of Service*, FACEBOOK (Dec. 11, 2012), www.facebook.com/legal/terms (incorporating other legal terms, such as its "Data Use Policy" and "Promotions Guidelines," into its primary "Terms of Use" agreement through hyperlinks, making it difficult to navigate to those terms on mobile devices).

56. *See, e.g.*, *Bug 743799: Strange User Interface Variation*, BUGZILLA (Oct. 27, 2012, 11:02 AM), https://bugzilla.redhat.com/show_bug.cgi?id=743799 (explaining interface bug); Alex Heath, *One Inch Makes All The Difference: Why Apple Thinks The iPad mini's Display Is In A "Whole Other League,"* CULT OF MAC (Oct. 25, 2012), http://www.cultofmac.com/198279/one-inch-makes-all-the-difference-why-apple-thinks-the-ipad-minis-display-is-in-a-whole-other-league/.

57. *See, e.g.*, SQUARE, http://www.square.com/ (rollover required to make legal terms link plainly visible).

58. *See* Yuval Feldman & Doron Teichman, *Are All Contractual Obligations Created Equal*, 100 GEO. L.J. 5, 8, 18, 25, 44 (2011).

59. *See, e.g.*, Gail Hillebrand, *The Uniform Commercial Code Drafting Process: Will Articles 2, 2B, and 9 Be Fair to Consumers?*, 75 WASH. U. L.Q. 69, 78 (1997).

Further, substantively, these technology contracts may be written using esoteric specialized technology or legal terminology unfamiliar to most consumers.[60] These contracts also may be drafted in an intentionally ambiguous manner in order to reserve maximum flexibility for the drafter; because these agreements are frequently unnegotiated and unnegotiable, the terms almost always remain in their original ambiguous form, governing the relationship in a one-sided manner for the benefit of the drafter.[61]

Finally, many form technology agreements allow for the drafter—the website operator or application author—to amend the agreements in his sole discretion. The user may not even be aware that terms have changed. When these dynamics are coupled with the substantial length of the average user agreements—length that has been increasing over time[62]—and their poor readability, concerns about unfair surprise and oppression exist.[63]

When one party capitalizes on known deficiencies of information for strategic benefit, courts in physical space contexts often view this advantage negatively, but these norms have not yet transferred into contract caselaw involving technology contexts. For example, where one party is known to lack the capacity required to understand the agreement, courts have historically set aside these agreements in consumer contexts.[64] When the drafter leverages, capitalizes on, or exacerbates the user's deficiencies of knowledge—such as technology knowledge—courts should be equally

60. *See, e.g.*, Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts*," 78 U. CHI. L. REV. 165, 166 (2011).

61. The contract interpretation principle of *contra proferentem* is driven by the premise that an ambiguity should be construed against the drafter to avoid the possibility of gaming by drafters. *See* 11 WILLISTON ON CONTRACTS § 32:12 (4th ed. 2012). For a discussion of strategic vagueness and ambiguity, see B. Douglas Bernheim & Michael D. Whinston, *Incomplete Contracts and Strategic Ambiguity*, 88 AM. ECON. REV. 902 (1998).

62. *See* Marotta-Wurgler, *supra* note 60, at 168, 177–78, 181. *Compare, e.g.*, Legal Information & Notices, ITUNES (May 13, 2004), *available at* http://web.archive.org/web/20040627044803/http://www.apple.com/legal/default.html, *with* Legal Information & Notices, ITUNES (Nov. 20, 2009), http://www.apple.com/legal/terms/site.html (last visited Feb. 26, 2013) (demonstrating changes in the "Accounts, Passwords and Security" section which emphasizes the burden on the consumer in addition to changes in the "Governing Law; Dispute Resolution" section. Also, the following sections were deleted: "Trademark Information"; "Copyright Information"; "Rights and Permissions"; "Piracy Prevention"; "Software Piracy"; "Software Asset Management"; "Internet Piracy"; "Apple's Unsolicited Idea Submission Policy"; "Terms of Idea Submission"; "Product Feedback"; "Software and Documentation Information"; and "Legal Contracts.").

63. This language intentionally mirrors the language of unconscionability, a traditional concern of contract law. *See* 8 WILLISTON ON CONTRACTS § 18:9 (4th ed. 2012).

64. *See* Wendy Chung Rossiter, *No Protection for the Elderly: The Inadequacy of the Capacity Doctrine in Avoiding Unfair Contracts Involving Seniors*, 78 OR. L. REV. 807, 807–09 (1999).

vigilant. Yet, it is quixotic to expect that drafters will act in a manner contrary to their self-interest when the digital space grants them an inherent advantage. Indeed, one may argue that such an expectation would perhaps even be inconsistent with current contract law, which lacks a duty of good faith in negotiation in the United States.[65] This deficit of a duty to negotiate in good faith makes it even more necessary to compensate for new procedural disadvantages one bargaining party faces due to technology.

b) Technology Exceptionalism in Formation Is Appropriate

The formation obstacles described above reflect drafters' use of the digital medium to gain a strategic advantage. Although some of the concerns noted above already existed in the context of standard form contracts, for example, technology alters and exacerbates them to a meaningful degree, almost always to the detriment of the weaker party. As such, a technology exceptionalist approach to formation benefits the weaker party: it rebalances the interests of the parties toward a more level playing field.

I have argued elsewhere that the concerns with respect to unfair surprise and oppression in technology contracting are so severe that they warrant a new construction of meaningful consent hinged on actual understandings of real users that evolve across time,[66] and that state contract law should expressly incorporate a series of implied promises to compensate for the lack of a negotiability of technology contracts.[67] In the sections that follow, this Article argues the opposite with respect to contract breach. The strategic contract gaming behaviors in breach contexts reflect a different dynamic than the gaming behaviors in formation contexts. Whereas a technology exceptionalist analysis in formation is appropriate to protect the weaker party and prevent unfair surprise and oppression,[68] in breach it is not. Applying an exceptionalist analysis to breach exacerbates rather than remedies existing power imbalances between the parties; exceptionalism in breach harms the weaker party and additionally skews the playing field in favor of the more powerful party—usually the drafter. Staying true to traditional contract principles in technology breach contexts instead requires treating technology breach and other contractual breach as equivalent.

65. *See, e.g.*, John Klein & Carla Bachechi, *Precontractual Liability and the Duty of Good Faith Negotiation in International Transactions*, 17 HOUS. J. INT'L L. 1, 16 (1994) (discussing the absence of a duty of good faith in negotiations in the United States).

66. Matwyshyn, *Technoconsen(t)sus*, *supra* note 47, at 532, 560–62.

67. Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 86 S. CAL. L. REV. (forthcoming 2013).

68. Matwyshyn, *Technoconsen(t)sus*, *supra* note 47, at 533–34, 559.

2. *Principle 2—Freedom from Contract in Breach: Reasonable Enforcement in Line with Contractual Liberty and Rights of Exit*

The corollary principle in contract law to the freedom *to* contract has always been freedom *from* contract. In other words, while the law should support parties' liberty to enter into deals—even deals with unwise business terms[69]—the law should also support parties' liberty to exit contractual relationships in a reasonable manner.

a) Duties of Good Faith in Performance and Enforcement

A duty of good faith in performance and enforcement exists under U.S. law.[70] However, the ability to perform this duty assumes that a party is capable of understanding her contractual obligations. Currently in many contracting situations that involve technology, neither side is clear on the extent of their obligations to the other. In other words, in light of the formation challenges presented above, breach becomes significantly more likely: parties to a contract who do not understand their obligations may be more likely to fail to perform or to perform obligations incorrectly. Similarly, parties who do not understand the obligations of the other side of the contract are less likely to correctly understand when breach by the other side has occurred. Because of the unnegotiated nature of many technology contracts, drafters may insert intentionally vague language into the agreement

69. So long as some form of consideration exists, courts do not evaluate the adequacy of consideration when ruling on contract enforceability. *See, e.g.*, In re Xonics Photochemical, Inc., 841 F.2d 198, 201–02 (7th Cir. 1988) (holding that a now-bankrupt company's guarantee of an affiliate's $15–20 million loan when its own net assets totaled $1.7 million was enforceable because the company voluntarily assented to the loan guarantee and derived some indirect benefit from the agreement, even if minimal); Hoffa v. Fitzsimmons, 673 F.2d 1345, 1359–60 (D.C. Cir. 1982) (holding that a union pension agreement was not unenforceable just because the intended consideration had already been conveyed prior to execution of the contract, since the agreement conferred other ancillary legal and practical benefits upon the beneficiary); Cleveland-Cliffs Iron Co. v. Chi. & N. W. Transp. Co., 581 F. Supp. 1144, 1150 (W.D. Mich. 1984) (noting that unless the consideration is "so grossly inadequate as to shock the conscience, the general rule is that courts will not inquire into the adequacy of the consideration of a contract") (internal citation and quotation omitted); In re Estate of Duncan v. Kinsolving, 70 P.3d 1260, 1265 (N.M. 2003) ("Absent a showing of fraud, inadequacy of consideration is not sufficient to void a contract.") (internal quotation omitted); Horace Mann Ins. Co. v. Gov't Emps. Ins. Co., 344 S.E.2d 906, 908 (Va. 1986) ("[P]arties to a contract are at liberty to determine their own valuations, and courts generally will not inquire into the adequacy of consideration."); Buckingham v. Wray, 366 N.W.2d 753, 756 (Neb. 1985); Osborne v. Locke Steel Chain Co., 218 A.2d 526, 530 (Conn. 1966) ("The doctrine of consideration does not require or imply an equal exchange between the contracting parties. . . . The courts do not unmake bargains unwisely made.").

70. *See* Richard E. Speidel, *The "Duty" of Good Faith in Contract Performance and Enforcement*, 46 J. LEGAL EDUC. 537, 539 (1996).

with a goal of preserving more flexibility in enforcement, as explained above. Meanwhile, although ambiguities have traditionally been construed against the drafter in physical space contexts,[71] this norm does not appear to have transferred itself into digital spaces as yet.

These types of contractual comprehension deficits harm the market stability and commercial trust that duties of good faith intended to foster.[72] As the hypothetical with Grandma and Dr. Whiskers highlights, an average consumer simply may not understand how to conform performance to her duties of good faith. Yet a mere breach of contract in technology contexts now brings a risk of criminal prosecution and uncertain civil consequences—a misguided technology exceptionalism which will be discussed at length in Part III, *infra*.

b) Ability to Exit and "Digital Peonage" Concerns

It has long been a hallmark of contract law that parties can exit their contractual relationships, even if that exit is accompanied by a breach and damages. Further, courts are loathe to require even specific performance of contractual obligations and do so extremely rarely in the context of service agreements.[73] To do otherwise would potentially be a form of forced labor under penalty of law or "peonage."[74] In technology contexts, we might label this concern as a concern over "digital peonage."[75]

---

71. 11 WILLISTON ON CONTRACTS § 32:12 (4th ed. 2012).

72. For a discussion of the role of contractual misunderstandings and relational trust in commercial exchange, see, e.g., Ian R. Macneil, *Relational Contract Theory: Challenges and Queries*, 94 NW. U. L. REV. 877 (2000).

73. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 359(1) (2012) (noting that specific performance is appropriate only when money damages would be inadequate "to protect the expectation interest of the injured party"); Nathan B. Oman, *Specific Performance and the Thirteenth Amendment*, 93 MINN. L. REV. 2020, 2022–23 (2009) (recalling how courts and scholars frequently deny or argue against specific performance as a remedy for breach of service agreements on the grounds that doing so would violate the Thirteenth Amendment, which prohibits involuntary servitude).

74. Peonage, a system that allowed "the holding of any person to service or labor," was abolished by the Anti-Peonage Act of 1867:

> [A]ll acts, laws, resolutions, orders, regulations, or usages of any Territory or State, which have heretofore established, maintained, or enforced, or by virtue of which any attempt shall hereafter be made to establish, maintain, or enforce, directly or indirectly, the voluntary or involuntary service or labor of any persons as peons, in liquidation of any debt or obligation, or otherwise, are declared null and void.

42 U.S.C. § 1994 (2011).

75. As the Idaho Supreme Court explained in the context of physical space:

The Supreme Court has reminded us that policy concerns are implicated whenever a contract limits the right to exit a contractual relationship.[76] In particular, in the Peonage Cases, the U.S. Supreme Court invalidated laws that criminalized breach of employment contracts.[77] As the Peonage Cases attest, threatened criminal prosecution for breach of contract, in particular, chills exit: employees would be worried to leave their employment for fear of losing their liberty in the process. Under the English master and servant acts, a laborer could be criminally punished for breach of contract, but criminal punishment of this kind did not exist in the United States, said the Court.[78]

These concerns with respect to freedom to exit contractual relationships also pervade current law surrounding noncompetition and nonsolicitation contracts, for example.[79] Courts and legislatures have placed express restrictions on the ability of employers to limit employees' exit and future work contracts.[80] The reason for this robust law around noncompetition and nonsolicitation contracts involves, first, an acknowledgement of the power imbalance inherent in an employer and employee relationship, and, second,

---

> Life in the competitive commercial world has at least equal capacity to bestow ruin as benefit, and it is presumed that those who enter this world do so willingly, accepting the risk of encountering the former as part of the cost of achieving the latter. Absent clear evidence to the contrary we will not presume that the parties to a contract such as the one before us meant to insure each other's emotional tranquility.

Hatfield v. Max Rouse & Sons Nw., 606 P.2d 944, 952 (Idaho 1980). These same dynamics are at issue in the context of digital peonage inquiries—employers seek to obtain emotional tranquility by sanctioning employees unexpectedly heavily for exit.

76. *See* Pollock v. Williams, 322 U.S. 4, 18 (1944). In *Pollock*, the U.S. Supreme Court stated:

> When the master can compel and the laborer cannot escape the obligation to go on [working], there is no power below to redress and no incentive above to relieve a harsh overlordship or unwholesome conditions of work. . . . Whatever of social value there may be, and of course it is great, in enforcing contracts and collection of debts, Congress has put it beyond debate that no indebtedness warrants a suspension of the right to be free from compulsory service.

Id. at 18.

77. *Id.* at 25.

78. *Id.* at 18.

79. *See* Ken Matheny & Marion Crain, *Disloyal Workers and the "Un-American" Labor Law*, 82 N.C. L. REV. 1705, 1746 (2004) ("[M]any courts remain troubled by the fact that noncompetes contravene a basic precept of capitalism—free competition in the market.").

80. *See* CAL. BUS. & PROF. CODE § 16600 (West 1987 & Supp. 2003) (rendering noncompetition agreements void).

the undesirability as a matter of social policy in allowing private parties to restrict mobility of talent.[81]

However, precisely these types of peonage concerns arise in case law involving technology breach: "digital peonage." When technology questions emerge in breach analysis, a second set of concerns arise: technology exceptionalism in breach opens the door to unpredictable new forms of draconian punishment for exit—even criminal penalties—that violate traditional contract principles. The ambiguities in technology contracting contexts, particularly the threat of possible criminal prosecution described in Part III, *infra*, may cause parties to view themselves as unable to exit a contractual relationship.

As such, this situation is distinctly different from the dynamics of the desirable technology exceptionalism in questions of formation. Exceptionalism in breach results in granting additional rights to the drafter, rights that may not even be expressly articulated in the contract and perhaps not reasonably foreseeable to the disempowered party.

