VIRGINIA JOURNAL OF LAW & TECHNOLOGY

WINTER 2013 UNIVERSITY OF VIRGINIA VOL. 17, NO. 04

A New Proposal for the Department of Justice's Interpretation of the Computer Fraud & Abuse Act

Note

NATCH GREYES[†]

[†] J.D. Candidate 2013, William & Mary School of Law. Mr. Greyes can be reached at NGreyes@email.wm.edu.

ABSTRACT

This Note looks at one narrow, yet important piece of legislation, the Computer Fraud and Abuse Act (CFAA) and how the Department of Justice (DOJ) has interpreted the CFAA, from its inception in *United States v. Drew* to its attempt for legislative adoption of its interpretation by Congress. That interpretation varies from the traditional interpretation of the CFAA, something this Note highlights, and has been given a hostile reception by the courts, especially in *United States v. Nosal*. Nevertheless, the DOJ's interpretation is persuasive and its implications are examined in this Note. These implications are contrasted with a historical analogy, the No Electronic Theft (NET) Act, and a new solution is proposed, one that both achieves the DOJ's goals and protects the rights of those who use the internet, by expanding negligent manslaughter to punish conduct like Lori Drew's and the creation of a new statute to punish conduct like David Nosal's.

TABLE OF CONTENTS

I. Introduction 296

II. CFAA: The DOJ's Proposal 297
- A. The Move to Criminalize Formerly Private Contracts 298
- B. The Starting Point: *United States v. Drew* 302
- C. The Legislative Attempt for Redefinition 306
- D. The Judicial Attempt for Redefinition: *United States v. Nosal* 309

III. The Duty to Read 315
- A. Clickwrap 321
- B. Browsewrap 322
- C. Recent Developments in Enforceability: The Law of Software Contracts 325

IV. The Current CFAA Prosecutions: We've Been Here Before 327
- A. The Problem: United States v. LaMacchia 328
- B. The Solution: The NET Act 330

V. A Proposed Solution 336
- A. Subsuming the Private Contract Law 337
- B. The Empirical Problem with Subsuming the Private Contract Law 339
- C. The Proposed Solution 343
  - 1. Punishing Lori Drew's Conduct 344
  - 2. Punishing David Nosal's Conduct 347
  - 3. A Better Solution? 349

VI. Conclusion 352

I. INTRODUCTION

Imagine that you visit the main page of Australian humorist David Thorne's website, 27b/6.[1] In the top left corner you see a column titled "Disclaimer," in bold typeface.[2] You do not read down this column, but if you did you would encounter the following sentence: "You are not granted permission to access the information on this site, and if you choose to do so by viewing any of the articles either through this page or from an external link, you agree to waive all rights."[3] Now, imagine that you view one of the articles through the home page. The next day the Federal Bureau of Investigation comes to your house, arrests you, and charges you with violating the Computer Fraud and Abuse Act (CFAA) by "intentionally accessing a computer without authorization or exceeding authorized access," thereby obtaining "information from a protected computer."[4] Sound farfetched? The Department of Justice (DOJ) does not think so.[5]

---

[1] For the purposes of this example, assume that the United States has jurisdiction over Thorne's website. *See* Paul Lilly, *U.S. Claims Jurisdiction Over All .com and .net Domains*, MAXIMUMPC (July 5, 2011, 8:38 AM), http://www.maximumpc.com/article/news/us_claims_jurisdiction_over_all_com_and_net_domains (noting U.S. Immigration and Customs Enforcement (ICE) argues that it has jurisdiction over all .com websites because they are routed through VeriSign, a service based in Virginia).

[2] David Thorne, 27B/6, http://www.27bslash6.com/ (last visited Feb. 20, 2012).

[3] *Id.*

[4] Consumer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030(a)(2)(c) (2008).

[5] *See Cybersecurity: Protecting America's New Frontier: Hearing Before the House Judiciary Subcomm. on Crime, Terrorism and Homeland Security*, 112th Cong. (2011) [hereinafter *Cyber Security Hearings*] (statement of Richard Downing, Deputy Section Chief), *available at*

Part II of this Note will examine the evolution of the DOJ's interpretation of the CFAA, from its inception in *United States v. Drew*[6] to its attempt for legislative adoption of its interpretation by Congress and, in the alternative, a court-based adoption of its interpretation in *United States v. Nosal*.[7] Part III will examine the elements of the private contract law that the DOJ's proposed interpretation could subsume into the criminal law. Part IV will look at a historical analogy, the No Electronic Theft (NET) Act, to support the proposition that the solution proposed in Part V would be more effective than the one the DOJ is currently pursuing. Finally, Part V will argue that there exists a better solution for enabling the prosecution of the kind of conduct the DOJ wishes to prosecute than the solution that has been proposed by the DOJ, namely, one that focuses on the expansion of negligent manslaughter to punish conduct like Lori Drew's and the creation of a new statute to punish conduct like David Nosal's.

II. CFAA: THE DOJ'S PROPOSAL

The DOJ's interpretation of "exceeds authorized access," as used in the CFAA, differs from the interpretation of that phrase by Congress[8] and the courts.[9] In the DOJ's view, the phrase "exceeds authorized access" allows the government to prosecute any individual who violates any provision of any

http://www.justice.gov/criminal/pr/speeches/2011/crm-speech-1111151.html.

[6] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

[7] Oral Argument, United States v. Nosal, 676 F.3d 854 (No. 10-10038), *available at* http://www.youtube.com/watch?v=c8F93nzDqP0.

[8] Personal Data Privacy and Security Act, S. 1151, 112th Cong. (2011) (amended 2011).

[9] *See, e.g.*, *Drew*, 259 F.R.D. at 461.

website's terms of service.[10] This proposal first took shape during the prosecution of Lori Drew, the woman who impersonated a teenage boy on MySpace, a social network website, in order to taunt a teenage girl who later committed suicide.[11] After the district court dismissed the misdemeanor conviction of Lori Drew, the DOJ began to pursue its current two-prong strategy for a favorable definition of "exceeds authorized access."[12] The first prong of this strategy consists of a legislative attempt to redefine the term "exceeds authorized access," a term with a fairly extensive legislative history, while the second prong consists of a judicial attempt to redefine that term.[13]

A. The Move to Criminalize Formerly Private Contracts

Originally, passage of the CFAA was motivated by the 1983 movie *War Games*, in which a young American "hacker" unwittingly accesses the supercomputer that controls the nuclear arsenal of the United States.[14] The CFAA was originally designed to allow the DOJ to prosecute computer

[10] *See Cyber Security Hearings*, *supra* note 5 (statement of Richard Downing).
[11] Christopher Maag, *A Hoax Turned Fatal Draws Anger but No Charges*, N.Y. TIMES (Nov. 28, 2007), http://www.nytimes.com/2007/11/28/us/28hoax.html.
[12] *See infra* Part II.C & Part II.D.
[13] *See* Greg Pollaro, *Disloyal Computer Use and the Computer Fraud & Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12, paras. 4–7 (2010).
[14] *Id.* at para. 4. *See also* H.R. REP. NO. 98-894, at 10 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3696 ("The motion picture 'War Games' showed a realistic representation of the automatic dialing and access capabilities of the personal computer.").

"hackers," like the protagonist in *War Games*.[15] It also allowed the prosecution of those individuals who used a computer to obtain "classified information," "financial or credit records," or to interfere with the government's use of a computer.[16]

In 1986, Congress overhauled the CFAA, after recognizing that the statute, as originally written, was ambiguous and far reaching.[17] In that revision, Congress limited federal prosecutions to instances in which the affected computers were owned by the federal government or "certain financial institutions" or "where the crime itself is interstate in nature."[18] This limited prosecutions based on intrastate hacking.[19] Congress also substituted the phrase "exceeds authorized access" for "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" in an attempt to simplify the language of the statute.[20] This change was aimed at eliminating a confusing area of the statute, one which allowed the prosecution of a federal employee in some

---

[15] H.R. REP. NO. 98-894, at 10, 21.

[16] Pollaro, *supra* note 13, at para. 5 (Specifically, the original formulation proscribed: "[1] knowingly accessing a computer without authorization or exceeding authorization to obtain classified information with intent or belief that such information would be used to harm the United States; [2] knowingly accessing a computer without authorization or exceeding authorization to obtain financial or credit records from a financial institution; and [3] knowingly accessing a computer used by or on behalf of the United States if such access interferes with the government's use of the computer.").

[17] *Id.* at para. 7.

[18] S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.

[19] *See id.*

[20] *Id.* at 9.

circumstances, but not others.[21] By changing the statute, Congress hoped to clarify when a federal employee might be subject to criminal prosecution.[22]

Under the DOJ's current interpretation of "exceeds authorized access" as used in the CFAA, the government would be able to prosecute individuals who violate contractual agreements with employers or providers of services, something that seems at odds with Congress's original intent.[23] In the DOJ's view, the CFAA allows it to prosecute a computer user who violates "the access rules put in place by the computer owner," hence, exceeding authorized access, and, in the course of that access, "commits fraud or obtains information."[24] This view has led courts[25] and commentators[26] alike to charge that

---

[21] *Id.* at 21 (noting that even Congress was unsure about when the statute allowed a federal employee to be prosecuted).

[22] *Id.* ("This remove[d] from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee'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."); *see also* United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012) (implying the change clarified that "without authorization" applies "to outside hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' [applies] to inside hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)").

[23] *Compare* S. REP. NO. 99-432 at 21, *with Cyber Security Hearings*, *supra* note 5 (statement of Richard Downing).

[24] *Cyber Security Hearings*, *supra* note 5 (statement of Richard Downing).

[25] *See, e.g.*, Oral Argument, *supra* note 7, at 4:42, 14:40, 16:40.