3. Principle 3—Damages: Preserving Primacy of Traditional Contract Remedies

As the previous Section explained, exceptionalizing technology breach skews the dynamics of contract performance and enforcement. Logically, these disruptions also have ripple effects in the context of damages: technology exceptionalism in breach also disrupts the traditional contract principle of monetary damages as the primary recourse for contract harms. Arguing in favor of technology exceptionalism in breach, courts have been willing to provide plaintiffs a method to leverage already existing regimes of punishment from outside contract law, in lieu of preserving the primacy of damages.

a) Damages Primacy

The primary goal of contract damages, generally speaking, is compensating harmed parties for actual economic losses, not to punish the breacher for a "bad" act of breach.[82] For example, courts generally do not

81. Christina L. Wu, Comment, *Noncompete Agreements in California: Should California Courts Uphold Choice of Law Provisions Specifying Another State's Law?*, 51 UCLA L. REV. 593, 608–10 (2003).

82. RESTATEMENT (SECOND) OF CONTRACTS, § 355 (1981) ("Punitive damages are not recoverable for a breach of contract unless the conduct constituting the breach is also a tort for which punitive damages are recoverable.").

enforce punitive damages clauses[83] and, as a general rule, we do not criminalize breaches of contract.[84] As Farnsworth has stated, a "stipulated sum [that] is significantly larger than the amount required to compensate the injured party for its loss . . . would allow the parties to depart from the fundamental principle that the law's goal on breach of contract is not to deter breach by compelling the promisor to perform, but rather to redress breach by compensating the promissee [sic]" and therefore is prohibited "when a court characterizes such a provision as a penalty."[85] Attaching a draconian contract penalty such as specific performance, gratuitously high damages, or incarceration to a technology exceptionalist analysis runs opposite to this guiding contract principle.

An exceptionalized technology breach regime becomes disconnected from the goal of providing the benefit of the bargain to the wronged party; it instead focuses on whether breach implicates technology and on punishing the breacher. Even adopting a more morality-driven stance, such as that of the *Third Restatement of Restitution*, a traditional damages approach focuses on actual financial harms, not on the deterrence of future breach, retribution, incapacitation, or rehabilitation of breachers.[86] Though criminal law may adopt these goals, contract law generally does not. Even in the context of the most aggressive traditional damages calculation, expectation damages,[87] Professors Fuller and Perdue argue in favor of protecting reliance and facilitating business contracts in a system where the economy and the legal institutions are intertwined.[88] Thus, an exceptionalized breach analysis that allows remedies other than damages or, in the most severe situations, an

83. *See* Charles R. Calleros, *Punitive Damages, Liquidated Damages, and Clauses Penale in Contract Actions: A Comparative Analysis of the American Common Law and the French Civil Code*, 32 BROOK. J. INT'L L. 67, 69 (2006).

84. *See supra* notes 76–82 and accompanying text. Considering this general rule against criminalization of breaches of contract, the approach currently used by a number of courts in interpreting the CFAA, which purports to do precisely that, is all the more problematic. This problem will be discussed in detail in Part III, *infra*.

85. E. ALLAN FARNSWORTH, FARNSWORTH ON CONTRACTS § 12.18 (3d ed. 2004).

86. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 et seq. (2011).

87. For a discussion of the definition of expectation damages and, in particular, their relationship to contractual misunderstandings, see Daniel P. O'Gorman, *Expectations Damages, the Objective Theory of Contracts, and the "Hairy Hand" Case: A Proposed Modification to the Effect of Two Classical Contract Law Axioms in Cases Involving Contractual Misunderstandings*, 99 KY. L.J. 327 (2011).

88. L.L. Fuller & William R. Perdue, Jr., *The Reliance Interest in Contract Damages: 2*, 46 YALE L. J. 373 (1937).

injunction, unnecessarily violates traditional contract principles.[89] It exceeds even the most aggressive traditional contract remedies without a compelling justification.

b) The Unique Concerns of Information Harms

But, playing devil's advocate, perhaps technology-connected harms are so severe that current calculations of damages are incapable of encompassing the extent of information harms. Perhaps a more aggressive set of remedies is needed for information harms.[90]

Although this argument may hold superficial appeal, scholars have posited that even extraordinary situations of information breach can be addressed successfully using a damages regime modeled from traditional contract principles of damages. As Melvin Eisenberg has convincingly argued, disgorgement damages in particular offer a potent remedy for information-based contract harms.[91] Disgorgement is also appropriate where losses would be very difficult to establish with sufficient certainty for an expectation damages calculation. Eisenberg asserts that a disgorgement calculation has worked well in a line of cases concerning damages in breaches of noncompete agreements or agreements to give the plaintiff exclusive territorial rights.[92] Courts have successfully awarded damages based on the defendant's profits, explicitly protected the disgorgement interest, or used a disgorgement measure as a surrogate for the expectation measure.[93] Theoretically, this calculation protects the integrity of contract law, argues Eisenberg: "unless disgorgement is awarded in such cases, a promisor could subvert the right to specific performance simply by completing an irreversible breach before the promisee can get to court."[94] In other words, disgorgement offers a damages construction that approximates specific

89. A second contract theory debate that becomes permanently altered in an exceptionalized technology contract breach environment relates to damages and the duty by the nonbreaching party to mitigate losses. For a discussion of the duty to mitigate damages in contract, see, e.g., 25 C.J.S. *Damages* § 46 (2013).

90. For example, although specific performance is rarely granted, this remedy does exist for some types of extreme contract harm situations. *See* FARNSWORTH, CONTRACTS § 12.4 (3d ed. 1999) ("[A]lthough the injured party can always claim damages for breach of contract, that party's right to specific relief as an alternative is much more limited.").

91. This calculation of damages is appropriate in cases in which the nonbreaching party would have been awarded specific performance if the nonbreaching party had been able to bring suit before the breacher's wrongful action. *See* Melvin A. Eisenberg, *The Disgorgement Interest in Contract Law*, 105 MICH. L. REV. 559, 584 (2006).

92. *Id.* at 588.

93. *Id.* at 578–81.

94. *Id.* at 584.

performance better than an expectation measure in the case where, for example, information is stolen or a system is used to harm others.

For example, in *Snepp v. United States*, a former CIA employee breached an employment agreement requiring that he "not . . . publish . . . any information or material relating to the Agency, its activities or intelligence activities generally, either during or after the term of [his] employment . . . without specific prior approval by the Agency."[95] Snepp had left the CIA and published a book about CIA activities in South Vietnam that happened during the term of his employment, failing to submit the material for approval.[96] The Government sued Snepp for disgorgement of his profits from the book, and the Supreme Court agreed with the argument that disgorgement was warranted.[97] The Court applied a disgorgement-based calculation of damages, stating that despite the Government being harmed by Snepp's book, proving the extent of that harm would be difficult, and the Government could not pursue other remedies "without losing the benefit of the bargain it seeks to enforce."[98] Ergo, argues Eisenberg, a disgorgement measure of damages made the government whole for this commercial harm.[99] The same rationale should apply to any rogue insider situation where harm, including digitally-caused harm, occurs.

4. Principle 4—Supplementing But Not Supplanting Contract

To date, contract law has provided the dominant structures for organization of technology contexts; the reason for this supremacy rests in contract law's flexibility. It offers nimble structures that allow for customization of obligations and self-help, as well as default shared norms of permissible conduct.[100] In this way, contract simultaneously fosters innovation and entrepreneurship without letting entrepreneurs cause unfettered damage to others. However, contract law is by no means the only law that impacts technology use and innovation. As the reach of existing technology exceptionalist statutes expand, and Congress drafts a growing number of statutes, technology exceptionalism threatens to unbalance the relationship between contract law and technology law. Although technology exceptionalist statutes address real harms in Congress's estimation, such

95. Snepp v. United States, 444 U.S. 507, 508 (1980).
96. *Id.* at 507.
97. *Id.* at 508, 516.
98. *Id.* at 514.
99. Eisenberg, *supra* note 91, at 589.
100. *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1019–25 (1994) (advocating self-help, custom, and contract to regulate cyberspace).

statutes should buttress rather than override the fundamental principles of contract law.

Contract law is an evolutionary framework. For example, when emergent circumstances warrant shifts in consumer protection posture, tweaks to contract law frequently offer a more successful and less disruptive solution than a new technology exceptionalist statutory regime.[101] As such, new technology exceptionalist approaches should begin where the structure afforded by contract law ends, or they should work in tandem with contract law without usurping its role. Future innovation and user adoption will be better served through the preservation of private ordering and contract remedies than through aggressive technology-exceptionalist legislative approaches.

As Part III, *infra*, will demonstrate through the example of computer intrusion and contract breach, when shifting contract drafting and enforcement norms are coupled with a failure to maintain contractual supremacy over technology-exceptionalist legal regimes, the negative consequences become amplified. In the context of the circuit split on contract breach/CFAA analysis, the failure to maintain contractual supremacy "weaponizes" contract breach. By weaponizing breach, courts inappropriately repurpose contract law from its traditional role as a means for private ordering. Contract law is instead corrupted into a mere springboard to leverage potentially draconian remedies available under other legal regimes—particularly intellectual property law and technology law. The next Part elaborates on this undesirable dynamic of weaponized breach and how CFAA analysis threatens to usurp the traditional role of contract remedies for technology-related contract breach.

III. HORSES AND CLAPPING COCONUTS: THE PROBLEMATIC CASE OF WEAPONIZED BREACH AND COMPUTER INTRUSION UNDER THE CFAA

> "King Arthur: We have ridden the length and breadth of the land in search of knights who will join me in my court at Camelot. I must speak with your lord and master.
>
> 1st soldier: What? Ridden on a horse?
>
> King Arthur: Yes!
>
> 1st soldier: You're using coconuts!

101. *See* Matwyshyn, *Technoconsen(t)sus*, *supra* note 47, at 557–59 (discussing the benefits of tweaking contract law to address consumer consent to security-invasive technologies).

> King Arthur: What?
>
> 1st soldier: You've got two empty halves of coconut and you're bangin' 'em together."

– *Monty Python and the Holy Grail*[102]

In an iconic scene from the movie *Monty Python and The Holy Grail*, a soldier with a keen interest in birds hears the sound of hoofbeats, only to realize that instead of a horse arriving, it is merely a person clapping coconuts together.[103] Breach in technology contexts is the contract law equivalent of a person clapping coconuts—from the noise, a hearer may believe the sound to arise from a horse or a zebra, but the source is actually neither. The previous section introduced the argument that technology exceptionalism was overwhelming traditional legal paradigms in contract, crafting an unnecessarily exotic legal regime that derails traditional contract law—a "law of the zebra." A "law of the zebra" approach for contract breach is unwarranted, and even a "law of the horse" exceptionalized approach is unnecessary.

This Part elaborates on the importance of adopting a paradigm of restrained technology exceptionalism for contract breach analysis through an example of "the law of the zebra": the circuit split on the relationship of breach and computer intrusion under the Computer Fraud and Abuse Act ("CFAA").[104] As the previous sections explained, contract breaches have traditionally—very intentionally—not been viewed as crimes. Yet this particular legal query between the relationship of contract breach and

---

102. *Memorable quotes for Monty Python and the Holy Grail*, IMDB, http://www.imdb.com/title/tt0071853/quotes (last visited Jan. 16, 2013).

103. MONTY PYTHON AND THE HOLY GRAIL (Python (Monty) Pictures Ltd. 1974).

104. The CFAA is the primary computer intrusion or "hacking" statute in the United States. It hinges on the idea of whether "authorized access" has occurred or whether the access in question is unauthorized or exceeds the scope of authorization. It prohibits obtaining:

> (A) information contained in a financial record of a financial institution, or of a card issuer . . . or contained in a file of a consumer reporting agency on a consumer . . . ;
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer . . . .

18 U.S.C. § 1030(a)(2) (2011). The CFAA defines the term "financial institution" to include a range of financial institutions, such as banks, credit unions, and broker-dealers. *Id.* at § 1030(e)(4). The CFAA is also violated when a person uses or sells passwords to access machines, uses a computer with an intent to extort money or anything of value, or transmits communications threatening damage to a protected computer though interstate or foreign commerce. *Id.* § 1030(a)(6), (a)(7).

computer intrusion has split the Seventh and Ninth Circuits in the context of CFAA analysis.[105] Although contract breaches involving technology may on their surface appear to warrant a technology exceptionalist analysis, the technology aspects of the breach are ultimately irrelevant—the mere use of a computer does not alter the capacity of contract law to redress the harm.[106]

This Part introduces four very different types of "contract hackers" impacted by this weaponized breach dynamic, and argues that weaponzing breach is highly undesirable as a matter of contract doctrine, theory, private ordering and innovation, and entrepreneurship policy. Applying paradigms from developmental and social psychology, this Part then postulates that courts' misguided tendency to weaponize breach in technology-related cases is likely rooted in essentialism and confirmation bias rather than traditional contract law analysis.

A. WEAPONIZING BREACH: THE CFAA AND A TALE OF FOUR "CONTRACT HACKERS"

> "[E]ven without [a] voluntary release there are perhaps no contracts or engagements . . . of which one can venture to say that there ought to be no liberty whatever of retraction."
>
> – John Stuart Mill[107]

This Section asks a superficially simple breach question: should a breach of contract relating to a computer or network automatically provide the basis for a criminal charge of computer intrusion under the CFAA?[108] The CFAA has a checkered past, with several amendments that significantly expanded

105. *See infra* notes 134–43.

106. Similarly, detection of a breach may be even more likely because of the extent of digital monitoring used in an average workplace.

107. JOHN STUART MILL, ON LIBERTY 199 (Boston: Ticknor & Fields 1863).

108. Proponents of a technology exceptionalist analysis would argue, among other things, that information loss has become a more pressing problem than in the past, that stealing information is easier and more prevalent because of technology interconnection, and that lost information is harder to detect. While each of these points may be descriptively correct, none of them explains why current contract law is inadequate to address technology-related breach cases. Similarly, none of these arguments provide a justification for disrupting traditional contract law around breach as the most effective means of addressing these challenges. Further, advocates of a "law of the zebra" fail to demonstrate the presence of new categories of harm outside of those that contract law already contemplates. Contract law around breach and damages can already effectively address the harms arising from breaches involving technology. While we may need a legislative correction to buttress—but not override—traditional concerns in contract formation in technology contexts, traditional contract law around breach should not be mutated into a construct violative of its own foundational principles. Criminalizing breaches of contract would do precisely that.

the scope of the Act.[109] Intended primarily as a criminal statute to address third party "hackers,"[110] it was passed originally in 1984, perhaps partially in response to a cyberwar-themed movie.[111] The statute has been amended on multiple occasions since its passage and has been expanded to include civil matters.[112] Despite numerous amendments to the statutory framework created by the CFAA, it continues to be beset with problems. Indeed, two circuit splits currently exist with respect to its interpretation.[113] The first split is outside the scope of this Article.[114] The second split, which is partially the subject of this article, relates essentially to the meaning of "authorized access" under the statute and the relationship of the statute to contract law.

---

109. For a discussion of the history behind unauthorized access statutes, including the CFAA, see Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–71 (2010).

110. *See id.* (providing a history of the CFAA).

111. The movie *WarGames* was released in 1983, before the passage of the CFAA in 1986. WARGAMES (United Artists 1983) (depicting a teenage hacker accidentally compromising a weapons system at the Pentagon, believing it to be a computer game); s*ee also In re* America Online, 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001) (discussing the legislative history, noting that the CFAA has expanded beyond federal and financial systems). The *America Online* court quoted the Senate Report:

> As computers continue to proliferate in business and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary framework to fight computer crime.

Id. (quoting S. Report, 104-357, at 5 (1996)).

112. An interesting parallel in the expansion to the CFAA for civil matters can be found in another troubled statute, RICO. Like the CFAA, RICO is simultaneously criminal and civil and has also caused circuit splits. Some of the dynamics that this section highlights in the context of contract and CFAA enforcement have predecessors in the RICO caselaw, which may hold lessons for the future of the CFAA. *See, e.g.*, Randy D. Gordon, *Clarity and Confusion: RICO's Recent Trips to the United States Supreme Court*, 85 TUL. L. REV. 677 (2011) (discussing Racketeering Influenced and Corrupt Organizations Act ("RICO") and the challenges in application raised by its dual civil and criminal nature).

113. *Id.*

114. The first split relates to whether a plaintiff must plead both "damage" and "loss" for a recovery under the CFAA. The First Circuit has held that the CFAA provides for recovery of economic "loss" even in the absence of any physical "damage" to the computer system or its information. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 ("As we move into increasingly electronic world, the instances of physical damage will likely be fewer while the value to the victim or what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever-larger."). However, in *Garelli Wong & Assocs. v. Nichols*, a district court in the Seventh Circuit read the statute to hold that a plaintiff under the CFAA must plead both "damage" and "loss." 551 F. Supp. 2d 704, 708 (N.D. Ill. 2008). This split is outside the scope of this Article.

The CFAA creates civil and criminal penalties for unauthorized access or access that exceeds authorization to computer data.[115] In general, two categories of alleged intruders in systems are possible—first, the group of alleged intruders with no preexisting contractual relationship to the network or computer owner,[116] and second, the group of alleged intruders where a preexisting relationship exists.[117] In the first situation, where the alleged intruder has no contractual relationship to the owner of the system, CFAA analysis is somewhat straightforward: no authorization exists, and determining liability becomes primarily a fact-driven question as to whether the alleged intruder has indeed violated the boundaries of the network or accessed the machine in question. These unaffiliated intruders include the malicious third parties who attack networks, and they are those "hackers" the CFAA originally sought to address.[118]

The second group of alleged computer intruders might be termed "contract hackers"—those alleged intruders who have a preexisting contractual relationship to the system owner. A "contract hacker" analysis under the CFAA inevitably starts with some variant of a traditional contract law inquiry—for example, an employment or nondisclosure or noncompetition agreement, an end user license agreement, or terms of use.[119] The Parts that follow argue that if courts engage in a technology exceptionalist analysis of contract breach in CFAA cases, they inappropriately "weaponize" breach and cause permanent damage to the future contract law as a whole.

Contract breach weaponized with penalties under the CFAA overreaches not only by applying criminal liability for the defendants, but also by

115. 18 U.S.C. § 1030 (2011).

116. David M. Hafele, *Three Different Shades of Ethical Hacking*, SANS INSTITUTE (Feb. 23, 2004), http://www.sans.org/reading_room/whitepapers/hackers/shades-ethical-hacking-black-white-gray_1390.

117. Often this preexisting relationship takes the form of an employment relationship accompanied by a confidentiality agreement or permitted computer use policy. *See* Colette Thomason, Case Summary, United States v. Nosal*: Separating Violations of Employers' Computer-Use Policies from Criminal Computer Hacking Invasions*, 43 GOLDEN GATE U. L. REV. 163, 164 (2013).

118. These "hackers" include the malicious third parties who attack networks and whom are referred to colloquially in the information security community as "black hats." Though the dynamics of this CFAA case law with respect to unaffiliated third-party "hackers" should also be revisited and clarified, these inquiries are outside the scope of this Article. The "hacker" collective Anonymous in particular has triggered a need to craft lines between computer intrusion and permissible methods of digital protest. *See, e.g.*, Sean Captain, *The Real Role of Anonymous at Occupy Wall Street*, FAST COMPANY, (Oct. 17, 2011), http://www.fastcompany.com/1788397/the-real-role-of-anonymous-at-occupy-wall-street.

119. *See Nosal II*, 676 F.3d 854, 860–62 (9th Cir. 2012) (en banc).

imposing duplicative financial remedies in civil claims, and thereby threatening to derail contract law. Cases involving four different types of "contract hackers" illustrate the dangers of contract breach weaponized with the CFAA, including (1) consumer users of technology, (2) "disloyal" employees or business partners, (3) entrepreneurs, and (4) security researchers. These cases demonstrate a pressing need to resolve the tension between contract breach and computer intrusion law.

1. Consumer Users of Technology as "Contract Hackers": Confusing Minor Breach with Black Hat Hacking

We again return to the Grandma and Dr. Whiskers hypothetical. Does a consumer user who breaches an end user license agreement or terms of use agreement on a website lose authorization and, therefore, create the basis for a charge of criminal intrusion under the CFAA? At least one jury has problematically concluded that the answer is yes.

In *United States v. Drew*, an adult created a fictitious profile on the social networking website Myspace and used this account to communicate with a teenager, who committed suicide after one such communication.[120] In doing so, the jury found, the defendant completed a CAPTCHA and consented to (and then violated) Myspace's Terms of Service.[121] The jury convicted the defendant of a misdemeanor under the CFAA on the basis of her contract breach.[122]

The court, however, ultimately set aside the conviction, asserting that "[t]he pivotal issue herein is whether basing a CFAA misdemeanor violation as per 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine."[123] The court concluded that it did run afoul "primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies."[124] However, it is troubling that the same judge who set aside the verdict in the *Drew* case, nevertheless, appeared to agree with the jury's CFAA-weaponized breach analysis. The court in *Drew* explained that "an intentional breach of the [MySpace Terms of Service] can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statute," apparently suggesting that a mere breach of contract can indeed provide the

120. United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).
121. *Id.* at 451.
122. *Id.*
123. *Id.* at 464.
124. *Id.*

basis for a criminal prosecution under the CFAA.[125] Further, a judge's use of JNOV as a procedural mechanism is a rare event.[126] Other courts may not be willing to set aside a jury verdict, and since we know that at least one jury has already convicted based on an exceptionalized technology contract breach argument,[127] the issue is likely to surface again in another court.

As consumers increasingly rely on technology in their daily lives, this type of breach will occur with regularity. As Part I, *supra*, explained, unnegotiable, unilaterally amendable technology contracts with vague terms empower the drafter to assert breach by the other party with ease. We may all soon become "contract hackers" at the mercy of the drafters of the contracts that accompany the technologies we use in daily life. Although the Senate Judiciary Committee appears somewhat concerned about this eventuality,[128] and a bill was introduced in the Senate to exempt this user-hacker scenario from the CFAA,[129] Congress has not so amended the CFAA as of this writing.

2. "Disloyal" Employees or Business Partners as "Contract Hackers": Confusing Intellectual Property Harms with Black Hat Hacking

Does an employee or business partner who has been initially granted access to a network through a contract lose such authorization if she accesses digital information for undesirable purposes in the opinion of her employer? By breaching her contract while accessing a network does she automatically become a "hacker"? The circuits are split in response.[130] These employee "contract hacker" cases roughly fall into two categories—what we might label cases dealing with alleged "thieves and vandals" and cases dealing with alleged "slackers."

---

125. *Id.* at 461.

126. *See, e.g.*, Dick Thornburgh, *The Dangers of Over-Criminalization and the Need for Real Reform: The Dilemma of Artificial Entities and Artificial Crimes*, 44 AM. CRIM. L. REV. 1279, 1284 (2007) ("[Judge Chin] took the rare step of overriding a jury's guilty verdict and granting a motion for judgment of acquittal . . . because the government failed to prove fraudulent or deceptive conduct . . . .").

127. *See Drew*, 259 F.R.D. at 453.

128. *See* Harley Geiger, *Senate Judiciary Committee Passes Three Data Security Bills*, CTR. FOR DEMOCRACY & TECH. (Sept. 23, 2011), https://www.cdt.org/blogs/harley-geiger/239 senate-judiciary-committee-passes-three-data-security-bills.

129. Cyber Crime Protection Security Act, S. 2111, 112th Cong. (as introduced, Feb. 15, 2012), *available at* http://thomas.loc.gov/cgi-bin/query/z?c112:S.2111:.

130. For a discussion of the split, see, e.g., Robert C. Kain, *Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, but Illegal in Miami, Dallas, Chicago, and Boston*, 87 FLA. BAR. J. 36 (2013).

a) The Alleged Thieves and Vandals

In *International Airport Centers, LLC v. Citrin*, Citrin, an employee who quit to start his own business, deleted data before turning in his company-issued laptop, including data that may potentially have demonstrated a breach of his noncompetition agreement.[131] He also installed a program to write over deleted files in order to prevent their recovery.[132] The employer sued, alleging violations of CFAA, violations of his employee's duty of loyalty, and breach of his employment contract.[133] The Seventh Circuit found a violation of the CFAA, using an inherently technology-exceptionalized analysis discussed in Part II, that "Citrin's breach of his duty of loyalty terminated . . . any rights he might have claimed as [the company's] agent . . . and with it his authority to access the laptop."[134]

Other courts have disagreed.[135] In *LVRC Holdings LLC v. Brekka*, the Ninth Circuit expressly declined to follow *Citrin* on the definition of access deemed "without authorization" under the CFAA.[136] There, Brekka had been employed by LVRC, but maintained two consulting businesses with LVRC's

131. 440 F.3d 418, 419 (7th Cir 2006).

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

133. *Id.* at 418–19.

134. *Id.* at 420–21; *see also* United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010) (upholding the conviction a worker for the Social Security Administration accessed the personal records of friends and acquaintances under 18 U.S.C. § 1030(a)(2)(B), which applies to government computers); EF Cultural Travel BV v. Explorica, Inc. 274 F.3d 577, 578–80, 585 (1st Cir. 2001) (finding a basis for CFAA liability where an employee's automated search queries violated the scope of his employment agreement); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp 2d 1121, 1124 (W.D. Wash. 2000) (concluding that once the employee acted on interests adverse to those of his employer by disseminating trade secret information via e-mail, he acted "without authorization" and could therefore be held liable under the CFAA). *But see Nosal II*, 676 F.3d 854, 855–56, 864 (9th Cir. 2012) (en banc) (finding that a group of employees' transfer of corporate information to a former employee did not provide a basis for a CFAA claim); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129–30, 1137 (9th Cir. 2007) (concluding an employee's transfer of corporate information to his personal email account did not trigger a CFAA violation).

135. A number of courts in other circuits have declined to follow *Citrin*. *See, e.g.*, Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373 (S.D.N.Y. 2010); ReMedPar, Inc. v. AllParts Medical, LLC, 683 F. Supp. 2d 605 (M.D. Tenn. 2010); US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1194 (D. Kan. 2009) ("The court agrees that the CFAA cannot be read to encompass (and criminalize) frauds that happen to involve the use of a computer someplace during the course of its commission."); Diamond Power Intern., Inc. v. Davidson, 540 F. Supp. 2d 1322, 1342–43 (N.D. Ga. 2007) (finding that employee's alleged misappropriation of employer information using employer's computer network did not provide a basis for a CFAA claim); B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007) (holding that accessing and deleting employer's files did not provide a basis for an employer's CFAA claim).

136. 581 F.3d 1127, 1134 (9th Cir. 2009).

knowledge.[137] While an LVRC employee, Brekka had e-mailed some LVRC documents to a personal email account, including a financial statement and marketing budget.[138] After Brekka terminated his employment, LVRC discovered that Brekka had accessed the company website using his log-in.[139] LVRC sued on the basis of both the emailed documents and the access after terminating employment.[140] But LVRC and Brekka had no written employment agreement, and LVRC had no published policy prohibiting employees from emailing LVRC documents to their personal computers.[141] The Ninth Circuit ruled that criminal statutes must be interpreted to require that defendants have ample notice regarding what actions are criminal, and that Brekka had not agreed to keep emailed documents confidential or to return or destroy them at the conclusion of his employment.[142] As the Ninth Circuit articulated in *Brekka*:

> For purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations . . . A person uses a computer "without authorization" under [section 1030(a)(4) only] when the person has not received the permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.[143]

These two cases suggest that employers, trade secret owners, and copyright owners may view the CFAA as providing a "bonus" cause of

137. *Id.* at 1129.
138. *Id.*
139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.* at 1133–35. In *United States v. Nosal*, a Ninth Circuit panel held that a former employee could be indicted under the CFAA for exceeding authorized access when he violated the employer's computer access policies and persuaded three employees of an executive search firm to help him start a competing business. *Nosal I*, 642 F.3d 781, 784–89 (9th Cir. 2011). The three employees sent the defendant source lists, names and contact information from the company's database. *Id.* at 783. The Ninth Circuit panel reversed a district court holding that the employees, who had permission to access work computers, did not exceed their authorized access for purposes of the CFAA. However, the Ninth Circuit granted a rehearing en banc, reversing the panel to bring the holding in line with *Brekka*. *Nosal II*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

action when traditional contract breach claims are more appropriate.[144] Under this dynamic, when an employee extracts data through digital means rather than, for example, by copying the same information by hand, a court might apply additional damages simply because a computer was used for the copying. This type of exceptionalized analysis, apart from weaponizing breach and providing greater than appropriate remedies, also privileges one technology over another illogically: a handwritten copy of secret information becomes somehow less evil than an emailed copy of the same information. Meanwhile, as Professor Kerr has argued, because the CFAA's scope of covered technologies may now apply very broadly, the question of whether using a copier to copy the same information (instead of emailing it) now falls under the CFAA is unclear.[145] As an result, the damage analysis might no longer turn on the value of the information taken, but rather on the means of its copying.

b) The Alleged Slackers

Perhaps one the most obvious attempts at employer abuse of the CFAA and weaponized breach involves a case where an employer alleged that an employee who spent excessive (in the employer's opinion) amounts of work time on Facebook, violating the technology use policy of the workplace and, through this breach, the CFAA.[146] In *Lee v. PMSI, Inc.*, a Florida court rejected this weaponized breach analysis proposed by the employer.[147] The court asserted that:

> Both the letter and the spirit of the CFAA convey that the statute is not intended to cover an employee who uses the internet instead of working . . . . The definition of "loss" contemplates damage to a system or data, rather than a lack of productivity . . . . Because the only information Lee allegedly accessed was on the personal

144. *See also* Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268 (S.D. Fla. 2003). There, Four Seasons litigated to protect its database of customer preferences from use by a former business coventurer, with whom a contract existed. *Id.* at 1271–72. The court found that the Four Season's detailed customer profiles qualified as trade secrets under Uniform Trade Secrets Act: the information had economic value, was not generally known or readily available by others, and was the subject of reasonable efforts by licensor to preserve its secrecy. *Id.* at 1326. The court valued the data at $2,090,000, doubled it as a penalty, and then added still more damages under the Computer Fraud and Abuse Act because of the means of acquisition. *Id.* at 1327; *see also* Salestraq America, LLC v. Zyskowski, 635 F. Supp. 2d 1178 (D. Nev. 2009) (considering the intersection of trade secret and computer intrusion law).

145. *See* Kerr, supra note 109, at 1562.

146. Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028, at *1 (M.D. Fla. May 6, 2011).

147. *Id.*

> websites, not PMSI's computer system, Lee never "obtained or alter[ed] information in the computer." Lee accessed her facebook [sic], personal email, and news websites but did not access any information that she was "not entitled so to obtain or alter."[148]

Florida courts have also held that checking personal email, even when it may contain information that breaches employer agreements with a defendant, does not constitute a violation of the CFAA.[149] However, employers in other jurisdictions will undoubtedly attempt to weaponize contract claims with the CFAA to reach alleged "slackers" and other courts, unlike this Florida court, may find the argument credible.