[26] *See, e.g.*, Stewart Baker, *Poisoning the Hamburger Helper*, VOLOKH CONSPIRACY (Sept. 11, 2011, 4:49 PM), http://volokh.com/2011/09/11/poisoning-the-hamburger-helper/; *see also* Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Defendants at 6–8, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)

such a broad view allows the DOJ to prosecute individuals who do nothing more than merely violate a website's terms of service.[27] To date, the DOJ has not disagreed with that assessment, saying only that it does not "have [the] time or resources to do that."[28]

It is, perhaps, unsurprising that Congress's[29] and courts'[30] understanding of "exceeds authorized access" is very different from the DOJ's recent interpretation of that phrase. In fact, Senators Franken (D-Minn.) and Grassley (R-Iowa) recently proposed an amendment to the CFAA to clarify that the term "exceeds authorized access" has a much narrower definition than the DOJ urges.[31] According to Senators Franken and Grassley, the phrase "exceeds authorized access" does not include a violation of a contract with an internet[32] service provider, website, or non-government employer, if that

(No. CR-08-0582-GW), *available at* https://www.eff.org/files/filenode/US_v_Drew/Drew_Amicus.pdf.

[27] *Cyber Security Hearings*, *supra* note 5 (statement of Richard Downing); *see also* Nosal, 676 F.3d at 862 ("The difference between puffery and prosecution may depend on whether you happen to be someone an [Assistant U.S. Attorney] has reason to go after.").

[28] Declan McCullagh, *DOJ: Lying on Match.com Needs to Be a Crime*, CNET (Nov. 18, 2011, 8:00 PM), http://news.cnet.com/8301-31921_3-57324779-281/doj-lying-on-match.com-needs-to-be-a-crime/.

[29] S. REP. No. 112-91 (2011).

[30] *See, e.g.*, *Drew*, 259 F.R.D. at 456.

[31] *See* S. REP. No. 112-19.

[32] This Note will follow *Wired*'s increasingly adopted convention of not capitalizing the word "internet." *See* Tony Long, *It's Just the 'internet' Now*, WIRED (Aug. 16, 2004), http://www.wired.com/culture/lifestyle/news/2004/08/64596.

violation is the only basis for believing that access was unauthorized.[33]

The interpretation of Senators Franken and Grassley builds off a broad concern about prosecutions being based on violations of terms of service.[34] This concern was first voiced by Judge Wu in his widely circulated opinion in *United States v. Drew*, which halted the DOJ's first major effort to prosecute individuals who violated websites' terms of service.[35]

B. The Starting Point: *United States v. Drew*

In *Drew*, the defendant, Lori Drew, was charged, among other things, with violating CFAA subsection (a)(2)(C), which prohibits intentionally accessing a computer without authorization or exceeding authorized access and obtaining "information from any protected computer."[36] The indictment alleged that Drew entered into a conspiracy to use an internet connected computer to obtain information without authorization or in excess of authorization in order to facilitate an intentional infliction of emotional distress against Drew's

[33] S. REP. No. 112-19 ("[E]xceeds authorized access . . . does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an [i]nternet service provider, [i]nternet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized.").
[34] Joshua Gruenspecht, *Bill Tweaked in Senate: Terms of Service No Longer Terms of Felony*, CENTER FOR DEMOCRACY & TECH. (Sept. 16, 2011), https://www.cdt.org/blogs/joshua-gruenspecht/169senate-tweaks-bill-terms-service-no-longer-terms-felony.
[35] *Drew*, 259 F.R.D. at 452.
[36] *Id.*

daughter's classmate, Megan Meier, a thirteen-year-old girl.[37] Specifically, Drew was alleged to have created the fictitious persona "Josh Evans" on MySpace.com ("MySpace") as part of a plan to contact and flirt with Megan.[38] Later, Megan killed herself, allegedly as a result of Drew's prompting.[39] While the creation of the "Josh Evans" persona was certainly a violation of MySpace's terms of service, there was some debate at the trial level about whether this violation also constituted a felony violation of CFAA subsection (a)(2)(C).[40] Ultimately, the jury found that, although Drew had not committed a felony violation of CFAA subsection (a)(2)(C), she had committed a lesser-included misdemeanor violation of that subsection.[41] After the jury rendered its verdict, Drew challenged the jury's determination that her violations of MySpace's terms of service could be a misdemeanor violation of CFAA subsection (a)(2)(C).[42]

Ultimately, the district court found for Drew.[43] Its decision largely rested on a contractual analysis, beginning with an enumeration of the elements of the alleged crime Drew committed: (1) the intentional accessing without authorization or exceeding authorized access of a computer; (2) involving interstate or foreign communication; and (3) the obtaining of information from a computer used in interstate or foreign commerce by accessing without authorization or exceeding

[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.* at 453.
[42] *Id.* at 451.
[43] *Id.* at 467.

authorized access.[44] The lynchpin of the ensuing analysis was the meaning of the word "access."[45] According to the court, a broad reading of "access" would allow the prosecution to claim that any breach of terms claiming to outline the permissible use of a system constituted unauthorized access of that system.[46] In other words, a broad reading would allow prosecution for any breach of a website's terms of service.[47] In contrast, a narrow reading would only allow the prosecution to file charges for a breach if that breach was a violation of a restriction prescribed by the United States Code.[48]

After examining analogous cases, the district court determined that most courts have determined that an intentional violation of a website's terms of service will be unauthorized and/or exceeding authorized access.[49] Other courts have held that, like other contracts, terms of service can define the limits of authorized access to a website and its affiliated computers and servers.[50] After adopting the majority position and determining that Drew could be liable for civil damages, the district court's analysis shifted towards the issue of notice.[51]

---

[44] *Id.* at 457.
[45] *See id.* at 457–67.
[46] *Id.* at 459 (quoting Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2253–54 (2004)) (noting that a broad reading of "access" would allow prosecution for any "breach of policies or contractual terms purporting to outline permissible uses of a system [to] constitute unauthorized access to the system.").
[47] *See id.* (citing Bellia, *supra* note 46, at 2253–54).
[48] *Id.* at 459–60 (quoting Bellia, *supra* note 46, at 2253–54) (noting that a narrow reading of "access" would only allow prosecution for a "breach of a code-based restriction.").
[49] *Id.* at 460.
[50] *Id.* at 464.
[51] *Id.*

The notice question the district court had to resolve was "whether individuals of 'common intelligence' [would be] on notice that a breach of a [website's] terms of service . . . can become a crime under the CFAA."[52]

The district court determined that because breaches of contract are not normally the subject of criminal prosecution, allowing prosecution under the CFAA would create a certain level of "indefiniteness" because any criminal prosecution under the CFAA would require the application of contract law.[53] The application of contract law would be required because "terms of service are essentially a contractual means for setting the scope of authorized access,"[54] and it is not entirely clear how contract law procedures and remedies could effectively mesh with criminal law procedures and remedies.[55] The district court wondered what, for instance, should be done with the arbitration clause.[56] Under contract law, the express terms of the contract govern and, so, Drew would theoretically have the right to demand that an arbitrator determine whether

[52] *Id.*

[53] *Id.* at 465 ("[B]ecause terms of service are essentially a contractual means for setting the scope of authorized access, a level of indefiniteness arises from the necessary application of contract law in general and/or other contractual requirements within the applicable terms of service to any criminal prosecution.").

[54] *Id.* at 465.

[55] *See id.* at 464–66.

[56] *Id.* at 465 ("[T]he [MySpace Terms of Service] ha[ve] a provision wherein "any dispute" between MySpace and a visitor/member/user arising out of the terms of service is subject to arbitration upon the demand of either party. Before a breach of a term of service can be found and/or the effect of that breach upon MySpace's ability to terminate the visitor/member/user's access to the site can be determined, the issue would be subject to arbitration.").

she actually violated the terms of service, something that appears fundamentally inconsistent with the criminal law.[57] And, it would seem that the private contractual remedies afforded by the express terms should be the only ones that could bind Drew.[58] The problems that arose out of the mesh between contract law and the criminal law turned the final analysis into one of vagueness.[59] In finding that CFAA subsection (a)(2)(C) was too vague,[60] the district court laid the foundation for the DOJ's to pursue a two-pronged strategy to define "exceeds authorized access" favorably in either Congress or the courts.[61]

C. The Legislative Attempt for Redefinition

Drew was a setback for the DOJ's broad interpretation of the CFAA. However, in May 2011, the Obama administration gave the DOJ the opportunity to renew its effort to redefine the meaning of "exceeds authorized access." This is because the Obama administration indicated a willingness to support a DOJ-led congressional overhaul of the CFAA.[62] In his September 2011 testimony before Congress about the proposed overhaul, Associate Deputy Attorney General James Baker remarked that the DOJ was interested in being allowed

---

[57] *Id.* at 465 ("Thus, a question arises as to whether a finding of unauthorized access or in excess of authorized access can be made without arbitration.").
[58] *See id.* at 465.
[59] *See id.* at 463–67.
[60] *See id.*
[61] *See* Part II.C & Part II.D.
[62] Mathew J. Schwartz, *Treat Hackers as Organized Criminals, Says Government*, INFORMATIONWEEK (Sept. 9, 2011), http://www.informationweek.com/news/security/government/231601078.

to pursue cases like *Drew*.[63] Although he acknowledged that Senators Franken and Grassley had concerns about the scope of prosecutions involving violations of terms of service, Baker's testimony indicated that the only reason the DOJ decided not to appeal the *Drew* case was because of the district court's strong disagreement with the DOJ's interpretation of the statute, not because of some inherent flaw in the DOJ's proposed interpretation.[64]

The DOJ's effort to attain express congressional approval of statutory definitions compatible with the DOJ's understanding of the CFAA is not a new technique.[65] In 1997, as a result of the DOJ and other organizations' prompting, Representative Goodlatte (R-Va.) spearheaded the effort to overhaul copyright law to allow the DOJ to prosecute individuals "pirating" copyrighted works such as software, music, movie, and eBooks.[66] This law was specifically designed to patch the "*LaMacchia* loophole," that had allowed

---

[63] *See Cybercrime: Updating the Computer Fraud & Abuse Act to Protect Cyberspace & Combat Emerging Threats: Hearing Before the Senate Comm. on the Judiciary*, 112th Cong. 25 (2011) (statement of James A. Baker, Associate Deputy Attorney General), *available at* http://www.judiciary.senate.gov/pdf/11-9-7BakerTestimony.pdf.

[64] *Id.* at 18, 25.

[65] *See, e.g.*, No Electronic Theft (NET) Act, Pub. L. 105-147, 111 Stat. 2678 (1997).

[66] *See Copyright Piracy, and H.R. 2265, the No Electronic Theft (NET) Act: Hearing on H.R. 2265 Before the Subcomm. on Courts & Intellectual Prop.*, 105th Cong. 3–6 (1997) (statement of Hon. Howard Coble (R-N.C. (06), Chairman), *available at* http://commdocs.house.gov/committees/judiciary/hju48724.000/hju487240f.htm; Declan McCullagh, *Perspective: The New Jailbird Jingle*, CNET (Jan. 27, 2003, 4:00 AM), http://news.cnet.com/2010-1071-982121.html.

copyright "pirates" to go unprosecuted,[67] much like the reformation of the CFAA would allow the prosecution of people like Drew. The problem with the DOJ's attempt at obtaining a legislative redefinition of "exceeds authorized access" is that, if recent legislative efforts to curtail online "piracy," such as the Stop Online Piracy Act (SOPA)[68] and PROTECT IP Act (PIPA),[69] are any indication, such an effort will be deeply unpopular and met with widespread protest, something that almost guarantees congressional inaction.[70] The DOJ appears to have recognized this risk and, as a result, placed greater emphasis on its attempt to obtain a judicial

[67] H.R. REP. No. 105-339, at 3 (1997); 143 CONG. REC. S12689 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch, "This bill plugs the 'LaMacchia Loophole' in criminal copyright enforcement."); 143 CONG. REC. S12689, S12691 (daily ed. Nov. 13, 1997) (statement of Sen. Kyl); 143 CONG. REC. H9883, H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte).

[68] H.R. 3261, 112th Cong. (2011), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.3261:.

[69] S. 968, 112th Cong. (2011), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d112:SN00968:.

[70] *See* Jenna Wortham, *Public Outcry Over Antipiracy Bills Began as Grass-Roots Grumbling*, N.Y. TIMES (Jan. 19, 2012), http://www.nytimes.com/2012/01/20/technology/public-outcry-over-antipiracy-bills-began-as-grass-roots-grumbling.html?_r=1&pagewanted=1&ref=technology (noting 115,000 websites voluntarily blacked out all or part of their sites on January 18, 2012 to protest SOPA and more than three million Americans e-mailed Congress to voice their opposition); *see also* David A. Fahrenthold, *SOPA Protests Shut Down Web Sites*, WASH. POST, (Jan. 18, 2012), http://www.washingtonpost.com/politics/sopa-protests-to-shut-down-web-sites/2012/01/17/gIQA4WYl6P_story.html (noting that "[o]ne Republican aide said that 'SOPA' had already become 'a dirty word beyond anything you can imagine,'" on the day before the blackout protest).

reinterpretation of "exceeds authorized access," as demonstrated in *United States v. Nosal*.[71]

D. The Judicial Attempt for Redefinition: *United States v. Nosal*

The DOJ's legislative effort to obtain a redefinition of "exceeds authorized access" goes hand-in-hand with its recent courtroom attempt to obtain a new, court-adopted reinterpretation of "exceeds authorized access."[72] At oral argument in *Nosal*, the DOJ attempted to get the Ninth Circuit en banc to accept an interpretation of "exceeds authorized access" that was very similar to the interpretation it advanced in *Drew*.[73] If the argument in *United States v. Nosal* is viewed in light of Associate Deputy Attorney General James Baker's testimony about the DOJ's position on *Drew*, then it seems that the only reason the DOJ appealed the district court's ruling in *Nosal* was because it felt that the Ninth Circuit would be more sympathetic to its interpretation of "exceeds authorized access" than was the *Drew* court.[74]

David Nosal was charged with numerous violations of CFAA subsection (a)(4), which allows the government to prosecute anyone who knowingly exceeds authorized access or

---

[71] *See* Oral Argument, *supra* note 7, at 4:42, 14:40, 16:40.
[72] *See id.*
[73] *See id.* This interpretation, like the prosecution of Drew, was ultimately rejected by the court. United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (specifically invoking *Drew* as a reason to reject the DOJ's interpretation of the CFAA).
[74] *See Cybercrime: Updating the Computer Fraud & Abuse Act to Protect Cyberspace & Combat Emerging Threats: Before the Senate Committee on the Judiciary*, *supra* note 63, at 18.

who accesses, without authorization, a computer with the intent to defraud and, via that access, obtains anything of value.[75] Nosal had worked as an executive for Korn/Ferry International, an executive search firm, from April 1996 to October 2004.[76] As part of his release agreement, Nosal had agreed not to compete with Korn/Ferry International for a period of one year after termination of his employment.[77] Nosal violated this agreement by orchestrating a conspiracy involving three other Korn/Ferry International employees to start a competing business, using information obtained from Korn/Ferry International's computers shortly after leaving Korn/Ferry International.[78]

The indictment obtained by the DOJ "allege[d] that Nosal's co-conspirators exceeded their authorized access to their employer's computer system in violation of [CFAA subsection] (a)(4) by obtaining information from the computer system for the purpose of defrauding their employer and helping Nosal set up a competing business."[79] Nosal filed a motion in the district court to dismiss the indictment, arguing that the CFAA was aimed at computer "hackers" and not employees who "misappropriate information" or use employer-

[75] United States v. Nosal, 642 F.3d 781, 782 (9th Cir. 2011) (quoting the CFAA) (allowing prosecution of "anyone who 'knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value.'"), *rev'd en banc*, 676 F.3d 854 (9th Cir. 2012).
[76] *Id.*
[77] *Id.*
[78] *Id.* at 783.
[79] *Id.* at 782.

owned information in a way that violates a confidentiality contract.[80]

After the Ninth Circuit Court of Appeals decided *LVRC Holdings LLC v. Brekka*,[81] which involved a civil application of the CFAA in the context of an employer-employee relationship, the district court granted Nosal's motion to dismiss, reasoning that, because Nosal's co-conspirators had permission to access the information they accessed, what they chose to do with that information was irrelevant as far as CFAA subsection (a)(4) was concerned.[82] The DOJ appealed the dismissal to the Ninth Circuit, which agreed to hear the case *en banc* after a divided three-judge panel issued a decision reversing the district court over the strong dissent of Judge Campbell.[83]

At oral argument, the DOJ, represented by Jenny C. Ellickson, argued that Nosal's co-conspirators' conduct and, therefore, Nosal's conduct was "squarely within the definition of 'exceeds authorized access'" as that term is used in CFAA subsection (a)(4).[84] Ellickson supported this argument by arguing that Congress meant "exceeds authorized access" to be an access restriction violation on a computer by obtaining or altering information on a computer without authorization.[85]

---

[80] *Id.* at 783.
[81] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).
[82] *Nosal*, 642 F.3d at 784–85.
[83] United States v. Nosal, 661 F.3d 1180 (9th Cir. 2011); *Nosal*, 642 F.3d at 782, 789.
[84] Oral Argument, *supra* note 7, at 3:42 ("This conduct falls squarely within the definition of 'exceeds authorized access' in 18 U.S.C. § 1030 and also constitutes a core violation of §(a)(4).").
[85] *Id.* at 4:42 ("[W]hat Congress said what 'exceeding authorized access' means is to access a computer with authorization and to use such access to

This, in Ellickson's view, allows the DOJ to prosecute someone when "a partial restriction to access to certain data" is violated.[86] This view seems to cause confusions analogous to those under the original CFAA formulation, which allowed a federal employee to be charged for illegitimate conduct that was largely indistinguishable from legitimate conduct.[87]

Ellickson's argument was not well received by Chief Judge Kozinski or Judge McKeon.[88] Both Judge Kozinski and Judge McKeon were very concerned about the DOJ's interpretation of the phrase "exceeds authorized access" in subsection (a)(4) because the same phrase is used in subsection (a)(2) and, as stated by Judge Kozinski, the meaning of a phrase used in two different places in the same statute should be interpreted as consistent across both usages, so a court construing the meaning of that phrase needs to be cognizant of both usages.[89] As a consequence, Ellickson was faced with

---

obtain or alter information on the computer that the accessor is not entitled so to obtain or alter.").

[86] *Id.* at 5:15 ("[T]his court must recognize that . . . a violation of a partial restriction to access to certain data would fall within the scope of the definition of 'exceeds authorized access.'").

[87] S. REP. NO. 99-432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494–95 ("This remove[d] from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee'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.").

[88] *See, e.g.*, Oral Argument, *supra* note 7, at 5:30, 9:40, 11:45, 16:40.

[89] *Id.* at 9:40; *see also* United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) ("Once we define the phrase for the purpose of subsection 1030(a)(4), that definition must apply equally to the rest of the statute pursuant to the 'standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be

numerous questions about the interpretation of "exceeds authorized access" as it is used in subsection (a)(2).[90]

At oral argument, the court appeared to struggle with the fact that under the DOJ's interpretation of whether an act exceeds authorized access depends on how the restriction to access is drafted.[91] In other words, the court was concerned that the contract Nosal signed or the terms of service to which users ostensibly manifest agreement by either clicking 'I Agree' or simply using the website determines, in the DOJ's view, the extent to which the user may use the service without threat of prosecution.[92] The court's concern with the DOJ's interpretation as it was described by Ellickson is highlighted by the following exchange:

> Kozinski: You have a criminal violation when you access Facebook or Google in violation of their terms of service, right?
>
> Ellickson: That's not actually necessarily true. Subsection (a)(2) requires that you exceed authorized access intentionally. So, that means that the . . .
>
> Kozinski: Well, I'm sorry. I was precluding the idea that you stumble on Facebook. I've managed to be on my computer for days and

given the same meaning.'") (quoting Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007)).