As I argue in Part III, *infra*, contract law and other bodies of law already embody adequate vehicles for providing remedies in almost all instances, even in complicated cases of improperly used information by "hacker" insiders. Because courts in general do not award information misuse damages under CFAA recoveries, employers' ability to threaten criminal prosecution for a contract breach in technology contexts creates a new type of punishment for disloyalty—the "digital peonage" concern discussed at Section II.B.2, *supra*. Digital peonage presents potentially problematic constitutional concerns. As the Court explained in *Pollack v. Williams*, "[w]hatever of social value there may be, and of course it is great, in enforcing contracts and collection of debts, Congress has put it beyond debate that no indebtedness warrants a suspension of the right to be free from compulsory service."[150] Particularly when the Supreme Court has already indicated an unwillingness to enforce contract regimes where employees' fear that merely leaving employment may give rise a criminal charge, this reasoning is likely to be expanded to the question of employee exit and the risk of computer intrusion charges. As explained in Part I, *supra*, such a regime would be highly subject to the possibility of employer abuse.[151]

148. *Id.* at *1–3.

149. *See* Clarity Servs. v. Barney, 698 F. Supp. 2d 1309, 1313–14, 1316 (M.D. Fla. 2010) (rejecting company's claim under 18 U.S.C. § 1030 where an employee solicited and read an email from a customer on the employee's company email account after resigning from the company, and deleted information from his company laptop before returning the laptop to his former employer, holding that the defendant did not lack authorization to access the information or exceed his authorization).

150. Pollock v. Williams, 322 U.S. 4, 18 (1944).

151. *See* Kathleen Kim, *The Coercion of Trafficked Workers*, 96 IOWA L. REV. 409 (2011) (discussing modern peonage contexts).

3. Entrepreneurs as "Contract Hackers": Confusing Innovation with Black Hat Hacking

Arguably the most complex category of "contract hackers" for purposes of a CFAA analysis are those who agree to a contract, but whose activities later exceed the boundaries of authorized conduct when they apply their own code or specialized knowledge. At least two types of commercial cases potentially implicate these behaviors: (1) entrepreneurs who author applications performing services on behalf of users, and (2) competitors or entrepreneurs who use code to aggregate information.

a) Application Builders

The first category of these entrepreneur "contract hacker" cases involve computer applications that have been assigned express authorization from a user—a user who has entered into a contract with each party—to perform services on behalf of that user. A recent California case, *Facebook v. Power Ventures*, raises the specter of this type of CFAA case in the future.[152] In that case, Facebook sued a company providing a content curation application.[153] The application allowed Facebook users to access their own messages, friends lists, and other content from their profiles on various social networking websites inside a single application.[154] Facebook argued that by offering these services,[155] Power Ventures violated Facebook's terms of use and, therefore, the CFAA and California computer crime law.[156]

This weaponized breach argument is problematic. It can be argued that a Facebook user simply assigns her access rights to Power Ventures when using the aggregation application. As a matter of basic contract, it is not clear that Power Ventures stands in privity with Facebook; if Power Ventures is not in privity with Facebook, a breach of a contract by Power Ventures cannot exist. Thus, the weaponized breach argument must fail immediately purely on the most basic contract formation grounds. However, assuming that Power Ventures lacks privity, then the party who is in privity with Facebook and may have breached the terms is the average consumer user who authorized the Power Ventures application. In other words, we return

152. 844 F. Supp. 2d 1025, 1027 (N.D. Cal. 2012).

153. *Id.*

154. *Id.*

155. *Id.* at 1027–28. Power Ventures also sent out advertising emails that appeared to be originated by Facebook email accounts. *Id.* Consequently, Facebook also argued that Power Ventures violated the CAN-SPAM Act. The court agreed, and granted summary judgment. *Id.* at 1030.

156. *Id.* at 1036–38.

right back to the deeply troubling Grandma and Dr. Whiskers hypothetical and its implications discussed earlier in this section.

However, even assuming Power Ventures is in privity with Facebook, a contract breach argument against an application builder like Power Ventures is weak at best. Conducting a traditional breach analysis, the existence of any economic harm to Facebook due to this type of intermediation will be difficult to prove. In fact, intermediation and applications that facilitate user content creation may be examples of desirable technology entrepreneurship, not commercially harmful conduct. Here again the appeal of a weaponized breach analysis for plaintiffs becomes apparent: in a breach analysis weaponized with the CFAA, the extent of economic damages becomes basically irrelevant for criminal application of the CFAA. Consequently, the potency of a possible CFAA charge is clear, even when no recourse would be appropriate for the breach under contract law.[157] Weaponized breach offers a vehicle for existing market players to limit entrepreneurial efforts that build on their business models.

b) Data Aggregators

The second group of entrepreneur "contact hacker" cases involves data aggregators seeking to technologically capture and use information. A number of cases to date have involved competitor aggregators using automated programs such as spiders to capture information from a company's website for their own business interests in this manner.

Recently, in *United States v. Lowson*, a New Jersey court allowed a criminal prosecution arising out of a weaponized breach claim to continue to trial.[158] The defendant ticket aggregators and resellers were accused of taking various steps to defeat Ticketmaster's code-based security measures, including CAPTCHAs and encryption and implementing "hacks" and using backdoors to enable automated programs to purchase tickets.[159] The defendants also

157. In *Power Ventures*, this question of whether any contract damages existed was not reached. On summary judgment the court chose not to analyze the question of whether a contract existed, instead focusing on the changes in IP addresses made by Power Ventures as acts of circumvention of technological limitations on access. *Id.*

158. Indictment at 1, United States v. Lowson, No. 2:10-cr-00114-KSH (D.N.J. Feb. 23, 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2010/03/wiseguys-indictment-filed.pdf.

159. CAPTCHAs or HIPs are typing tests used to ascertain that a particular user is a human rather than a bot. *See* Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096, 1112 (C.D. Cal. 2007) ("Here, CAPTCHA both *controls access* to a protected work because a user cannot proceed to copyright protected webpages without solving CAPTCHA, and *protects rights* of a copyright owner because, by preventing automated access to the ticket purchase webpage, CAPTCHA prevents users from copying those pages.").

allegedly disregarded cease-and-desist letters and hired programmers to defeat security restrictions.[160] The prosecution's argument hinged at least in part on a weaponized breach argument: the indictment stated that the defendants' behavior was an act of computer intrusion in part because "[ticket v]endors using CAPTCHA technology on their websites routinely added Terms of Service that expressly stated that users were not permitted to access a CAPTCHA-protected website using automated software."[161] By including this argument, the prosecution implied that the basis for unauthorized access under the CFAA arose out of a breach of the Terms of Service.[162] Problematically, although the matter ultimately ended in a plea bargain, the court initially denied the motion to dismiss, apparently indicating that the court afforded some traction to the argument that a criminal violation of the CFAA can be predicated on a breach of contract.[163]

The use of this weaponized breach line of argument in these data aggregator entrepreneur cases is a relatively new development. Looking back to earlier case law dealing with data aggregators, such as *Register.com v. Verio*, we see allegations of both contract breach and violations under the CFAA.[164] In *Verio*, however, the court identified those claims as separate rather than combining them under a single cause of action.[165] Even Ticketmaster, one of the vendors most interested in the prosecution of the defendants in *Lowson*, had not connected breach of contract claims with CFAA claims in previous rounds of litigation against data aggregators.[166] For example, in *Ticketmaster v. Tickets.com*, Ticketmaster had attempted to pursue claims under contract,

160. United States v. Lowson, No. 2:10-cr-00114-KSH, at *12 (D.N.J. Oct. 12, 2010) (ruling on motion to dismiss), *available at* http://www.wired.com/images_blogs/threatlevel/2010/10/Wiseguys_Ruling-on-Motion-to-Dismiss.pdf.

161. *Id.* at 10.

162. Indictment at 1, United States v. Lowson, No. 2:10-cr-00114-KSH (D.N.J. Feb. 23, 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2010/03/wiseguys-indictment-filed.pdf.

163. United States v. Lowson, No. 2:10-cr-00114-KSH, at *8 (D.N.J. Oct. 12, 2010) (ruling on motion to dismiss), *available at* http://www.wired.com/images_blogs/threatlevel/2010/10/Wiseguys_Ruling-on-Motion-to-Dismiss.pdf.

164. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 425, 439 (2d Cir. 2004) (separately assessing the merits of a breach of contract claim and a CFAA claim in connection with an alleged violation of terms of use).

165. *Id.*

166. *See, e.g.*, Defendant's Motion to Dismiss, Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654HLHVBKX, 2000 WL 525390 (C.D. Cal. Mar. 27, 2000); Defendant's Motion for Summary Judgment, Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654HLHVBKX, 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003).

copyright, and trespass to chattels as independent bases of recourse.[167] Only the contract law claim survived summary judgment.[168] As such, it is perhaps unsurprising that in this next iteration of commercial wrangling between established internet companies and data aggregators, this new and particularly aggressive strategy has emerged—an attempt to buttress contract claims with a second harsher regime through breach weaponized with the CFAA.

4. Security Researchers as "Contract Hackers": Confusing Code Auditing and White Hat Hacking with Black Hat Hacking

Perhaps the most problematic group of "contract hackers" are information security researchers who may violate terms in an end user license agreement in the course of their research into the behaviors of websites or other technology-related products. These researchers hold a vital consumer protection role in the ecosystem of information security vulnerabilities that cannot easily be filled any other way.[169] Although determining who qualifies as a security vulnerability researcher, the permissible scope of information security research, and proper disclosure processes are a matter of debate,[170] what has become clear is that some researchers' work in the security space, such as the work of computer academics, is essential as a code audit mechanism.[171] Knowing that code is reviewed by third parties after release for security vulnerabilities and privacy invasive conduct keeps companies honest, and it prevents severe information security harms from spreading throughout the digital ecosystem.[172]

As I have explained in other work, sometimes code can behave in ways that damage consumers and enterprise information security, but the authors of the code do not always feel obligated to prevent these harms or disclose the risk.[173] Third-party information security researchers frequently uncover these risks and alert the public.[174] For example, researchers play a vital role in identifying vulnerabilities related to digital rights management ("DRM") tactics that companies sometimes use in the name of intellectual property

167. Ticketmaster Corp v, Tickets.com, Inc. No. CV99-7654 HLHVBKX, 2003 WL 21406289, at *1 (C.D. Cal. Mar. 7. 2003).

168. *Id.* at *2–3, *6.

169. For a discussion of the role of information security researchers in the software ecosystem, see Andrea M. Matwyshyn, *Hacking Speech*, 107 NW. L. REV. 795 (2013).

170. For a discussion of diverging norms in information security vulnerability disclosure, see *id.* at 825–27.

171. *Id.*

172. *Id.*

173. *See* Matwyshyn, *supra* note 47, at 438–41.

174. *See* Bruce Schneier, *Sony's DRM Rootkit: the Real Story*, SCHNEIER ON SECURITY (Nov. 17, 2005), http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html.

protection, tactics which are sometimes functionally similar or identical to the tactics used by black-hat hackers.[175] The key difference is that, ostensibly, the DRM is placed on the user's hard drive with contractual consent from the user through the product's end user license agreement. In practice, however, the agreement may not explain the manner in which the code behaves. Without a third party-technology expert analysis of the behavior of the code, the marketplace will never know how this code functions—functionality that may cause millions of dollars of information security damage.[176]

Each time a security researcher analyzes a product or decompiles it to track behaviors for the benefit of all users of the product, the researcher now potentially risks criminal prosecution as a result of an alleged contract breach in the course of a code audit. Numerous examples exist with respect to security researchers—including Ivy League academics—being threatened with litigation and even criminal prosecution in connection with their research into information security vulnerabilities.[177] If weaponized breach analysis persists, society imposes on information security researchers a very high legal cost for engaging in socially beneficial research.

Meanwhile, in a less traditional research space, sometimes one company's information security researchers discover vulnerabilities in another company's products. In this scenario, a company that becomes annoyed with a competitor's disclosing their vulnerabilities may attempt to legally sanction the individual researchers working for the competitor, as well as the competitor itself, with CFAA-weaponized breach claims. There have already

175. *Id.* Digital rights management technologies are code-based methods of limiting a user's ability to interact with digital content.

176. *See* Deirdre K. Mulligan, *The Magnificence of the Disaster: Reconstructing the Sony MBG Rootkit Incident*, 22 BERKELEY TECH. L.J. 1157, 1158 (2007) (discussing the Sony DRM rootkit incident).

177. By way of example, let us take the case of Professor Edward Felten at Princeton University, formerly the chief technologist at the Federal Trade Commission. *FTC Names Edward W. Felten as Agency's Chief Technologist; Eileen Harrington as Executive Director*, FED. TRADE COMM'N (Nov. 4, 2010), http://www.ftc.gov/opa/2010/11/cted.shtm. Professor Felten, his colleagues, and his graduate students in his lab at Princeton frequently audit code in order to assess the behaviors for consumer protection reasons. *See* CENTER FOR INFORMATION TECHNOLOGY POLICY AT PRINCETON UNIVERSITY, https://citp.princeton.edu/research/ (last visited Feb. 28, 2012). Their research, which undoubtedly breaches end user license agreements and terms of use at least occasionally, now carries with it a risk of criminal prosecution under the CFAA. Yet it is indisputable that their research fulfills a critical role in the information ecosystem. Professor Felten himself was already once threatened with criminal prosecution for his research under the Digital Millennium Copyright Act in connection with publishing a paper exposing flaws in a DRM technology. *See* Letter from Matthew J. Oppenheim, Esq., RIAA Counsel, to Professor Edward Felten (Apr. 9, 2001), *available at* http://cryptome.org/sdmi-attack.htm.

been squabbles between major technology companies over precisely these dynamics,[178] and major information security conferences have been disrupted with speakers being sued over allegedly violating the CFAA via a breach of contract.[179] Most such disputes end in settlement. Currently, however, the legal questions remain unresolved and the dynamics remain volatile.

B. THE RISKS OF WEAPONIZING BREACH WITH THE CFAA

As the previous Section's discussion illustrated, contract breach weaponized with the CFAA implicates at least four different types of "contract hackers" and strategic litigant interests. As a result, a blanket weaponized breach approach further balkanizes traditional contract law in a particularly destructive manner. First, weaponized breach derails contract doctrine through judicial activism. Second, it eviscerates the possibility of a contract theory discourse regarding the nature, morality, and appropriate consequences of breach. Third, it disrupts the private ordering that has been the main regulator of technology-mediated spaces to date. Fourth, weaponized breach harms entrepreneurship and innovation policy. Finally, it stunts development of other, perhaps more suitable legal regimes to address information harms. The remainder of this Part considers each of these negative consequences in turn.

1. Contract Doctrine and Judicial Activism

Weaponizing breach with a CFAA analysis threatens the future of contract doctrine. The CFAA offers no guidance on the relationship between contract and computer intrusion, and Congress has never directly addressed their interplay.[180] The paradigm that existed in the minds of legislators at the

178. *See, e.g.*, Graham Cluley, *Tavis Ormandy – are you pleased with yourself? Website exploits Microsoft zero-day*, SOPHOS NAKED SECURITY (June 15, 2010), http://nakedsecurity.sophos.com/2010/06/15/tavis-ormandy-pleased-website-exploits-microsoft-zeroday/ (describing tension between Microsoft Corporation and a Google employee's chosen method of vulnerability disclosure). Vulnerabilities may be found by one company in another's product when, for example, a researcher is trying to customize or secure their own products to interoperate with the vulnerable product.

179. *See, e.g.*, Jennifer Granick, *An Insider's View of Ciscogate*, WIRED.COM, Aug. 5, 2005, http://www.wired.com/science/discoveries/news/2005/08/68435?currentPage=2 (describing the events around Michael Lynn's disclosure of a vulnerability in Cisco IOS software).

180. In 1986, Congress deleted the part of the statute that prohibited those with authorization from using the system for unauthorized purposes and substituted the phrase "exceeds authorized access." *See* Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (quoting S. Rep. No. 99-432, at 9 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2486). The *Werner-Masuda* court explained the change as follows: "By enacting this amendment, and providing an express definition for exceeds authorized access, the intent was to eliminate coverage for authorized access that

time of passage of the CFAA was most likely that of the "hacker"—a third-party outsider or "black hat" hacker. It is unlikely that entrepreneurs, information security researchers and, in particular, the Grandma and Dr. Whiskers of the world were within the mental model of "hackers" legislators used as the basis for the CFAA.[181] As such, judicial restraint in interpretation of breach and the CFAA is warranted rather than building a common law of the zebra. Until Congress speaks directly on this matter, judicial restraint is appropriate. In the words of a lower court, even assuming that "[w]hat the Government is seeking to do is to punish conduct that reasonable people might agree deserves the sanctions of the criminal law," the wiser course was to leave it to Congress to prescribe crime and establish penalties.[182]

> Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market . . . . Congress has the institutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.[183]

Contract law is predominantly a state law construct, and without clear evidence of Congressional intent to the contrary, courts should not interfere with state-law contract claims by weaponizing them under the federal CFAA. In *Morrison v. National Australia Bank*, the Supreme Court cautioned against "judicial speculation-made-law divining what Congress would have wanted if it had thought of the situation before the court."[184] Yet, that is precisely what judicial activism in expanding the reach of the CFAA to mere breaches of contract does. As the Court has elsewhere noted, "the historic police powers

aims at purposes to which such authorization does not extend, thereby removing from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization." *Id.* at 499 n.12 (quoting S. Rep. No. 99-432, at 21, reprinted in 1986 U.S.C.C.A.N. at 2494–95) (internal quotations omitted).

181. Recent Senate Judiciary Committee activity indicates that some members of Congress disagree with the idea of extending the CFAA to cover consumers who breach contracts. *See* Geiger, *Senate Judiciary Committee Passes Three Data Security Bills*, *supra* note 128.

182. United States v. LaMacchia, 871 F. Supp. 535, 544 (D. Mass. 1994) (citing Dowling v. United States, 473 U.S. 207, 225 (1985)).

183. *LaMacchia*, 871 F. Supp. at 544 (citing Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984)).

184. 130 S. Ct. 2869, 2881 (2010).

of the States [are] not to be superseded by [a] [f]ederal Act unless that was the clear and manifest purpose of Congress."[185]

One of the strategic benefits a weaponized breach claim may offer a litigant is a basis for removing a run-of-the-mill state contract law dispute to federal court.[186] While this may be desirable for some litigants, flooding the federal courts with contract claims has systemic consequences. Contract claims belong in state courts as a general rule. If increasing numbers of contracts involve some aspect of technology, and if the weaponized breach litigation trend continues, soon the federal courts may find themselves overwhelmed with litigants asserting weaponized breach claims.[187]

Furthermore, in the context of entrepreneur "contract hackers," another reason why the CFAA-weaponized contract breach claims have gained popularity among litigants may be because they are the only claims that "stick" in technology contexts that offer more aggressive penalties.[188] However, this type of overreaching by leveraging contract to latch onto federal law remedies is unnecessary and misguided. Other regimes already exist to provide remedy for these harms. State trade secret law, for example, already protects confidential information of various types that is frequently not otherwise protectable under other areas of intellectual property law.[189] However, if trade secret does not cover the alleged harm at issue, then perhaps only a contract law remedy, or no remedy at all, is appropriate.

185. Wyeth v. Levine, 129 S. Ct. 1187, 1194–95 (2009) (quoting Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947)).

186. *See, e.g.*, Justin R. Long, Against Certification, 78 GEO. WASH. L. REV. 114, 119 (2009) ("Plaintiffs can choose where to file, and defendants can choose whether to remove, based on strategic considerations of how the lower state and federal courts have treated the open question of state law in the case.").

187. When faced with a similar tension in the context of tort law and federal actions under Section 1983, the Supreme Court clearly indicated that only state law remedies apply. *Paul v. Davis*, 424 U.S. 693, 700–01 (1976) (considering whether a privacy interest was violated by a flyer posted by an officer alleging Davis was an "active shoplifter" and presented cause of action under Section 1983). As the Court in *Davis* asserted, "Congress should not be understood to have attempted 'to make all torts of state officials federal crimes.' It brought within (the criminal provision) only specified acts 'under color' of law and then only those acts which deprived a person of some right secured by the Constitution or laws of the United States." *Id.* at 700 (citing *Screws v. United States*, 325 U.S. 91, 109 (1945)).

188. *See* discussion *supra* Section III.A.3.

189. For example, in some states, trade secret law may protect a client list, while neither copyright nor patent law would provide protection for a client list. For a discussion of trade secret law and client lists, see Erini R. Svokos, *What About the Client? Trade Secret Law and Fiduciary Duty Law as Applied to Law Firm Client Lists*, 24 GEO. J. LEGAL ETHICS 937, 941 (2011).

But, one might argue, perhaps penalizing the mere use of technology as part of a commercial transaction in breach is a socially desirable state of affairs.[190] I argue it is not. Punishing breach more harshly in digital contexts in essence creates a type of technology contracting "tax" that is anathema to Congress's asserted intent of crafting parity for digital and offline contracts. Specifically, in the E-Sign Act, Congress has articulated an express goal of legal equivalence between technology-mediated contract and physical, offline contracts.[191] Thus, an exceptionalized breach analysis runs contrary to Congress's explicit intent. Congress' goal in the E-Sign Act might also be described as seeking to extend contract law into digital spaces, but only in a minimally disruptive manner, and certainly not in a manner that supplants existing contract doctrine.[192]

2. How Weaponized Breach Disrupts Contract Theory

Just as a weaponized breach analysis disrupts the relationship of contract doctrine and may run afoul of Congressional intent, it also problematizes contract theory and scholarship. Neither a traditional efficient breach/"bad man" approach to contract analysis nor an autonomy theory analysis can co-exist with weaponized breach. In 1897 Supreme Court Justice Oliver Wendell Holmes articulated a "strict liability" approach to contract breach: "The duty to keep a contract at common law means a prediction that you must pay damages if you do not keep it, and nothing else."[193] A traditional law-and-

190. For example, perhaps one can argue that we are inevitably moving toward a surveillance society where human relationships and legal responsibility need to be reconfigured to acknowledge this new reality. Perhaps traditional legal balances between liberty interests and criminal responsibility and civil liability should be disregarded.

191. Electronic Signatures in Global and National Commerce Act ("E-SIGN") Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified at 15 U.S.C. §§ 7001–7006, 7021, 7031 (2000)). Although Congress has usually been substantially behind the pace of technology innovation with respect to making law, one notable example of forward-thinking occurred—the E-Sign Act. In the context of legislating rules for technology-mediated contract formation, federal and state digital signature legislation established parity for physical space and virtual space technology-mediated signatures at a relatively early point in the mainstreaming and commercialization of the Internet.

192. *See generally* Stephen E. Friedman, *Protecting Consumers from Arbitration Provisions in Cyberspace, the Federal Arbitration Act and E-Sign Notwithstanding*, 57 CATH. U. L. REV. 377 (2008) (providing discussion of the E-Sign Act); Stephen E. Blythe, *Digital Signatures Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in e-Commerce with Enhanced Security*, 11 RICH. J.L. & TECH. 6 (2005) (comparing digital signature legislation in the European Union, United States, and United Kingdom).

193. O.W. Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 462 (1897). As more recently expressed by Justice Scalia: "Virtually every contract operates, not as a guarantee of particular future conduct, but as an assumption of liability in the event of

economics notion of efficient breach, as well as this Holmesian "bad man" notion—i.e. one which views breach as a viable option provided one pays damages arising therefrom—view a contractual promise being no more than an option to breach and pay damages.[194] An efficient breach approach does not consider compensated breach to be wrongful. In fact, if it is efficient, it may even be desirable.[195] One such debate focuses on whether the act of breaching a contract is even itself a legal wrong or merely a choice that a party in privity makes with respect to performing or paying damages. Professor Shiffrin cites Justice Holmes and argues that breach of contract is "not a legal wrong" because the law views every contract as an agreement in the alternative—to perform or to pay an amount of money equal to the value of performance.[196]

A weaponized breach analysis also does not comport with an autonomy theory analysis of contract, which focuses on the bilateral structure of contractual liability and expectation damages.[197] As Professor Oman argues:

> [A]utonomy itself places limits on the sort of remedies that the law can impose. The basic intuition behind this argument is that specific performance represents a greater intrusion into personal freedom than do money damages, and so long as damages compensate the promisee for her loss, we ought to choose the remedy that intrudes on liberty the least.[198]

Similarly, Charles Fried, a defender of an autonomy theory of contract, writes:

> If I make a promise to you, I should do as I promise; and if I fail to keep my promise, it is fair that I should be made to hand over the equivalent of the promised performance. In contract doctrine this proposition appears as the expectation measure of damages for breach. The expectation standard gives the victim of a breach no

nonperformance . . . ." United States v. Winstar Corp., 518 U.S. 839, 919 (1996) (Scalia, J., concurring).

194. *See* Barry E. Adler, *Efficient Breach Theory Through the Looking Glass*, 83 N.Y.U. L. REV. 1679 (2008) (arguing that a willful efficient breach must simply be priced accurately).

195. *Id.*

196. Thus, for Professor Shiffrin "contract diverges from promise" in that the "contents of the legal obligations and the legal significance of their breach do not correspond to the moral obligations and the moral significance of their breach." Seana Valentine Shiffrin, *The Divergence of Contract and Promise*, 120 HARV. L. REV. 708, 709 (2007).

197. *See* Gregory Klass, *Promise Etc.*, 45 SUFFOLK U. L. REV. 695, 696–97 (2012) (discussing autonomy theory).

198. Nathan B. Oman, *The Failure of Economic Interpretations of the Law of Contract Damages*, 64 WASH. & LEE L. REV. 829, 869 (2007).

> more or less than he would have had had there been no breach—in other words, he gets the benefit of his bargain.[199]

In an environment where choosing not to perform a contractual promise can lead to liberty deprivation, no true "option" to breach exists. Becoming a felon can never be the efficient or autonomous outcome in a contractual relationship. Hence, the contract theory discourse dies, despite a long-standing debate in both the courts and the legal academy about the nature of breach and its connection to morality.[200] Regardless of whether one subscribes to an "efficient breach" or autonomy-driven analysis of contract law, the theory behind providing redress for contract "wrongs" is driven by financial redress on an individual level—not righting a wrong against society as a whole like in criminal law. In the most generous calculations, contract damages provide the benefit of the anticipated bargain to the victim of the breach or, in limited cases, contract law seeks to disgorge ill-gotten gains as a consequence of the breach.[201] Even punitive damages are a disfavored remedy, and liquidated damages provisions are generally enforced only when the stipulated sums are connected to actual economic loss arising from breach, not driven by a desire to punish the breacher.[202]

The possibility of criminal consequences of a mere breach does not, therefore, generally appear in contract discourse. Even if we assume that breach is immoral, contract theory discourse does not equate "immorality"

---

199. CHARLES FRIED, CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION 17–19 (1981).

200. *See generally* Steven Shavell, *Is Breach of Contract Immoral?*, 56 EMORY L.J. 439, 439–57 (2006) (discussing the contract theory debate over breach and morality).

201. *See* RESTATEMENT (SECOND) OF CONTRACTS § 355 cmt. a (1981) ("The purpose[] of awarding contract damages is to compensate the injured party . . . . For this reason, courts in contract cases do not award damages to punish the party in breach or to serve as an example to others unless the conduct constituting the breach is also a tort for which punitive damages are recoverable.").

202. *See* 22 AM. JUR. 2d *Damages* § 574 (2012).

> Punitive damages are generally not available under a contract theory . . . Specifically, courts generally hold as a general rule that punitive damages are not available as a remedy for breach of contract without an underlying tort . . . Courts have explained that punitive damages are not ordinarily recoverable in actions for breach of contract because: (1) the damages for breach of contract are generally limited to the pecuniary loss sustained; and (2) the purpose of punitive damages is not to remedy private wrongs but to vindicate public rights . . . Nonetheless, it has also been held that a contract provision immunizing a party from liability for punitive damages is substantively unconscionable as violating public policy.

Id. (citations omitted).

with criminal penalties like weaponized breach analysis does.[203] Weaponized breach analysis means that, because of the stick of criminal law, one side automatically loses—the side of permissible exit. Thus, with only one logical outcome possible because of the fear of criminal sanctions, the contract theory debates are obliterated.

Further, the weaponization of breach destroys one of the core doctrinal distinctions in contract law—the distinction between a material and a minor breach.[204] When breach is weaponized, even a minor breach can ostensibly provide the basis for a criminal penalty under the CFAA or a duplicative financial penalty under both civil CFAA remedies and traditional contract remedies. A weaponized breach analysis is counter to the contract default rule of preserving contractual relationships whenever possible.[205] When a party's breach is material, the nonbreaching party has the option of receiving damages and terminating the contractual relationship. However, in an instance of a minor breach, courts prefer to preserve the existence of the relationship and simply award damages to compensate for actual losses suffered by the nonbreaching party.[206] As such, it can be said that the dominant lens courts apply is closer to a relational notion of contract than a moralistic one that views breaches as irretrievable wrongs.[207] But, again, in a

---

203. *See* DAVID HUME, A TREATISE OF HUMAN NATURE 523 (L.A. Selby-Bigge ed., 2d ed. 1978) (describing promise-keeping as a social good, saying that "a sentiment of morals concurs with interest, and becomes a new obligation upon mankind."). As Fried explains:

> There exists a convention that defines the practice of promising and its entailments. This convention provides a way that a person may create expectations in others. By virtue of the basic Kantian principles of trust and respect, it is wrong to invoke that convention in order to make a promise, and then to break it.

FRIED, *supra* note 199, at 17. *But see* Richard Craswell, *Contract Law, Default Rules, and the Philosophy of Promising*, 88 MICH. L. REV. 489, 489 (1989).

> [A]nalyses such as Fried's have little or no relevance to those parts of contract law that govern the proper remedies for breach, the conditions under which the promisor is excused from her duty to perform, or the additional obligations . . . imputed to the promisor as an implicit part of her promise.

Id.; *see also* Steven Shavell, *Why Breach of Contract May Not Be Immoral Given the Incompleteness of Contracts*, 107 MICH. L. REV. 1569, 1569 (2009) ("[Although it is a] widely held view that breach of contract is immoral . . . breach may often be seen as moral, once one appreciates that contracts are incompletely detailed agreements and that breach may be committed in problematic contingencies that were not explicitly addressed by the governing contracts.").

204. 23 WILLISTON ON CONTRACTS § 63:3 (4th ed.)

205. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 237 (1981).