[90] *See, e.g.*, Oral Argument, *supra* note 7, at 5:30, 9:40, 11:45, 16:40.

[91] *Id.* at 14:40.

[92] *See, e.g.*, *id.* at 14:40, 16:40. The four minutes of argument following 16:40 are especially insightful.

never stumbled on Facebook. Let's say you do it intentionally. People lie about their age or they lie about their email address or lie about whatever . . .

McKeown: I mean they violated the terms of service . . . You have to be truthful about your personal information.

Ellickson: . . . [T]he question would be whether you actually violated subsection (a)(2) by having that necessary intent . . .

McKeown: What kind of intent do I need? I mean, I'm on Facebook or I'm on Match.com or some other site and [I lie]. I would violate the terms of service, correct?

Ellickson: If you violated the terms of service that would constitute exceeding authorized access, . . . but the government would have the burden in that type of case of proving that the user knew what they were prohibited from doing and intentionally went beyond the limits that the computer owner had placed on . . .

Kozinski: But that's not so difficult. [There is really no question that people lie or that they lie intentionally.] . . .

Ellickson: Your Honor, if, in fact, the user understood that this was something they were prohibited from doing and yet they intentionally

> did it anyway that would fall within the four corners of subsection (a)(2).[93]

This exchange appears to confirm that the DOJ believes that it can prosecute someone for intentionally violating the terms of service of a website.[94] Later, during oral argument, Ellickson did state, however, that, because most people will not have actually read the terms of service and, therefore, will not understand what they can and cannot do, most people cannot be charged with violating subsection (a)(2).[95] This was of little comfort to nine of the eleven judges on the panel[96] and should be of little comfort to those familiar with the development of the duty to read under private contract law.[97]

III. THE DUTY TO READ

Before the widespread adoption of form contracts, the terms within an individual contract had to be negotiated by the

---

[93] *Id.* at 16:40.

[94] *See* Orin Kerr, *Thoughts on the Oral Arguments in United States v. Nosal*, VOLOKH CONSPIRACY (Dec. 19, 2011, 12:46 AM), http://volokh.com/2011/12/19/thoughts-on-the-oral-arguments-in-united-states-v-nosal/; Ginny LaRoe, *Untested Computer-Crime Statute Gets 9th Circuit Workout*, FLA. BUS. REV. (ONLINE), Dec. 19, 2011, *available at* LEXIS; McCullagh, *supra* note 28.

[95] Oral Argument, *supra* note 7, at 23:07 ("[T]he large majority of people who violate the terms of service for a website, for example, would not be violating subsection (a)(2) . . . [because] [t]he large majority of those people will not have read the terms of service [and] will not understand what they are and are not permitted to do.").

[96] United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) (holding nine to two that Nosal did not violate the CFAA).

[97] *See infra* Part III (detailing the development of the duty to read).

parties to that contract.[98] After negotiation, the parties would manifest assent to the contract terms, typically by signing the contract.[99] In the absence of fraud, distress, or mutual mistake, courts would enforce the terms of the contract, believing the parties, who had ostensibly negotiated the contract, had an intimate understanding of the terms to which they had agreed.[100] At this early stage in the development of contract law, it was understandable that courts believed that both parties to a contract had read and understood that contract.[101]

With the advent of forms, it became unreasonable for courts to believe that a party to a simple commercial transaction would negotiate the terms of the contract as common practice began to dictate the use of form contracts.[102] Today, nearly all consumer contracts are forms.[103] Parties to a form contract often do not read the contract prior to signing.[104] Yet, courts routinely treat parties to traditional consumer transactions as if they had read and agreed to the terms in the

---

[98] *See* ARTHUR L. CORBIN, CORBIN ON CONTRACTS § 2.1 (2012), *available at* Lexis CORBIN.

[99] Rossi v. Douglas, 100 A.2d 3, 7 (Md. 1953) ("[O]ne having the capacity to understand a written document who reads it, or, without reading it or having it read to him, signs it, is bound by his signature."); CORBIN, *supra* note 98, at § 29.8.

[100] *See* Rossi, 203 Md. at 199, 100 A.2d at 7; CORBIN, *supra* note 98, at § 29.8.

[101] CORBIN, *supra* note 98, at § 29.12.

[102] *See* Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585, 593 (1991).

[103] AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740, 1750 (2011) (citing Carbajal v. H & R Block Tax Servs., Inc., 372 F.3d 903, 906 (7th Cir. 2004); Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149 (7th Cir. 1997)).

[104] CORBIN, *supra* note 98, at § 29.12. *See also infra* Part V.B (recounting the empirical proof that parties to a license presented by software often do not read that license before "agreeing" to the terms of that license).

form contracts to which they manifest assent.[105] This creates a problem for the DOJ because, if, as suggested in Part V.A, the private contract law is subsumed into the criminal law under the DOJ's interpretation, those who have not read a website's terms of service and who did not know what they could and could not do on that website would be subject to criminal prosecution if they violated the terms of service of that website.[106]

[105] *See, e.g.*, *AT&T Mobility*, 131 S. Ct. 1740.

[106] Judge Kozinski pointed this out to the DOJ in Oral Argument, *supra* note 7, at 23:07:

> Kozinski: But, as you stand there, there is no way you can tell us a way of adopting your definition of (a)(4) that does not expose everybody who lies to Facebook or Google or any Match.com or Roommates.com doesn't expose them to possible prosecution as criminals, right?
> Ellickson: Your Honor, the large majority of people who violate the terms of service for a website for example would not be violating §§ (a)(2) . . .
> Kozkinski: Why?
> Ellickson: The large majority of those people will not have read the terms of service, will not understand what they are and are not permitted to do, and when they do those things on . . .
> Kozinski: But that's a question of proof depending on what the government can prove is going on in their head and you start off with the fact that they have checked the box that says "I have read and understand the terms of service" and in my experience U.S. Attorneys tend to be pretty happy when they have something like that where the person has said "I have read and understand and accept." Of course, you can take the stand and say "No, I didn't" but in my experience it's rare for U.S. Attorneys to pass something like that up.

This problem is compounded by the historical development of case law often applied to software licensing and website usage.[107] Much of this case law stems from Judge Easterbrook's twin opinions in *ProCD, Inc. v. Zeidenberg*[108] and *Hill v. Gateway 2000, Inc.*[109] In *ProCD*, a seller of software included a license agreement that was printed in the manual contained in the box the software came packaged in and appeared as a splash screen each time the software was run.[110] The license agreement that appeared as a splash screen required the user to "indicate acceptance" before it allowed the user to use the software.[111] After holding that ProCD could invite acceptance of the license agreement by conduct, Judge Easterbrook found that the buyer's[112] conduct indicated

See also United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) ("Were we to adopt the government's proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct.").

[107] *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17 (2d Cir. 2002); Van Tassell v. United Mktg. Grp., LLC, 795 F. Supp. 2d 770 (N.D. Ill. 2011); PDC Labs., Inc. v. Hach Co., No. 09-1110, 2009 WL 2605270 (C.D. Ill. Aug. 25, 2009); Hubbert v. Dell Corp., 835 N.E.2d 113 (Ill. App. Ct. 2005).

[108] 86 F.3d 1447, 1449 (7th Cir. 1996).

[109] 105 F.3d 1147 (7th Cir. 1997).

[110] *ProCD*, 86 F.3d at 1450.

[111] *Id.* at 1452 ("[T]he software splashed the license on the screen and would not let [the buyer] proceed without indicating acceptance."). In this way, the software at issue was very similar to "clickwrap." *See infra* Part III.A.

[112] Judge Easterbrook treats the paying party as a "buyer," rather than a "licensee" in both *ProCD* and *Hill*. *Hill*, 105 F.3d at 1149 ("*ProCD* did not depend on the fact that the seller characterized the transaction as a license rather than as a contract; we treated it as a contract for the sale of goods and reserved the question whether for other purposes a 'license' characterization might be preferable.").

acceptance of the license agreement.[113] As a consequence, the license agreement was enforceable.[114] In *Hill*, the buyer purchased a computer over the telephone.[115] The box shipped to the buyer contained both the computer and a list of terms.[116] Relying on *ProCD*, Judge Easterbrook found that the terms within the box limiting the warranty were enforceable.[117]

Interestingly, Judge Easterbrook's analysis in neither *ProCD* nor *Hill* appears to conform to standard common law contract doctrine or Uniform Commercial Code (U.C.C.) analysis.[118] A sale[119] typically works as follows: the seller solicits offers, the buyer makes an offer, and the seller accepts (or rejects) that offer.[120] Thus, it is the buyer who is "master of the offer," not the seller, as it is the buyer who must choose

---

[113] *Id.* at 1452 ("A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance.").

[114] *Id.* at 1455. Note that *which* license (in box or splash screen) was enforceable does not appear to be expressly resolved by Judge Easterbrook within *ProCD*. On the one hand, he discusses software delivery by the internet, *id.* at 1451, and notes that, here, "[the buyer] inspected the package, tried out the software, learned of the license, and did not reject the goods," *id.* at 1453, indicating the splash screen license is at issue. On the other hand, in *Hill*, he states that *ProCD* stands for the proposition that "terms inside a box of software bind consumers who use the software after an opportunity to read the terms and to reject them by returning the product." *Id.* at 1148.