206. *Id.*

207. *See* Macaulay, *Relational Contracts*, *supra* note 42, at 793–94 (discussing relational contracts).

weaponized breach analysis, particularly one marked with the possibility of prison, this distinction disappears. Every breach becomes the basis for a possible corollary criminal charge. Thus, with weaponized breach a type of permanent specific performance mandate suddenly pertains to all contractual obligations no matter how big or small and no matter how efficient it might be for all parties involved to breach obligations: each time a party debates breaching an agreement, that party essentially accepts the risk of a potential criminal prosecution.

3. Private Ordering

The law has generally adopted a restrained approach to technology regulation because of the rapid evolution of internet business models, traditionally deferring to business partners' privately ordered arrangements through contract as defining the relationship.[208] Weaponized breach analysis that triggers an immediate right to pursue remedies under the CFAA eliminates this deference. It limits the ability of parties to set their own deal terms through private ordering: an enforcement remedy through the CFAA essentially eviscerates the negotiated contractual deal as the definitive set of rules governing the exchange. The person controlling the technology always holds the ability to inflict criminal punishment for breach on the other party.[209]

In this manner, weaponized breach analysis creates a new technology-driven imbalance in the relationship that the parties cannot contract around: the specter of criminal punishment exists *regardless of the deal terms and even when the two parties are similarly situated*, except for one side managing the network that is implicated by the contract. In a legal regime of weaponized breach, the balance of power between otherwise equally situated parties becomes disrupted if one controls the network and has possible recourse under the CFAA while the other does not. For example, weaponized breach destroys the efficacy of indemnification provisions and limitations of liability as the primary monetary terms of recourse and risk management. Regardless of how the parties negotiated out liability terms and indemnification obligations,

208. *See* Henry H. Perritt, Jr., *The Internet is Changing the Public International Legal System*, 88 KY. L.J. 885, 921–31 (1999) (discussing private ordering and internet regulation).

209. *See, e.g.*, Edward A. Morse, *Private Ordering In Light Of The Law: Achieving Consumer Protection Through Payment Card Security Measures*, 10 DEPAUL BUS. & COM. L.J. 213, 215 (2012); Robert M. Yeh, Note, *The Public Paid for the Invention: Who Owns It?*, 27 BERKELEY TECH. L.J. 453 (2012); D. Gordon Smith, *Private Ordering With Shareholder Bylaws*, 80 FORDHAM L. REV. 125, 127 (2011) (discussing private ordering and various contracts).

the party that controls the technology suddenly holds a trump card–the ability to weaponize any breach.[210]

4. Innovation and Entrepreneurship Policy

The ability of entrepreneurs to experiment with innovative technology business models is threatened when each contractual transgression may result in a criminal sentence. Entrepreneurs face not only the possibility of their own imprisonment under weaponized breach, but further challenges when raising capital, as it creates perverse incentives for venture capitalists to invest in the most novel digital enterprises when those enterprises carry a higher likelihood of contract breach and founder felony convictions. Further, the approach of weaponized breach privileges corporate entities over human ones: a lone inventor who breaches an agreement may find himself facing computer intrusion charges and potentially prison, but a corporation that breaches an agreement faces no incarceration risk under the CFAA.[211] In this way, legally sophisticated entrepreneurs may avoid prison, but the smallest startups where founders have not correctly selected a corporate form to insulate themselves are vulnerable. This state of affairs is highly undesirable as a matter of innovation policy.

Further, weaponizing breach chills innovation policy debates about technology conduct in gray legal areas. For example, norms in the technology community around the appropriate protocols for white-hat, well-intentioned hacking are in flux. Many companies such as Google and Mozilla expressly encourage breaking of their products and offer monetary rewards[212] to researchers who find and submit problems with corporate code. However,

210. Further, this type of a dynamic creates disincentives for the party operating a network or a database to practice good network security and data management practices. As will be discussed later, where the ability to harshly punish through weaponized breach exists, the desire to take precautions against breach diminishes. *See* discussion *infra* Section II.B.4. The failure to take these information security precautions has negative effects outside the business relationship and simultaneously devalues corporate information assets. *See, e.g.*, Andrea M. Matwyshyn, *Imagining the Intangible*, 34 DEL. J. CORP. L. 965, 976–80 (2009) (discussing the devaluation of intangible assets through information security breaches).

211. In the absence of a basis for personal responsibility of the officers and directors of a company, a business entity cannot physically be incarcerated because it is inanimate, even if its officers can be. In other words, only individuals participating in criminal activity may be incarcerated. For a discussion of corporate criminal responsibility, see 18B AM. JUR. 2D *Corporations* § 1640 (2012).

212. Google recently offered a one million-dollar bug bounty for vulnerabilities in Chrome. *See* Kim Zetter, *Google Offers $1 Million in Hacker Bounties for Exploits Against Chrome*, WIRED.COM (Feb. 28, 2012), http://www.wired.com/threatlevel/2012/02/google-1-million-dollar-hack-contest; *see also Bug Bounty Program*, MOZILLA (Mar. 3, 2013), http://www.mozilla.org/security/bug-bounty.html.

other companies view this type of vulnerability research as an intrusion and attack on the integrity of their code.[213] As such, it is likely that a company will attempt to use the CFAA as a weapon against a security researcher on the basis of a contract breach argument.[214] Weaponizing breach in this manner short-circuits the technology policy discussion around white hat hacking and security vulnerability disclosure. Such chilling of this debate is highly undesirable; courts should seek to preserve, not destroy, this ongoing social policy and technology business conversation.

Finally, concerns regarding children's experimentation with technology warrant review. It is clearly in our national interest to encourage children's interest in technology: the next Bill Gates or Steve Jobs is likely in grade school today. Yet, as generations of children grow up as "digital natives"[215] using technology from their very early years, a world of weaponized breach may result in inquisitive six-year olds charged with CFAA offenses for registering their pets as social network users.[216] While I argue elsewhere that a strong form of the capacity doctrine with respect to children's right to disavow their agreements in most cases should be expressly extended to digital spaces, courts do not always adopt this approach.[217] A weaponized breach regime leaves children vulnerable when they are tinkering with code.

5. Competing Legal Regimes

Finally, the weaponized breach approach is appealing to litigants despite its flaws. It is an expedient path to imposing high costs on a breaching party, and litigants are utilizing it with increasing frequency.[218] Because of the

213. For example, Apple recently banned a security researcher from its application store after he demonstrated a vulnerability in iOS. *See* Alex Heath, *Apple Kicks Security Researcher Out Of The App Store After iOS Exploit Demonstration*, CULT OF MAC (Nov. 7, 2011), http://www.cultofmac.com/128577/apple-kicks-security-researcher-out-of-app-store-and-developer-program-after-ios-vulnerability-demonstration/.

214. Companies frequently adopt aggressive postures with security researchers. *See* Robert MacMillan, *Black Hat: ISS researcher quits job to detail Cisco flaws*, *IDGNS*, INFOWORLD.COM (July 27, 2005), http://www.infoworld.com/d/security-central/black-hat-iss-researcher-quits-job-detail-cisco-flaws-088.

215. *See* JOHN PALFREY AND URS GASSER, BORN DIGITAL (2008) (discussing how today's children are growing up as digital natives).

216. *See Nosal II*, 676 F.3d 854, 861 (9th Cir. 2012) (en banc) (noting that the government's asserted statutory construction would criminalize the conduct of "vast numbers of teens and pre-teens" under the CFAA).

217. Andrea Matwyshyn, *Generation C: Childhood, Technology and the Future of Identity*, 87 NOTRE DAME L. REV. 1979, 1983–89 (2012).

218. A query of the Westlaw ALLFEDS database with the search term "CFAA /20 contract" yields an upward trajectory in volume of cases. Between 1996 and 2005, thirteen cases fit these search criteria, but between 2006 and 2011, eighty-five cases fit these criteria. *See* ALLFEDS database, Westlaw, http://www.westlaw.com (Nov. 7, 2012).

convenience and potency of reaching for a weaponized breach CFAA allegation, plaintiffs will consequently be unlikely to invest in litigating more novel and legally appropriate measures of harm. In this way, weaponized breach potentially stunts the development of other bodies of law that could more successfully address exceptional harms that result from the involvement of technology.

For example, tort and other bodies of law may be better suited than weaponized breach to address financial harms that arise in a manner tangential to but not contemplated by contracts. As Professor Bellia argues:

> [A]n approach recognizing a system owner's right to set the conditions of access, so long as she provides adequate notice of those conditions (through actual notice or adopting a system configuration that makes restrictions plain to the user), provides a better baseline for access to network resources than a pure liability rule or one requiring strong technical measures to trigger injunctive relief. In addition, where necessary to compensate for the inadequacies of this sort of property-rule protection, we must look to technology-displacing rules rather than pure liability or strong code-based approaches to achieve the appropriate level of access.[219]

Through crafting a restrained, contract-based approach to digital harms in "contract hacker" cases, disputes which are better addressed through regimes other than contract and criminal law will become more clearly visible for legislators and judges. Yet the law of the horse cannot successfully develop in the shadow of the law of the zebra.

C. WHY COURTS MAY HAVE BECOME CONFUSED

Given the parade of horribles articulated in the sections above, it seems incomprehensible that any court would sanction a weaponized breach analysis. But a number of courts have indeed sent contract doctrine down this path of the law of the zebra. Although the reasons that courts select this destructive choice are not entirely clear, several theories exist.

Professor Ohm argues that a myth of a "superuser" with extraordinary technology skills emerged in policy circles in other legal contexts.[220] Ohm argues that this mythology leads legislators to engage in overzealous regulation to stop the mythical force of this dangerous being.[221] Relying on the theory of moral panic of sociologist Stanley Cohen, Ohm argues that the

219. Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2272 (2004).

220. Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1338 (2008).

221. *Id.* at 1396–97.

superuser or "hacker" is a type of folk devil.[222] Ohm asserts that "[t]he trope arises in every single branch of Internet law, including intellectual property, computer crime, information privacy, information security, Internet governance, telecommunications, innovation policy, First Amendment law, and jurisdiction."[223]

Ohm does not expressly reference contract law in his list of fields affected by this approach, but it is a logical addition. What Ohm calls a folk devil and mythology, I will reframe here as a problem of psychology.[224] Psychology has long studied the heuristics that humans use to classify our existence, especially when we are confronted with novelty. Ascribing negative characteristics to objects or skills we cannot fully understand or fear reflects two psychological phenomena: essentialism and confirmation bias.

1. Essentialism

In developmental psychology, "essentialism" is a form of early cognitive bias describing the tendency to search for hidden, non-obvious features of things.[225] A type of misguided technology essentialism is now visible in judicial contract analysis. Without recognizing their error, people frequently attempt to cope with new situations by trying to generalize existing knowledge to new categories and construct causal explanations in order to make sense of new information.[226] They look for familiarity through the isolation of key shared characteristics across various people or objects. Each person or object of this "kind" then is ascribed a list of characteristics by default. This type of processing, known as "cognitive essentialism,"[227]can give rise to incorrect generalizations, despite its utility in assisting humans in coping and learning. Sometimes this classification taxonomy results in a

222. *Id.* at 1337–38.

223. *Id.* at 1338.

224. I also must respectfully differ with Prof. Ohm when he states: "Computer experts rarely assess a risk of online harm as anything but, 'significant,' and they almost never compare different categories of harm for relative risk." Paul Ohm, *The Myth of the Superuser, Part Three, The Failure of Expertise*, VOLOKH CONSPIRACY (Apr. 11, 2007, 1:09 PM), http://volokh.com/archives/archive_2007_04_08-2007_04_14.shtml#1176311368. As I have argued elsewhere, skilled information security professionals today apply scales of risk to determine the severity of various attacks. Many attacks are routinely found to be unlikely, low-priority and, ergo, not a significant risk. *See* Matwyshyn, *Hidden Engines*, *supra* note 48, at 139–40; *see also* Ryan Hurst, *The Contrition of a Security Practitioner*, UNMITIGATED RISK (May 27, 2010), http://unmitigatedrisk.com/?p=6 (analyzing these dynamics from the perspective of experienced IT professionals).

225. SUSAN GELMAN, THE ESSENTIAL CHILD: ORIGINS OF ESSENTIALISM IN EVERYDAY THOUGHT 6–13 (2003).

226. *Id.*

227. *Id.*

classification fortuitously consistent with that of the external world, but sometimes the taxonomy is incoherent in context of the external world.[228]

A similar dynamic can occur when courts and legislatures encounter seemingly novel legal questions; cognitive biases inevitably creep into legal analysis because law is made by humans for humans. Courts sometimes erroneously fixate on computer use in their analysis of questions of breach. However, this computer use is merely a façade of essentialism and is substantively irrelevant. With increasing frequency, the digital breacher is being essentialized through his association with a computer. Immediately mislabeled "hacking" simply because the breach involves a computer, courts erroneously allow plaintiffs and prosecutors to reach for the CFAA. As discussed in Section III.B.2, *supra*, the various types of breaches of these exceptionalized "contract hackers" actually have little in common conceptually; hence, the one salient characteristic that appears to link them is the involvement of a computer.[229]

In addition to the essentialism visible in contract breach analysis, a similar dynamic exists with courts' and Congress's perceptions not only of "hackers" but of technology expertise in general–an "essentialism" of computer "experts" or "hackers." In the recent debates over SOPA, for example, legislators frequently referenced, in arguably disrespectful fashion, "bring[ing] in some nerds" to explain the technology aspects on digital piracy.[230] This act of "othering" technology experts in a derisive fashion is consistent with the harbingers of essentialist analysis in contract law performed by courts.

2. Confirmation Bias

Framing these observations another way, human decision-making also frequently reflects a "confirmation bias"—the tendency that many people hold to confirm their pre-existing beliefs.[231] Particularly when the topic is an emotionally-charged or threatening issue, confirmation bias is a common occurrence.[232] In essence, confirmation bias demonstrates a form of limited information processing: in lieu of processing information in a scientific way, when a person demonstrates confirmation bias he seek out information that

228. *Id.*

229. *See* discussion *supra* Section III.B.2.

230. *See, e.g.*, Kriss Kritto, *Congress Speak: Nerd*, THE HILL, Dec. 26, 2011, *available at* http://thehill.com/capital-living/congress-speak/201345-congress-speak-nerd.

231. *See, e.g.*, DANIEL HAHNEMAN, THINKING, FAST AND SLOW 62 (2011) (discussing confirmation bias).

232. *Id.*

tends to confirm his existing biases and beliefs about a given problem.[233] Therefore, if a judge or jury holds fears about computers and their destructive potential, this finder of fact may be more susceptible to confirmation bias and fixate on the role of the computer in a breach.

Perhaps because contract disputes involving technology contexts seem novel and more threatening than other contract scenarios, judges may have unconsciously given in to essentialism and confirmation bias. Instead of preserving contractual supremacy and viewing technology exceptionalist legislation as merely a type of "gap filler," judges have overreacted to the novelty of technology in contract. This overreaction should be doctrinally corrected; the law of the zebra should be avoided.

The next Part presents an operationalization of using the restrained technology exceptionalism paradigm for correcting the relationship between contracts, breach, and the CFAA, and resolving the circuit split on this issue.

IV. APPLYING RESTRAINED EXCEPTIONALISM: A PRIVITY MODEL OF AUTHORIZED ACCESS

Although legal literature discusses various aspects of the CFAA, contract law questions connected with this statute have thus far been analyzed primarily as a corollary to an argument based on CFAA analysis or rooted in another area of law. To the extent the civil applications of the CFAA[234] and

233. *See* R.S. Nickerson, *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises*, 2 REV. GEN. PSYCHOL. 175, 177 (1998); P.C. Wason, *On the Failure to Eliminate Hypotheses in a Conceptual Task*, 12 Q. J. EXPERIMENTAL PSYCHOL. 129, 132 (1960).

234. The EFF discusses the CFAA as follows:

> The CFAA is primarily a criminal statute. However, in 1994 a civil suit provision was added that provides a private cause of action if a violation causes loss or damage, as those terms are defined in the statute. 18 U.S.C. § 1030(g) (2006). To state a civil claim for violation of the CFAA, (1) a plaintiff must allege damage or loss; (2) caused by a violation of one of the substantive provisions set forth in § 1030(a); and (3) conduct involving one of the factors in § 1030(c)(4)(A)(i)(I)–(V). *Id.* An action under this section must be bought within two years of the date the act is complained or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware. *Id.* In 2008, Congress amended the CFAA through the Identity Theft Enforcement and Restitution Act, Pub. Law 110-326, 122 Stat. 3560. This amendment enhanced a number of aspects of the CFAA. Most notably, the 2008 amendment eliminated the need for Plaintiff's loss to be greater than $5,000 and made it a felony for a user to cause damage to ten or more computers. *Id.* Thus, while the previous $5,000 threshold has been

breach have been analyzed, such discussions have been few,[235] sometimes in the context of the prospective tort of cybertrespass.[236]

Arguing through the lens of property law, Professor Bellia argues that contract breach should not provide a basis for criminal CFAA prosecution. She states that "as a matter of statutory interpretation, coverage of unauthorized 'access' should be limited to activities that breach some technical limitation on access."[237] Professor Galbraith similarly argues against contract breach serving as a basis for criminal CFAA prosecution, particularly in the case of intellectual property harms on publicly accessible websites.[238] Meanwhile, Professor Madison presents a thought-provoking analysis, asking whether confusion over metaphors of the internet as place or thing have led us to confusion regarding contract and computer intrusion.[239]

One of the most thorough and recent examinations of the subject of contract, breach, and CFAA criminal computer intrusion is that of Professor Kerr, who similarly notes that a breach of contract should not constitute an act of unauthorized access for purposes of CFAA criminal prosecution.[240] He argues that violations of code-based restrictions and contract-based restrictions usually divide into two relatively easily distinguishable, discrete categories.[241] For Kerr, violations of code-based restrictions and whether the user has tricked the computer are the dispositive inquiries with respect to CFAA criminal analysis. He asserts that "[r]egulation by contract offers a significantly weaker form of regulation than regulation by code. Regulation

> eliminated, a plaintiff still needs to show that they suffered damage or loss.

Computer Fraud and Abuse Act (CFAA), INTERNET LAW TREATISE, https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA) (last visited Mar. 14, 2013).

235. *See* Bellia, *supra* note 219.

236. Peter Winn has also argued in favor of revitalizing cybertrespass and crafting a standard triggered by reasonableness of conduct. *See* Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1428 (2007).

237. Bellia, *supra* note 219, at 2262. Professor Bellia's approach successfully conceptually addresses many of the CFAA questions raised in my argument above, albeit through a more property-focused lens. One area where this property-based approach as well as Professor Kerr's approach arguably fall short is addressing hybrid contract-code restrictions on access such as CAPTCHAs, which seem to be increasing in use. The privity approach presented in this Article is capable of addressing hybrid code-contract scenarios more effectively.

238. Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 324 (2004).

239. Michael J. Madison, *The Narratives of Cyberspace Law (Or, Learning from Casablanca)*, 27 COLUM. J.L. & ARTS 249 (2004).

240. Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1600 (2003).

241. *Id.*

by code enforces limits on privileges by actually blocking the user from performing the proscribed act, at least absent circumvention."[242] Professor Kerr's analysis is clearly appropriate for the first category of intruder; strictly third-party criminal context of accessing a "protected computer" where no contractual relationship of any kind is formed.[243]

However, Kerr's approach is somewhat less satisfying in current commercial contexts. Many commercial contexts today present a blended set of code-based and contract-based restrictions: for example, CAPTCHAs or human interactive proofs provide a case of a hybrid code-based and contract-based restriction.[244] Is employing a bot that acts like a human to solve CAPTCHAs a violation of a code-based restriction for Kerr? Is circumventing an (easily-avoided) end user license agreement text copy-protection measures also an act of computer intrusion? If a consumer accesses content on the *New York Times* website and avoids a technical restriction in a manner requiring no technical skill—perhaps his cat stands on the delete key and deletes the last piece of an article's URL[245]—is he properly classified a "hacker" for CFAA purposes, despite already being bound by the *New York Times* terms of use contract?[246] The dynamics of code and contract are becoming increasingly interwoven, and the definition of a "code-based"

242. *Id.*

243. 18 U.S.C. §1030(a)(2)(A)–(C) (2011). A "protected computer" is one that is exclusively for the use of the U.S. government or a financial institution, or if not exclusively for such use, when a computer is used by or for the U.S. government or a financial institution and the conduct constituting the offense affects that use; or is used in interstate or foreign commerce or communication. *Id.* §1030(e)(2). A person who obtains anything of value by accessing a protected computer, knowingly, without authorization and with the intent to defraud, violates the CFAA unless (a) the only thing of value that is obtained is the use of the computer itself, and (b) the use is valued at less than $5,000 during a one-year period. *Id.* §1030(a)(4).

244. A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a code-based test to determine whether a particular user is a human or code, such as a bot. CAPTCHAs usually accompany a requirement that the user agree to terms of use of a website. For a discussion of CAPTCHAs, see *Telling Humans and Computers Apart Automatically*, GOOGLE, http://www.google.com/recaptcha/captcha (last visited Nov. 18, 2012).

245. *See, e.g.*, Lauren Indvik, *How to hack the New York Times Paywall… With Your Delete Key*, MASHABLE, (Mar. 28, 2012), http://mashable.com/2011/03/28/how-to-bypass-new-york-times-paywall/ (describing how merely deleting the last portion of the New York Times URL would break the website's copy protection on articles at the time of this author's writing).

246. I submit that none of these qualify as triggering the CFAA. Each of these acts can be analyzed to have occurred within the context of a contractual relationship. As such, the privity model deems CFAA analysis inappropriate.

restriction has become an increasingly slippery slope. As the discussion of the four types of contract "hackers" demonstrates, gray areas abound.

I strongly agree in principle with Professor Kerr, Professor Bellia, and Professor Galbraith's conclusion that a breach of contract does not provide the basis for a criminal CFAA prosecution (or any other technology exceptionalist prosecution for that matter), but I submit that this question should be framed differently. The mere existence of an enforceable contract between the parties that covers the information at issue is dispositive. The existence of this contract trumps the applicability of the CFAA. Therefore, framing a contract inquiry with the CFAA as a starting point is overly deferential to the CFAA: this is the law of the zebra. Further, this framing captures only half of the problematic cases: I submit that a breach of contract also does not provide the basis for any civil CFAA action for the same reason as it does not support criminal actions. Contract law and other already existing legal regimes can continue to effectively address the types of harms implicated by the four "contract hackers" described in Section III.A, *supra*.

In the privity model that follows, I fundamentally invert Kerr's argument. Contract should be considered a superior and stronger form of regulation to that of code and technology exceptionalist approaches such as the CFAA: CFAA analysis is only appropriate provided there is no contract analysis possible. While the behaviors of code can cast doubt on the meaning of a contract term, as I describe in the next Part, if a contract has been validly formed, contractual agreements hold a superior position to CFAA analysis. They override the need for it, both civilly and criminally.

The privity model that follows thus takes into account hybrid contract-code restrictions. I argue that as a matter of contract law, when ambiguities arise in technology breach contexts and both contract and code breaches may exist, a contract-based analysis must control and ambiguities must be construed against the drafter of the contract at issue. In other words, I am arguing for the blanket supremacy of contract law over computer intrusion analysis where a contract between the parties giving access to the information in question was properly formed. Any other analysis results in an exceptionalized and undesirable construction of contract breach in technology contexts that threatens the future of contract law.[247] This "privity" model is explained below.

247. Additionally, breach weaponized with the CFAA presents the constitutional void-for-vagueness concerns that Professor Kerr addresses elsewhere. *See* Kerr, *supra* note 109, at 1562.

A. THE "PRIVITY" MODEL: CONTRACT TERMS AND NORMS OF ACCESS

In this Part, I propose a "privity"[248] model of understanding the relationship of contract and the CFAA. This privity model provides an operationalization of the paradigm of restrained technology exceptionalism introduced in Part II, *supra*. Embodying these principles, the privity model avoids the pitfalls of a weaponized breach analysis. It expressly divorces contract law analysis from CFAA analysis and frames contract as the superior regime. It does not, however, eliminate any other remedies that already exist in law apart from the CFAA: if the conduct in question is otherwise criminal or tortious, those penalties remain.

As the name of the model implies, the privity model is an analytical framework that gives supremacy to contract law analysis over CFAA analysis. As courts have recognized in various contexts, including even with respect to copyright, a contract inquiry is not preempted as an initial matter over other areas of law.[249] But for very limited circumstances,[250] contract law controls when an agreement exists between the parties: as *ProCD, Inc. v. Zeidenberg* suggests,[251] where a contract between the parties exists, contract law is usually not preempted.[252]

---

248. Privity refers to the contract law concept of the existence of a bilateral contractual relationship that gives the parties certain rights with respect to each other. For a discussion of privity, see, e.g., J.W. Neyers, *Explaining the Principled Exception to Privity of Contract*, 52 MCGILL L.J. 757, 760–63 (2007). Much like the concept of privity, the model focuses on the existence of a contractual relationship as the focal point of analysis.

249. *See generally* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1454–55 (7th Cir. 1996).

250. In *Rano v. Sipa Press, Inc.*, the Ninth Circuit held that copyright preempted state law relating to the termination at will of a license with an indefinite duration because "California law and federal law are in direct conflict, federal law must control." Rano v. Sipa Press, Inc., 987 F.2d 580, 585 (9th Cir. 1993). Assignability of a licensee's rights would provide another preemption basis because under federal law such rights cannot be assigned in a nonexclusive license without the consent of the licensor. *See In re* CFLC, Inc., 89 F.3d 673 (9th Cir. 1996); *cf.* Chamberlain v. Cocola Assocs., 958 F.2d 282 (9th Cir. 1992) (applying California statute regarding transfer of tangible object in case of transfer of intangible rights to use object).

251. *ProCD, Inc. v. Zeidenberg* was the first appellate ruling dealing with the enforceability of shrinkwrap licenses and that the contract restrictions it placed on the use of a noncopyrightable database were not preempted by copyright law. *ProCD*, 86 F.3d at 1454–55; *see also* Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005) (holding that license not preempted by fair use); Altera Corp. v. Clear Logic, Inc., 424 F.3d 1079, 1080 (9th Cir. 2005) (copyright does not preempt contract enforcement, citing *Zeidenberg*); DaimlerChrysler Servs. N. Am., LLC v. Summit Nat., Inc., 144 Fed. App'x. 542, 545 (6th Cir. 2005) (holding that copyright defenses irrelevant to contract enforcement); Bowers v. Baystate Techs., Inc., 320 F.3d 1317, 1325 (Fed. Cir. 2003) (holding that license not preempted by fair use).

252. *See* Guy A. Rub, *Winter, 2011 Symposium: the Licensing of Intellectual Property: Contracting Around Copyright: The Uneasy Case For Unbundling Of Rights In Creative Works*, 78 U. CHI. L. REV. 257, 257 (2011).

By framing the analysis from a contract law perspective, the privity model limits the reach of the CFAA and enables it to act as the basis for tort-like and equitable remedies (and criminal prosecution) only in cases of truly novel "hacking"[253] harms that happen outside the realm of privately ordered contractual relationships. In other words, the privity model converts the CFAA from being an instrumentality of the law of the zebra into a law of the horse approach—an approach limited to those circumstances where legal gaps cannot be successfully filled by traditional law.

1. The Privity Model

A privity model of contract breach and CFAA analysis can be summed up in one sentence: In the case where a contract was properly formed between the parties and a breach occurs, the use of a computer in connection with the breach is irrelevant. The CFAA is not implicated.

As demonstrated by Figure 1, *infra*, the privity model arises from a simple distinction in contract law: that breach can only arise when a contract has been properly formed.[254] As such, a privity model starts with a formation inquiry: has an oral or written contract been formed between the parties? Are the parties in privity with each other? Courts should define this act of contract formation broadly. Just as contracts can be formed in both oral and written form in physical space contexts, so too the mere extension of technology credentials, such as logins and passwords that allow access to a portion of a network, constitutes the formation of at least an oral agreement granting access to the extent of the credentials' authorization inside the system.

If the terms expressly give access to the allegedly violated information resource, the matter is a regular contract breach. Traditional contract breach analysis applies, and no claim under the CFAA is appropriate. If the terms ambiguously discuss access to the information, the contract is construed against the drafter, and a contract law claim for breach with traditional remedies is the appropriate recourse. No CFAA claim is appropriate.

253. I use the word hacking here colloquially. A "hacker" in the mind of an average consumer, as reflected by media depictions, refers to someone who possesses specialized computer skills and uses them to circumvent code-based restrictions on access to networks. Reasonable people will differ about the desirability and criminality of certain types of *Bowers v. Baystate Techs* "hacking" conduct, such as white hat hacking of a database to determine the existence of a dangerous vulnerability in the code. That question is beyond the scope of this Article.

254. *See* Fontanella v. Marcucci, 877 A.2d 828, 834–35 (Conn. App. Ct. 2005) ("To recover for breach of contract, the plaintiffs must establish the formation of an agreement, performance by one party, breach of the agreement by the other party, and damages.").

Construing any vagueness against the drafter is an analysis consistent with a traditional contract law approach. It is also the more equitable position: the drafter is in a better position to choose the desired scope of access with respect to information security default settings, both contractually and in practice. Similarly, the drafter is in the superior position to terminate the rights of access in both of these granting vehicles.[255]

If the access that permitted the alleged information theft was not expressly contemplated in the contract, however, the information security access settings of the network, profile, or information at issue are incorporated as implied terms of the contract. The contract is then construed against the drafter, and a traditional breach analysis is appropriate. CFAA remedies are again inapposite. An aggressive damages calculation for information harms can be constructed through coupling expectation damages with an injunction and disgorgement damages for extreme cases. This type of an aggressive damages regime would enable traditional contract remedies to sufficiently compensate damages plaintiffs for information harms in the vast majority, if not all, information theft instances arising out of a contractual relationship.

If, however, the access that occurred was permitted neither by the express language of the contract nor by the information security settings of the information owner at the time, then the particular act may fall outside the scope of the contractual relationship. In such case, a CFAA claim may be appropriate. However, in this case, the CFAA claim arises *as an independent claim that is unrelated to the contract. The basis for a CFAA claim does not arise out of the contract breach.* Even in a situation where a contractual relationship existed and was terminated, a CFAA claim is appropriate only if termination was done correctly. Access terminates through a notification of termination of the agreement itself in accordance with the terms stipulated in the agreement and, simultaneously, the reality of access must be terminated using information security controls. A failure to either provide notice or to terminate access in fact can be rightfully construed as a failure to terminate by the drafter and construed against him. If termination of access was incomplete or incorrect, no CFAA claim is appropriate—the existing contract was still in effect and a breach claim is appropriate.