[115] *Id.* at 1148.

[116] *Id.*

[117] *Id.* at 1150.

[118] Klocek v. Gateway, Inc., 104 F.Supp.2d 1332 (D. Kan. 2000).

[119] *Klocek*, like *ProCD* and *Hill*, appears not to distinguish between a "sale" and "license."

[120] *Klocek*, 104 F. Supp. 2d at 1340.

whether and how much to offer.[121] If the seller either performs or promises to perform, acceptance has occurred, unless the seller proposes additional or different terms and acceptance is "expressly made conditional" on assent to those terms.[122] It does not appear that acceptance was "expressly made conditional" on the additional terms. In a sale, if acceptance is "expressly made conditional" on the additional or different terms, U.C.C. § 2-207 analysis must be undertaken.[123] If acceptance is not "expressly made conditional" on the additional or different terms, a modification has been proposed and U.C.C. § 2-209 analysis must be undertaken.[124] Neither of those analyses occurs in *ProCD* or *Hill*.[125]

Still, Judge Easterbrook's reasoning in *ProCD* and *Hill* has been widely adopted as courts have struggled with issues arising out of widespread internet adoption.[126] Both *ProCD* and *Hill* were issued at a time when software was regularly bought in stores instead of downloaded, and websites with terms of service were somewhat unusual.[127] In time, software developers began to allow their products to be downloaded and websites began to incorporate terms of service, resulting in the creation of several different forms of license agreements.[128] Eventually, two major forms of licensing agreement, each with

---

[121] *Id.*
[122] *Id.* at 1339 (quoting U.C.C. § 2-207(1)(1966)).
[123] *Id.* at 1340.
[124] *See id.* at 1338, 1341.
[125] *Id.* at 1339 ("In [both *ProCD* and *Hill*] the Seventh Circuit concluded without support that UCC § 2-207 was irrelevant because the cases involved only one written form.").
[126] *See, e.g.*, Specht v. Netscape Commc'ns Corp., 150 F. Supp. 2d 585, 592–94 (S.D.N.Y. 2001) *aff'd*, 306 F.3d 17 (2d Cir. 2002).
[127] Note that *ProCD* was issued in 1996 and *Hill* was issued in 1997.
[128] *Specht*, 150 F. Supp. at 592.

their own doctrine, emerged: (1) clickwrap, and (2) browsewrap.[129]

A. Clickwrap

Clickwrap is, basically, the same as what Judge Easterbrook called "shrinkwrap" in *ProCD*.[130] Both require some affirmative manifestation of assent—the check of a box or push of a button signaling "I Agree."[131] Clickwrap differs from "shrinkwrap" in that the license does not appear every time the software is run or webservice is logged into; instead it usually appears once prior to installation of the software or when the user first signs up for the webservice.[132] Like the agreement in *ProCD*, clickwrap requires a user to perform some kind of affirmative action manifesting his or her assent to the terms and conditions.[133] Unless assent is manifested, the software or service refuses to allow the user to proceed.[134]

---

[129] Van Tassell v. United Mktg. Grp., LLC, 795 F. Supp. 2d 770, 790 (N.D. Ill. 2011).

[130] *Specht*, 150 F. Supp. 2d at 593–94, n.12 (citing *ProCD*, 86 F.3d at 1452) (noting that clickwrap "presents the user with a message on his or her computer screen, requiring that the user manifest his or her assent to the terms of the license agreement by clicking on an icon," in a way very "similar to the shrink-wrap license at issue in *ProCD* [], which appeared on the user's computer screen when the software was used and could not be bypassed until the user indicated acceptance of its terms.").

[131] *Id.* at 593–94.

[132] *Id.* at 593–94.

[133] *Id.* at 595 (noting both "click-wrap license agreements and the shrink-wrap agreement at issue in *ProCD* require users to perform an affirmative action unambiguously expressing assent before they may use the software.").

[134] *Id.* at 594, n.12 (citing *ProCD*, 86 F.3d at 1452).

Courts routinely enforce clickwrap.[135] This is understandable: clickwrap requires users to manifest assent, similar to the way in which paper-based form contracts require parties to manifest assent by signing the bottom of the form. In some ways, clickwrap is better than a standard, paper-based form contract. With clickwrap, users cannot hope to use the software or service without manifesting assent, whereas, with paper-based form contracts instances of buyers obtaining goods or services without signing all the requisite forms abound. As a result of users having to manifest assent prior to use, courts really only focus on whether the party who was required to click "I Agree" actually clicked "I Agree" when analyzing clickwrap agreements.[136] This manifestation of assent allows courts to assume that the party clicking "I Agree" had notice of the agreement.[137]

B. Browsewrap

Browsewrap, unlike clickwrap, does not require a clear manifestation of assent to the terms and conditions displayed via clicking an "I Agree" button.[138] Browsewrap typically

[135] *See, e.g.*, Van Tassell v. United Mktg. Grp., LLC, 795 F. Supp. 2d 770, 790 (N.D. Ill. 2011); In re RealNetworks, Inc. Privacy Litigation, No. 00C1366, 2000 WL 631341, at *7 (N.D. Ill. May 8, 2000); Hotmail Corp. v. Van$ Money Pie, Inc., No. C 98–20064, 1998 WL 388389 (N.D. Cal. April 16, 1998).

[136] Major v. McCallister, 302 S.W.3d 227, 229 (Mo. Ct. App. 2009) (quoting Burcham v. Expedia, Inc., No. 4:07CV1963 CDP, 2009 WL 586513 (E.D. Mo. Mar. 6, 2009)).

[137] *See id.* at 229 (quoting *Burcham*, 2009 WL 586513).

[138] Sw. Airlines Co. v. BoardFirst, L.L.C., 3:06-CV-0891-B, 2007 WL 4823761 at *4 (N.D. Tex. Sept. 12, 2007) (noting browsewrap "does not require the user to manifest assent to the terms and conditions expressly-the user need not sign a document or click on an 'accept' or 'I agree' button.").

involves a website that has terms and conditions posted somewhere accessible via hyperlink.[139] These terms and conditions often condition use of the website upon compliance with the terms and conditions.[140] Often, no "I Agree" button or box is required to be checked before a user can actually access the contents of the website.[141] Instead, assent to the terms and conditions is simply made conditional upon use of the website.[142] Use indicates assent.[143]

In contrast to the "affirmative manifestation of assent" test used in clickwrap, courts routinely hold that "immediately visible notice" of the existence of terms of service is the determining factor for whether browsewrap will be enforced. However, the enforceability of browsewrap is somewhat more nuanced.[144] The leading case on unenforceable browsewrap is *Specht v. Netscape Communications Corp.*[145] In *Specht*, the only reference to the terms of service was on the bottom of the webpage, something that required the user to scroll down to another screen to view it.[146] The court held that, because the terms were relatively inaccessible, a reasonable user would be unaware of their existence before downloading the software.[147]

---

[139] *Id.* (noting browsewrap typically involves "a situation where a notice on a website conditions use of the site upon compliance with certain terms or conditions, which may be included on the same page as the notice or accessible via a hyperlink.").
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *See* Specht v. Netscape Commc'ns, 306 F.3d 17, 31 (2d Cir. 2002); Major v. McCallister, 302 S.W.3d 227, 230 (Mo. Ct. App. 2009).
[145] 306 F.3d 17 (2d Cir. 2002).
[146] *Id.* at 23.
[147] *Id.* at 20.

As a result, a reasonable user would not have had notice of the terms and, so, the browsewrap was unenforceable.[148] Similarly, in *Hines v. Overstock.com, Inc.*, the terms and conditions of the website were hyperlinked in small text at the bottom of each webpage between the words "privacy policy" and Overstock's trademark.[149] Because the plaintiff was never required to view the terms and conditions and the hyperlinks were not prominently displayed without requiring the plaintiff scroll down, the court found that she had no actual or constructive knowledge of the terms and conditions.[150]

Unlike *Specht*, the terms of service at issue in *Hubbert v. Dell Corp.* were accessible by clicking a blue hyperlink on each of the five online forms that the plaintiffs were required to view.[151] These terms were, in contrast to the terms in *Specht*, "visibly referenced several times through the order process."[152] As a result, the court found that notice was sufficient.[153] Similarly, in *PDC Laboratories, Inc. v. Hach Co.*, the terms were accessible by clicking an underlined, blue hyperlink on three of the order pages.[154] The court in *PDC Laboratories* also found that notice was sufficient.[155] More recently, in *Van Tassell v. United Marketing Group, LLC*, the court found that the terms of service were "far less conspicuous" than in

[148] *Id.*
[149] 668 F. Supp. 2d 362, 365 (E.D.N.Y. 2009) *aff'd*, 380 F. App'x 22 (2d Cir. 2010).
[150] *Id.* at 367.
[151] 835 N.E.2d 113, 118 (Ill. App. Ct. 2005).
[152] Van Tassell v. United Mktg. Grp., LLC, 795 F. Supp. 2d 770, 791 (N.D. Ill. 2011).
[153] *Hubbert*, 835 N.E.2d at 126.
[154] No. 09-1110, 2009 WL 2605270, at *3 (C.D. Ill. Aug. 25, 2009).
[155] *Id.* (citing Colo. Rev. Stat. Ann. § 4-1-201(b)(10) (2009 West)).