The privity model in this way encompasses a greater scope of activities and recourse than Professor Kerr's model, which focuses only on code-based

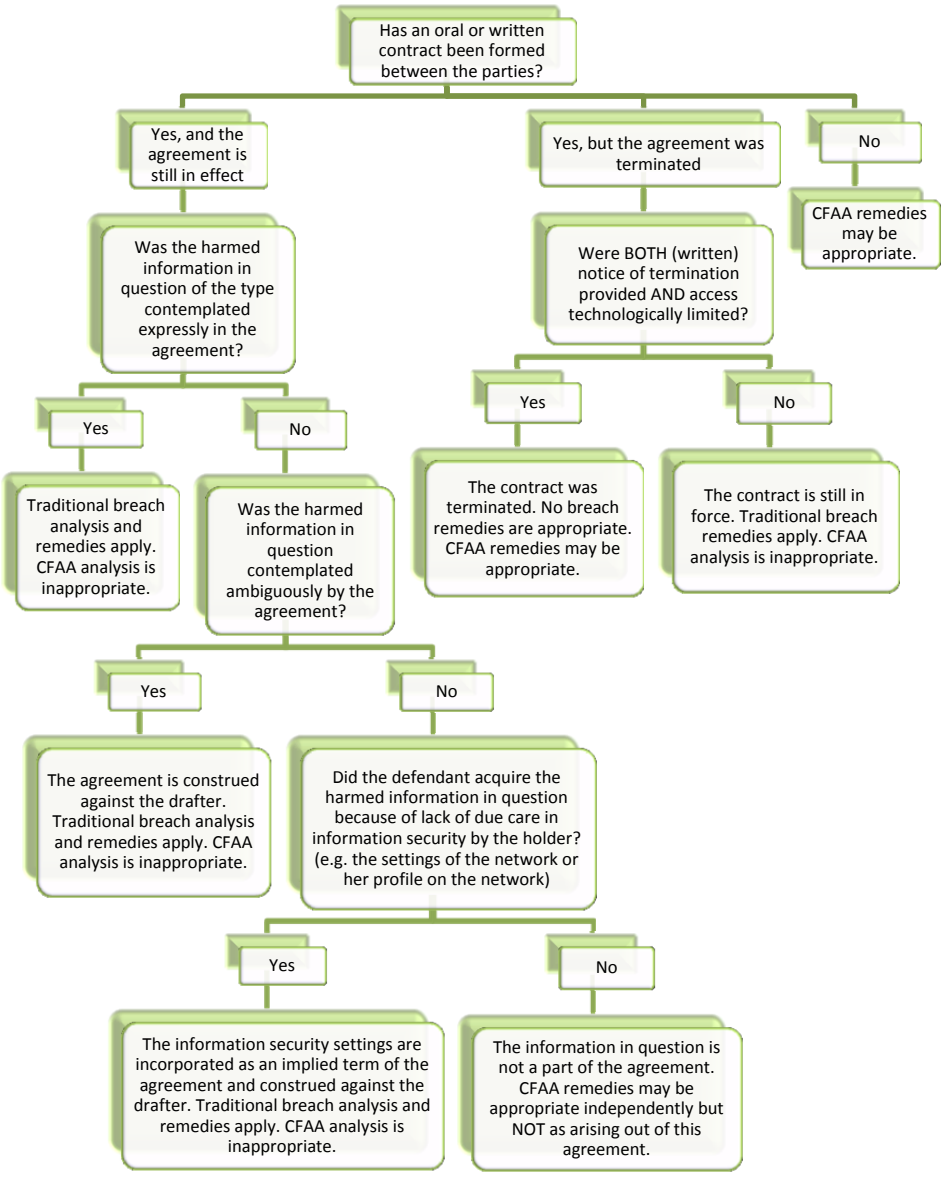
255. *See, e.g.*, David Horton, *Flipping the Script: Contra Proferentem and Standard Form Contracts*, 80 U. COLO. L. REV. 431 (2009) (discussing the contract law rule of construction of terms against the drafter).

regulation and criminal CFAA application. The privity model also extends the reach of contract law to address hybrid contract-code situations such as a human interactive proofs, an approach in line with the suggestion made by Professor Bellia regarding the merits of contemplating hybrid law and code notice-based approaches.[256] Most importantly, however, the privity model minimizes the extent to which technology is treated as "special." It also places an affirmative burden of care in information security on the information holder, limiting the holder's ability to weaponize contractual relationships. This approach is consistent with the duty to mitigate damages in contract law, as well as and basic principles of due care in information security. It also ensures that both the civil and criminal penalties of the CFAA are used only in extraordinary circumstances: to address truly novel harms arising out of technology, not as a means of contracting parties inflicting transaction costs on each other.

The privity model will next be applied to each of the four "contract hacker" situations in the following Section, demonstrating its effectiveness at handling the vast majority of the breach questions that arise in a technology contracts.

256. *See* Bellia, *supra* note 219, at 2272–73 (arguing that "the literature has thus far neglected the complex relationship between law and technical measures in this context—in particular, the possibility that too-weak legal protection will induce greater reliance on too-strong technical measures, whether or not the law in fact backs those measures.").

Figure 1: The "Privity" Model of Contract and CFAA Remedies



B. HANDLING THE FOUR "CONTRACT HACKERS"

The privity model offers contract law tools to address the harms caused by each of the four "contract hackers."

1. Users

With respect to Grandma, Dr. Whiskers, and end users in general, it is highly unlikely that any basis for a CFAA claim would exist under the privity

model. For example, if a user clicks on a portion of a site that is improperly coded and finds herself funneled into an interface which should be protected with restricted access, actual access capabilities fall within the scope of use permitted by the end user license agreement/terms of use. The privity model would thus incorporate the reality of this access as an implied term of the user agreement.

Grandma's use of Dr. Whiskers' information rather than her own on the website may indeed be a breach of contract. However, such a breach of contract would likely carry with it a very small remedy in damages, if anything, because actual damages would be difficult to prove on the part of the website owner. As such, the distinction of minor versus material breaches becomes intrinsically important again in contractual relations, and no CFAA civil or criminal claim would exist.

2. Employees and Business Partners

In the context of employee and business partner "contract hackers," the existence of the contractual relationship controls under the privity model if accessed information is misused. As one court correctly analyzed the question of employee "contract hackers," a distinction must be drawn between the existence of a contract that grants authorization to access and the bad use of information in a manner which breaches the contract. In *International Association of Machinists and Aerospace Workers v. Werner-Masuda*, the defendant, a union officer, was charged with exceeding her authorization to use a computer when she violated the terms of a terms-of-use agreement which granted her access to a membership list.[257] The court rejected the application of § 1030 of the CFAA, holding that even if the defendant breached a contract, that breach of a promise did not mean her access to that information was unauthorized or criminal. In the words of the court:

> [Even if] Werner-Masuda may have breached the Registration Agreement by *using* the information obtained for purposes contrary to the policies established by the [union] Constitution, it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of the . . . CFAA . . . the gravamen of [the plaintiff's] complaint is not so much that Werner-Masuda improperly accessed the information . . . but rather what she did with the information once she obtained it. . . . Nor do [the] terms [of the CFAA]

257. Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495–96 (D. Md. 2005).

> proscribe authorized access for unauthorized or illegitimate purposes.[258]

This distinction explained by the court preserves the role of contract breach in technology contracting. When a rogue insider such as an employee or a business partner chooses to inflict commercial harm that includes a technology-based operationalization—meaning involving a computer—this harm comes usually in the form of copied information that is published or shared with a competitor (potentially eviscerating trade secret protection), destruction of information assets inside the company, or using access to the corporate network to inflict technology harms to third parties. In each of these situations, both confidentiality agreements and separate agreements related to the business relationship should exist between the parties. Provided these agreements are well drafted, they will offer the basis for a full recovery for losses. With respect to the first and second scenario of damaged intellectual property assets, in addition to a suit in contract, the harmed party has an additional option to sue the breacher (and any recipient of information) for theft of trade secrets, and any party receiving information for possible tortious interference with contract. In the case of use of the corporate network to inflict technology pain on innocent third parties, breach of contract will cover any actual losses suffered by the company. Meanwhile, the third-party victims of the technology harms retain recourse against the individual under the CFAA—no contract controls that relationship and the parties do not stand in privity. As such, regardless of how technology is used in the course of the breach, a combination of a restitution and a disgorgement calculation of damages in contract, particularly if coupled with a trade secret remedy, can make a harmed party whole in the instance of a "contract hacker" insider.

3. Entrepreneurs

A similar analysis holds when an application developer or data aggregator is sued by an information holder or content owner. With respect to the

258. *Id.* at 499 (citations omitted); *see also* Shamrock Foods v. Gast, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008) (holding the CFAA did not apply when an employee emailed himself files for the benefit of a rival company in violation of the defendant's confidentiality agreement); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (rejecting a CFAA claim against an employee who violated an employment agreement by using his access to his employer's computer system to steal data for a competitor and holding that "a violation for accessing 'without authorization' occurs only where initial access is not permitted," while explaining further that a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted).

"contract hacker" entrepreneurs, the question again turns on whether a contract was formed. If a contract exists between the particular entrepreneur and the information holder who alleges that the entrepreneur has wrongly accessed information, then the privity model applies. If, however, contract formation has not occurred between the entrepreneur and the information owner, then the analysis may indeed implicate the CFAA.

In the case where the entrepreneur is acting through an assignment of access right from a consumer user,[259] the technological reality of the assignability of the credential controls. In other words, the contract rights of the user to access the website can be assigned to the entrepreneur by the consumer user. Although, again, this may be a contract breach on the part of the user and/or the entrepreneur, the access is through a contract right. If the information owner chooses to use technological means to restrict the access of the particular entrepreneur or all such entrepreneurs, this blocking is the prerogative of the information owner. Similarly, the information owner may seek to terminate its agreement with all users relying on the disfavored products.

The privity model also offers guidance in data aggregation cases. The analysis yet again turns on whether a contract was formed. The inquiry may be framed by a court in a manner which analyzes whether the code of the data aggregator behaved in a way consistent with the behaviors that a human user would demonstrate. If the code of the data aggregator behaved in a humanlike way—simply stepping into the shoes of an authorized human user—and a contract was indeed formed between the data aggregator and the information holder, then a contract law analysis applies. If no contract was formed or if the contractual relationship was appropriately terminated, then CFAA analysis may be appropriate.

It is in these cases where the potency of the remedy of an injunction in contract becomes apparent. Let us presume that the data aggregator, posing as a human user, formed an agreement with a ticketing website, and it sends queries in a manner that are human-like but in exceedingly high volume. The ticketing website may then notify the data aggregator that the access contract between the data aggregator and the website is terminated and that no additional access is appropriate. However, if the ticketing website creates

259. For example, the program Vtok is an application that facilitates communication through Google talk, text, and video on iPhones. Because no official Google chat application is available on iPhone, users rely on third-party applications such as Vtok to access their accounts. In order to access a user's Google account, Vtok requires the user's login credentials. The access has been expressly authorized by the user, but the user's access is intermediated by Vtok. *See* VTOK, http://www.vtokapp.com (last visited Mar. 15, 2013).

agreements with its users through the standard method of a terms of service contract on the homepage, i.e. forming a contract with anyone who cares to visit the website, each time the data aggregator revisits that homepage, a new contract is formed and access is again granted. Hence, if the ticketing website wishes to prevent the data aggregator from accessing the site and entering into additional contracts with the site, seeking injunctive relief from a court may be the appropriate remedy. A breach of contract, however, should not provide a basis for a CFAA claim simply because the ticketing website is technologically incapable of preventing the data aggregator from posing as a human and accessing the site.

4. Security Researchers

With respect to information security researchers, provided that an agreement has been formed through an end user license agreement, any acts of reverse engineering, decompiling, and any other analysis, even if these acts constitute a breach of the terms of the agreement, would not provide any basis for a CFAA civil suit or criminal prosecution. Although the security researcher may still be open to claims under the Digital Millennium Copyright Act and other intellectual property regimes, those are outside the scope of the privity model. Notably, none of these four contract hacker scenarios impacts the use of the CFAA in its traditional sphere of application–criminally prosecuting third party unaffiliated hackers who do not sit in contractual privity with an information holder or content owner.

C. CRAFTING GOOD NORMS IN INFORMATION SECURITY

Because the privity model provides an operationalization of restrained technology exceptionalism, it creates a line between contract law and other areas of law that has been sometimes blurred in recent case law. It avoids the list of deleterious consequences to contract law that were set forth in Part II and it resolves the fact-specific problems of the four contract hackers introduced in that Part. Further, the privity model allows for other areas of law to develop in this space around information regulation.

In particular, because the privity model incorporates the realities of information security control and construes them as an implied term of the contract, it creates a strong incentive for good information security behaviors on the part of information holders. As I have argued elsewhere, the incentives for good information security behaviors are not always apparent to information holders.[260] As rampant information security breaches

260. Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation*, 3 BERKELEY BUS. L.J. 129 n.174 (2005).

demonstrate, information management success and information security practices vary dramatically across entities, and widespread deficits exist.[261] One of the most basic principles of information security is the principle of least privilege–the idea that access to information should be granted in as stingy a manner as possible, with the fewest people possible having unfettered access and with others having the least amount of access necessary to fulfill responsibilities.[262] The privity model embodies this idea of least privilege and blends the technological and contractual access limitations. This approach is aligned with the spirit of the CFAA, which, as Professor Bellia notes, is a statute that "does in fact strike a balance that heavily favors technical measures as a predicate for legal protection."[263]

By creating rights of recourse for information holders that are contingent on exercise of care in their information handling, both the information holders and the rest of the information ecosystem benefit. I have explained elsewhere that neglecting security of key information assets can contribute to meaningful devaluation of corporate assets, a devaluation that potentially can be construed as a breach of fiduciary duty.[264] Further, the underlying approach of strong information security practices is fundamentally consistent with the duty to mitigate damages that already exists in contract law.[265] Even if a party is blameless in a breach, that party nevertheless has a duty in contract law to mitigate the damages resulting from that breach.[266] When an information holder chooses to exercise poor information control practices, the information holder runs afoul of the spirit of this duty to mitigate the damages arising from a breach. Similarly, trade secret law relies on the holder of the allegedly secret information to maintain reasonable precautions of secrecy.[267] As such, the privity model penalizes lack of due care in information handling by the information holder in a manner consistent with both contract and trade secret law.

261. *See, e.g.*, DATALOSS DB, http://www.datalossdb.org (last visited Feb. 18, 2012) (listing information security breaches); PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org (last visited Feb. 18, 2012) (same).

262. *See* DEPARTMENT OF DEFENSE, TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA 109 (1985), *available at* http://csrc.nist.gov/publications/history/dod85.pdf.

263. Bellia, *supra* note 219, at 2271.

264. Matwyshyn, *Imagining the Intangible*, *supra* note 210, at 990.

265. *See* RESTATEMENT (SECOND) OF CONTRACTS § 350 (1981).

266. *Id.*

267. Unif. Trade Secrets Act, 14 U.L.A. 433 (1990).

V. CONCLUSION

This Article warns of the "law of the zebra," an inherently disruptive paradigm seeping into contract law that prioritizes technology driven analysis over traditional contract law. In place of the law of the zebra, this Article argues in favor or restoring contract law to its traditional trajectory. It seeks to craft a minimally disruptive, predictable approach to analyzing contract law questions in technology contexts by offering the paradigm of "restrained technology exceptionalism"—a paradigm based on traditional contract law principles. In particular, through one operationalization of this paradigm in a "privity model," this Article offers a suggested roadmap for judicial interpretation of the CFAA contract hacker cases that are currently causing a circuit split in the federal courts.