Hubbert or *PDC Laboratories*.[156] There, a user would first have to go to the "Customer Service" page, linked off the homepage, before he or she would be able to find the terms of service.[157] The complicated route through the website to the terms of service caused the court to hold that the terms of service were unenforceable because it was possible for users to make purchasers on the website without ever seeing the terms of service or a link to the terms of service.[158] The relationship between notice and enforceability of browsewrap has relied heavily on fact-based determinations, an issue not resolved by the Principles of the Law of Software Contracts.[159]

C. Recent Developments in Enforceability: The Law of Software Contracts

The common law developments surrounding clickwrap and browsewrap outlined above were largely embraced in the Principles of the Law of Software Contracts, which was recently promulgated by the American Law Institute (ALI).[160] The Principles attempt to harmonize the case law of software contracts with best practices.[161] In attempting this harmonization, the Principles craft a unified approach to software contracts, ignoring whether the transaction would be classified as a sale or license and whether software would be

[156] *Van Tassell*, 795 F. Supp. 2d at 792.
[157] *Id.* at 792–93.
[158] *Id.* at 793.
[159] *See* AM. LAW INST., PRINCIPLES OF THE LAW OF SOFTWARE CONTRACTS § 2.02 (2010).
[160] *Compare id.* at § 2.02, *with infra* Part III.A, *and* Part III.B.
[161] *Id.* at intro.

classified a good or an intangible.[162] These distinctions are ignored in order to allow the Principles to address questions of formation (what constitutes assent to an agreement) and content (the meaning of standard terms).[163] Thus, the Principles address the problem identified in *ProCD*, whether to enforce terms that become known to the buyer only after payment, and cases following *ProCD*.[164] Generally, the comments to the Principles find clickwrap enforceable, but note that because notice alone may not be sufficient for first time users, an issue that must be overcome if the private contract law is subsumed into the criminal law, browsewrap may be unenforceable.[165] Other issues with the subsuming of the private contract law into the criminal law are discussed in Part V, which proposes a solution to the problems inherent with subsuming the private contract law into the criminal law. Before a solution is proposed, however, Part IV will examine the DOJ's effort in the mid-1990s to prosecute those who shared copyrighted software or other digitally convertible products—such as music

[162] *Id.* ("These Principles resolve these issues by setting forth a unified approach to software contracts that could apply regardless of whether, under previous interpretations, the transaction constituted a sale or license, or whether software is a good or an intangible.").
[163] *Id.*
[164] *See id.* ("One major set of questions involves whether to enforce contract terms that become available only after payment, or that are presented in a take-it-or-leave-it standard form, or both. Neither Article 2 of the U.C.C. nor the common law has satisfactorily resolved these issues, as evidenced by the amount of litigation, conflicting decisions, and ink spilled in the law reviews.").
[165] *Id.* at § 2.02. ("[M]ere reference to standard terms found on another page (browsewrap) may be insufficient under the reasonable-transferor test unless the transferee is already well-acquainted with the terms, for example, from previous notices and transactions.").

or movies[166]—as an analogy to the problem posed by the DOJ's current embrace of a new interpretation of the CFAA.

IV. THE CURRENT CFAA PROSECUTIONS: WE'VE BEEN HERE BEFORE

In the mid-1990s, the DOJ attempted to redefine the federal wire fraud statute to prosecute those who shared copyrighted software or other digitally convertible products—such as music or movies—in the absence of a statute specifically tailored to that offense.[167] Much like its effort to redefine the CFAA to prosecute Lori Drew and David Nosal, the DOJ's mid-1990s effort to redefine the federal wire fraud statute failed.[168] In response to the DOJ's protestations, Congress passed the No Electronic Theft (NET) Act, which aimed to bolster copyright protections,[169] but resulted in the criminalization of the ordinary conduct of a majority of citizens[170] similar to the way in which adopting the DOJ's definition of "exceeds authorized access" would criminalize the ordinary conduct of a majority of citizens.[171] Unsurprisingly, the NET Act failed to deter the broad swath of conduct Congress criminalized,[172] a fate that a redefinition of

[166] *See* United States v. LaMacchia, 871 F. Supp. 535, 536 (D. Mass. 1994) (giving a short background on the DOJ's effort to prosecute violators of software copyright).
[167] *See, e.g., id.*
[168] *Compare id. with* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).
[169] *See infra* Part IV.B.
[170] *Id.*
[171] *See* Oral Argument, *supra* note 7, at 16:40.
[172] *See infra* Part IV.B.

the CFAA seems to embrace.[173] Only recently has the DOJ reassessed its effort to enforce the NET Act and begun to tailor its strategy to have a significant impact on curtailing that conduct.[174]

A. The Problem: United States v. LaMacchia

The DOJ's attempt to criminalize software and other digital piracy began in the early 1990s and culminated in *United States v. LaMacchia*, a case that closely mirrored *Drew* in judicial distaste for the DOJ's interpretation of the relevant statute.[175] In the early 1990s, LaMacchia, a twenty-one-year-old student at the Massachusetts Institute of Technology (MIT), set up an electronic bulletin board to which users could upload copyrighted software and other users could download that copyrighted software for free.[176] In 1994, the DOJ obtained an indictment charging LaMacchia with violating the wire fraud statute by constructing a scheme to defraud that involved the illegal copying and distribution of copyrighted software on an international scale.[177] Under the wire fraud statute, this scheme required that the copyright infringement "done willfully and for commercial advantage or private financial gain,"[178] something the DOJ was unable to prove.[179]

---

[173] *See* Oral Argument, *supra* note 7.
[174] *Id.* at 16:40.
[175] *Compare* United States v. LaMacchia, 871 F. Supp. 535, 536 (D. Mass. 1994) *with* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).
[176] *LaMacchia*, 871 F.Supp. at 536.
[177] *Id.*
[178] David Goldstone & Michael O'Leary, *Novel Criminal Copyright Infringement Issues Related to the Internet*, 49 U.S. ATTORNEYS' BULLETIN 33, 34 (2001), http://www.justice.gov/usao/eousa/foia_reading_room/usab4903.pdf.

Ultimately, the wire fraud charge was dismissed by the district court because LaMacchia was not making any money from distributing the copyrighted software.[180]

Although the district court sympathized with the DOJ's plight, it held that adopting the DOJ's interpretation of the wire fraud statute would criminalize not only the reprehensible conduct of LaMacchia, but also the innocent conduct of many home users,[181] a sentiment echoed by Judges Kozinski and McKeown in *Nosal*.[182] This was a result the district court determined would be undesirable to even the software industry.[183] As a result, it dismissed the wire fraud charge against LaMacchia.[184]

---

[179] *LaMacchia*, 871 F.Supp. at 540, n.8 (quoting 138 CONG. REC. S. 17958–17959 (October 8, 1992)) ("As Senator Hatch (R-Utah), the Senate sponsor of the Act noted, 'the copying must be undertaken to make money, and even incidental financial benefits that might accrue as a result of the copying should not contravene the law where the achievement of those benefits [was] not the motivation behind the copying.'").

[180] *Id.* at 537.

[181] *Id.* at 544 (noting that the DOJ's "interpretation of the wire fraud statute would serve to criminalize the conduct of not only persons like LaMacchia, but also the myriad of home computer users who succumb to the temptation to copy even a single software program for private use . . . [something] that [not] even the software industry would consider desirable.").

[182] Oral Argument, *supra* note 7, at 5:30, 9:40, 11:45, 16:40.

[183] *LaMacchia*, 871 F.Supp. at 544. *See also LaMacchia*, 871 F.Supp. at 544, n. 18 (quoting Vice–President and General Counsel of the Computer & Communications Industry Association, hearing before the House Judiciary Subcommittee on Intellectual Property and Judicial Administration on S. 893 (Aug. 12, 1992) at p. 65).

[184] *Id.* at 545.

B. The Solution: The NET Act

The combination of a direct challenge to Congress to pass legislation criminalizing the kinds of acts LaMacchia engaged in by Judge Stearns,[185] a coalition of copyright owners outraged by the activities of people like LaMacchia,[186] and the DOJ's continued interest in prosecuting people like LaMacchia,[187] led Congress to pass the No Electronic Theft (NET) Act in 1997.[188] There is no question that the act was passed as a direct result of the holding in *LaMacchia* and expressly sought to overturn that case.[189]

In changing copyright, the NET Act supplemented the "for profit" requirement with an alternate requirement, the reproduction or distribution of copyrighted works worth at least $1,000 in a 180-day period, effectively criminalizing the conduct of those who, like LaMacchia, operated electronic bulletin boards to distribute copyrighted works.[190] Additionally, the NET Act altered the definition of "financial gain" to include "receipt (or expectation of receipt) of anything

---

[185] *Id.* at 545.

[186] Eric Goldman, *A Road to No Warez: The No Electronic Theft Act and Criminal Copyright Infringement*, 82 OR. L. REV. 369, 373 (2003), *available at* http://digitalcommons.law.scu.edu/facpubs/123.

[187] Goldstone & O'Leary, *supra* note 178, at 34.

[188] Goldman, *supra* note 186, at 373.

[189] H.R. REP. No. 105-339, at 3 (1997); 143 CONG. REC. S12689 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch, "This bill plugs the 'LaMacchia Loophole' in criminal copyright enforcement."); 143 CONG. REC. S12689, S12691 (daily ed. Nov. 13, 1997) (statement of Sen. Kyl); 143 CONG. REC. H9883, H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte).

[190] Eric Goldman & Julia Alpert Gladstone, *'No Electronic Theft Act' Proves a Partial Success*, NAT'L L.J., Mar. 17, 2003, at B9, *available at* http://www.ericgoldman.org/Articles/nljnetact.htm.

of value, including other copyrighted works," effectively criminalizing the conduct of those who used LaMacchia's bulletin board to download copyrighted works.[191] Further, Congress also increased the punishments attached to distributing or downloading copyrighted works.[192] Although these changes were supposed to be narrowly tailored to the kinds of activities people like LaMacchia were engaging in, the language of the NET Act was so broad in its scope that there was serious debate over the meaning of its changes.[193] Until 1997 and the passage of the NET Act, Congress had avoided significantly expanding the reach of the criminal law into copyright infringement.[194] With the passage of the NET Act, Congress began targeting a broader group of copyright infringers, effectively criminalizing the activities of a broad swath of the public by allowing the DOJ to prosecute those who downloaded copyrighted works as well as those who distributed copyrighted works.[195]

The DOJ's first prosecution under the NET Act occurred in 1999 under the auspices of Deputy Attorney General Eric H. Holder, Jr.'s "Intellectual Property Rights Initiative."[196] That prosecution saw Jeffrey Gerard Levy, a 22

---

[191] *Id.*
[192] *Id.*
[193] *See, e.g.*, Goldman, *supra* note 186, at 374–76; Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 WASH. U. L.Q. 835, 861–83 (1999).
[194] Loren, *supra* note 193, at 862.
[195] *See* United States v. LaMacchia, 871 F. Supp. 535, 536 (D. Mass. 1994). *Cf.* Goldman, *supra* note 186, at 369, 376 (noting that by enacting the NET Act, Congress specifically targeted "warez" trading.).
[196] Press Release, U.S. Dep't of Justice, First Criminal Copyright Conviction Under the "No Electronic Theft" (NET) Act for Unlawful

year-old senior at the University of Oregon, plead guilty to criminal infringement of a copyright in the United States district court in Eugene, Oregon.[197] Levy was caught by network administrators at the University of Oregon who noticed that visitors to Levy's website, hosted by the University of Oregon, downloaded, on average, 1.7 gigabytes of data every two hours.[198] Further investigation led the network administrators to discover that Levy was hosting copyrighted MP3s, software, and movie clips on his website.[199] Realizing that Levy was probably hosting these files illegally, the network administrators tipped off the FBI and Oregon State Police, who brought the case to the DOJ, which later prosecuted Levy.[200]

Although the Levy prosecution was highly touted by the DOJ, it soon became apparent that the DOJ was fighting a losing battle.[201] While the DOJ rolled out press releases celebrating the prosecution of Levy, the number of people distributing and downloading copyrighted works increased dramatically.[202] Rather than curb copyright infringements, the NET Act seems to have had no discernible impact on

---

Distribution of Software on the Internet (Aug. 20, 1999), *available at* http://www.justice.gov/opa/pr/1999/August/371crm.htm (noting then Deputy Attorney General Eric Holder's instrumental involvement in the push for the NET Act).

[197] *Id.*

[198] Andy Patrizio, *DOJ Cracks Down on MP3 Pirate*, WIRED (Aug. 23, 1999), http://www.wired.com/politics/law/news/1999/08/21391.

[199] *Id.*

[200] Press Release, U.S. Dep't of Justice, *supra* note 196.

[201] Goldman, *supra* note 186, 399 ("[E]mpirical evidence does not indicate that the Act has curbed infringements.").

[202] *Id.* at 398 (noting that empirical evidence "suggests that piracy covered by the Act has gone up since its passage.").

infringing activities.[203] Although it is virtually impossible to reliably estimate the extent of infringing activities, it is undisputed that the economic losses due to infringing activities are "sizeable."[204] On the software front, it is estimated that seventy-five percent of computers are running at least one illegally downloaded software application, while an estimated sixty-seven percent of digital piracy sites are hosted in North America or Western Europe.[205] On the music front, it is estimated that, as of 2008, the average iPod/MP3 player contained 842 pirated songs, or about $800 worth.[206] In sum, all the evidence appeared to point to the proposition that, by 2008, the NET Act had utterly failed.

The failure of the NET Act should not be surprising. It was a deterrence-theory-based[207] law designed to change

---

[203] *Id.* at 398.

[204] GOV'T ACCOUNTABILITY OFFICE, INTELLECTUAL PROPERTY: OBSERVATIONS ON EFFORTS TO QUANTIFY THE ECONOMIC EFFECTS OF COUNTERFEIT AND PIRATED GOODS 2 (April 12, 2010), *available at* http://www.gao.gov/assets/310/303057.pdf ("[M]ost experts observed that it is difficult, if not impossible, to quantify the economy-wide impacts [of piracy]."); Kal Raustiala & Chris Sprigman, *How Much Do Music and Movie Piracy Really Hurt the U.S. Economy?*, FREAKONOMICS (Jan 12, 2012), http://www.freakonomics.com/2012/01/12/how-much-do-music-and-movie-piracy-really-hurt-the-u-s-economy/ (noting that "we simply don't know" the loss due to piracy).

[205] *Online Piracy – Facts, Numbers, Rankings & More! [INFOGRAPH]*, TECH O'CLOCK (Nov. 16, 2011), http://www.techoclock.com/online-piracy-facts-numbers-rankings-more-infograph.

[206] Israel Peralta, *The Music Industry & Online Piracy by the Numbers*, ODDEE (Apr. 13, 2010), http://www.oddee.com/Infographic.aspx?i=Infog_Music_large.jpg&h=3605. *But see* Raustiala & Sprigman, *supra* note 204.

[207] U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL 9-71.010 (2011), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/71mcrm.htm ("[P]rosecution of felony offenses of

individuals' behavior and founded on a formulation that could not possibly hope to be effectuated. Research on the topic is virtually conclusive: certainty of punishment, not severity of punishment, is what produces deterrent effects.[208] The certainty of punishment for copyright violations is so miniscule that it is virtually zero[209] because, as the DOJ admitted before Congress in its testimony regarding the CFAA, it simply does not have the time or resources to prosecute every violation.[210]

Recently, there seems to be a refocusing of the DOJ's efforts aimed at maximizing effective use of the NET Act.[211]

---

comparatively moderate scale may have substantial deterrent impact. . . . A misdemeanor plea also serves a deterrent function because of the prospect of felony charges for a future offense. . . . An unsuccessful prosecution may be counterproductive not only in terms of allocation of resources, but also with respect to deterrence.").

[208] *See, e.g.*, VALERIE WRIGHT, THE SENTENCING PROJECT, DETERRENCE IN CRIMINAL JUSTICE: EVALUATING CERTAINTY VS. SEVERITY OF PUNISHMENT 1 (2010), *available at* http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf; George E. Higgins, Abby L. Wilson, & Brian D. Fell, *An Application of Deterrence Theory to Software Piracy*, 12 J. CRIM. JUST. & POPULAR CULTURE 166, 166 (2005), *available at* http://www.albany.edu/scj/jcjpc/vol12is3/featured%20article%202.pdf ("The findings from the analysis showed that certainty and not severity was important in reducing software piracy.").

[209] I. Trotter Hardy, *Criminal Copyright Enforcement*, 11 WM. & MARY BILL RTS. J. 305, 313 (2002), *available at* http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1320&context=wmborj.

[210] *See* McCullagh, *supra* note 28.

[211] *See, e.g.*, Tamlin H. Bason, *DOJ Adds Wire Fraud, More Criminal Infringement Counts Against Megaupload*, BLOOMBERG BNA (Feb. 22, 2012), http://www.bna.com/doj-adds-wire-n12884907997; Grant Gross, *Courts Shut Down 82 Sites for Alleged Copyright Violations*, PCWORLD (Nov. 29, 2010, 12:10 PM), http://www.pcworld.com/

Over the past few years, the DOJ has shifted its focus to content-hosting and content-linking websites, rather than individuals.[212] The effectiveness of this new theory is currently being tested in the prosecution of the owners and operators of Megaupload.com ("Megaupload"), the largest target the DOJ has taken on to date.[213] Basically, Megaupload was a content-hosting website.[214] Users would upload content to Megaupload, which would then create a unique web address allowing anyone to download that content.[215] On February 16, 2012, an indictment was filed alleging that Megaupload (1) actively solicited infringing material, (2) actively encouraged its users to distribute links to infringing material, and (3) ignored takedown requests sent pursuant to the Digital Millennium Copyright Act.[216] This combination of activities allowed the DOJ to charge Megaupload's owners and operators with racketeering, conspiracy to commit copyright infringement, conspiracy to commit money laundering, criminal copyright infringement, and wire fraud.[217] The case against Megaupload, which was alleged to be the thirteenth most popular website on the internet at one point,[218] already appears to be paying dividends for the DOJ as numerous content-hosting websites have taken steps to prevent U.S. visitors from uploading or

businesscenter/article/211832/courts_shut_down_82_sites_for_alleged_copyright_violations.html.

[212] *See, e.g.*, Gross, *supra* note 211.

[213] *See, e.g.*, Bason, *supra* note 211. *See generally* David Kravets, *Uncle Sam: If It Ends in .Com, It's .Seizable*, WIRED (Mar. 6, 2012, 9:30 AM), http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites/all/1 (discussing recent developments in copyright enforcement).

[214] Bason, *supra* note 211.

[215] *Id.*

[216] *Id.*

[217] *Id.*

[218] *Id.*

downloading content.[219] While only time will tell whether the DOJ's shift in focus will effectively deter those who wish to pirate copyrighted material, avoiding a lag in effective enforcement is an important aspect of the solution proposed in Part V to the problems the DOJ faces regarding the CFAA.

V. A PROPOSED SOLUTION

As the DOJ believes is necessary, the easiest way to prove that an individual had actual knowledge of a website's terms and conditions would be to subsume the developed (and developing) private contract law into the criminal law. It is fairly easy to imagine how the criminal law would impute assent and notice onto the accused, but doing so would seem to create a criminal law that assumes things about the accused that are empirically false. A better solution might be to tailor a broad law, or a set of laws, better suited to reach the kind of conduct that individuals like Lori Drew and David Nosal engaged in, rather than redefining terms that were originally tailored to reach a very narrow, very specific class of offenders.

---

[219] *See, e.g.*, Enigmax, *RapidShare Slows Download Speeds To Drive Away Pirates*, TORRENTFREAK (Feb. 24, 2012), http://torrentfreak.com/rapidshare-slows-download-speeds-to-drive-away-pirates-120224/; Ernesto, *Is BitTorrent Done? Major Torrent Sites Consider Shutting Down*, TORRENTFREAK (Feb. 7, 2012), http://torrentfreak.com/is-bittorrent-done-major-torrent-sites-consider-shutting-down-120207/; Ernesto, *Turbobit.net Blocks US Visitors After MegaUpload Shutdown*, TORRENTFREAK (Feb. 7, 2012), http://torrentfreak.com/turbobit-net-blocks-us-visitors-after-megaupload-shutdown-120207/; Enigmax, *QuickSilverScreen Streaming Links Site Calls It Quits*, TORRENTFREAK (Feb. 7, 2012), http://torrentfreak.com/quicksilverscreen-streaming-site-calls-it-quits-120207/.

Part V.A discusses why the DOJ would want to subsume the private contract law into the criminal law for the purposes of proving the knowledge of the accused. Part V.B examines this approach in light of empirical studies that indicate that subsuming the private contract law into the criminal law creates a serious problem for the law. Part V.C discards the easy solution proposed in Part V.A and proposes a new solution, one that focuses on the expansion of negligent manslaughter to punish conduct like Lori Drew's and the creation of a new statutory scheme to punish conduct like David Nosal's.

A. Subsuming the Private Contract Law

The easiest way to facilitate prosecutions under the CFAA would be for the DOJ to subsume the private contract law into the criminal law.[220] While it is possible that the DOJ might not incorporate the developed and developing civil doctrines of clickwrap and browsewrap into its interpretation of the CFAA, it would very hard for the DOJ to prove, beyond a reasonable doubt, that the accused had actual knowledge of the terms of service if the DOJ did not incorporate those civil doctrines.[221] A successful prosecution would almost require that the government had a witness who could testify that the accused either discussed the terms of service with him or her or he or she saw the accused reading the terms of service.[222] It

[220] *See* Oral Argument, *supra* note 7, at 23:07–24:25 (discussing problems of proof).
[221] *See id.*
[222] The government could not, of course, rely on the testimony of the accused because the accused has the right not to take the stand. Griffin v. California, 380 U.S. 609, 613–14 (1965). *See also* Hoffman v. United States, 341 U.S. 479, 486 (1951) ("The [Fifth Amendment] privilege

would be the rare case that the government could procure such a witness, making it impractical, in most cases, for the government to pursue a case against the accused, regardless of the accused's alleged conduct.[223] The easiest and probably most practicable way to avoid this issue is to incorporate the civil rules of knowledge for clickwrap and browsewrap.[224]

If, then, the civil rules of knowledge for clickwrap are incorporated into the criminal law, there would, presumably, be no problem finding that the accused knew or should have known what the clickwrap said about what is and what is not allowed.[225] The accused had notice of the terms of service.[226] Those terms were present on the same page as the

---

[against self-incrimination] not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime."). And, in any case, the accused would have a strong incentive to testify that he or she had not read the terms of service, even if that were not true.

[223] It is easy to imagine scenarios similar to the one in *Drew* where the accused's knowledge of terms of service would be at issue. *See, e.g.*, David Kushner, *The Hacker is Watching*, GQ (Jan. 2012), *available at* http://www.gq.com/news-politics/newsmakers/201201/luis-mijangos-hacker-webcam-virus-internet.

[224] *See, e.g.*, Oral Argument, *supra* note 7, at 23:07–24:25 (reasoning that in cases of clickwrap the government would have a strong case for knowledge on the basis of the manifestation of agreement itself).

[225] *See, e.g.*, Van Tassell v. United Mktg. Grp., LLC, 795 F. Supp. 2d 770, 790 (N.D. Ill. 2011); In re RealNetworks, Inc. Privacy Litig., No. 00C1366, 2000 WL 631341; Hotmail Corp. v. Van$ Money Pie, Inc., No. C 98–20064, 1998 WL 388389, at *6 (N.D. Cal. Apr. 16, 1998).

[226] Major v. McCallister, 302 S.W.3d 227, 229 (Mo. Ct. App. 2009) (citing Burcham v. Expedia, Inc., No. 4:07CV1963 CDP, 2009 WL 586513, at *2 (E.D. Mo. Mar. 6, 2009)).

manifestation of assent.[227] It would be easy, then, to determine that the accused knew what he or she was allowed to do with the software or web service.

If the civil rules of knowledge for browsewrap are incorporated into criminal law, prosecutors would not have the advantage of being able to point to the manifestation of assent created by the accused clicking "I Agree" as with clickwrap.[228] However, it does not seem very difficult for prosecutors to prove that the accused had "sufficient notice" of the terms of service.[229] All that prosecutors need do is point to an instance where the terms of service are hyperlinked, preferably in blue, on a page the accused had to visit and that required no scrolling down to see the hyperlink.[230]

B. The Empirical Problem with Subsuming the Private Contract Law

While it may be easy to subsume the private contract rules into the criminal law, there is one serious problem with doing so: most people do not read the terms and conditions of

---

[227] *Id.*

[228] *See* Hotels.com, L.P. v. Canales, 195 S.W.3d 147, 154–55 (Tex. App. 2006).

[229] *Cf.* United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) ("Not only are the terms of service vague and generally unknown—unless you look real hard at the small print at the bottom of a webpage—but website owners retain the right to change the terms at any time and without notice . . . Accordingly, behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever.").

[230] *See* Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 365 (E.D.N.Y. 2009) *aff'd*, 380 F. App'x 22 (2d Cir. 2010); Hubbert v. Dell Corp., 835 N.E.2d 113, 118 (Ill. App. Ct. 2005).

clickwrap or browsewrap agreements.[231] It is estimated that fewer than two percent of users read the clickwrap agreements during software installation.[232] Indeed, there is evidence from large-scale field experiments involving more than 80,000 users that indicate the only thing clickwrap has done is train users to click "I Accept" whenever presented with a clickwrap agreement.[233]

User approach to browsewrap is similar.[234] Regulators in the United Kingdom have found that seventy-one percent of users do not read browsewrap.[235] Other evidence suggests that the percentage of users who do not read browsewrap may be as high as eighty-eight percent.[236] And it is not uncommon to see news articles about website owners playing practical jokes on their customers by incorporating clauses into their browsewrap that makes their customers, for instance, agree to furnish their

---

[231] *See, e.g.*, *7,500 Online Shoppers Unknowingly Sold Their Souls*, FOX NEWS (Apr. 15, 2010), http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/; RAINER BÖHME & STEFAN KÖPSELL, TRAINED TO ACCEPT? A FIELD EXPERIMENT ON CONSENT DIALOGS (2010), *available at* http://www.wi.uni-muenster.de/security/publications/BK2010_Trained_To_Accept_CHI.pdf; MATTHEW KAY & MICHAEL TERRY, TEXTURED AGREEMENTS: RE-ENVISIONING ELECTRONIC CONSENT 1 (2010), *available at* http://cups.cs.cmu.edu/soups/2010/proceedings/a13_kay.pdf; Mike Masnick, *People Don't Read Privacy Policies... but Want Them to Be Clearer*, TECHDIRT (Feb. 17, 2009), http://www.techdirt.com/articles/20090216/1803373786.shtml.

[232] KAY & TERRY, *supra* note 231, at 1.

[233] BÖHME & KÖPSELL, *supra* note 231, at 2406.

[234] Masnick, *supra* note 231.

[235] *Id.*

[236] *7,500 Online Shoppers Unknowingly Sold Their Souls*, *supra* note 231.

"immortal souls" in exchange for the privilege of being able to make purchases on that website.[237]

Many of the reasons why users do not read clickwrap or browsewrap are the same reasons why they do not read form contracts—the legalese is difficult to understand, they lack bargaining power, and it is more likely than not that nothing will go wrong.[238] Additionally, the internet aggravates the problem of important terms being hidden from those accepting the form contracts by forcing them to go to another page or scroll through a long document to find those terms.[239] Even in a class of contracts students, who, presumably, know all the reasons why users should read the terms, these factors are so persuasive that only four percent of them read while forty-four percent never read.[240] And, there is some indication that users who read do not actually account for the meanings of those terms in their decision-making processes.[241]

---

[237] *Id.*

[238] Robert A. Hillman, *Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?*, 104 MICH. L. REV. 837, 840–41 (2006).

[239] *Id.* at 841. *See also* Alexis Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (March 1, 2012), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ (indicating that it is not possible to read all the browsewrap agreements that a user encounters in one year).

[240] *See* Hillman, *supra* note 238, at 842.

[241] *Id.* at 856. *See generally* Alina Tugend, *Too Many Choices: A Problem That Can Paralyze*, N.Y. TIMES (Feb. 26, 2010), http://www.nytimes.com/2010/02/27/your-money/27shortcuts.html (discussing why being presented with too many factors in a decision making situation leads individuals to make bad choices).

The problem with subsuming the private contract rules into the criminal law is that the fundamental premise of criminal law that *ignorantia juris quod quisque tenetur scire, neminem excusat*,[242] which has long been recognized as a "useful fiction,"[243] becomes, quite obviously, a fiction[244] and not only because of empirical evidence stating that users do not read. In the realm of private contract law, there seems little serious disagreement that clickwrap and browsewrap can apply Llewellyn's "useful fiction": individuals who manifest assent to form contracts will be presumed to have read the terms of those contracts if they were given a reasonable opportunity to read the terms.[245] Indeed, this position was adopted by the American Law Institute in the Principle of the Law of Software Contracts.[246] This fiction works because, under private contract law, courts willing to police the "fairness of the contract" protect individuals who manifest assent.[247] Yet, there is a problem with subsuming this fiction into the criminal law. In

[242] 4 WILLIAM BLACKSTONE, COMMENTARIES *27 (translating as "ignorance of law, which everyone is bound to know, excuses no one.").
[243] LON L. FULLER, LEGAL FICTIONS 84 (1967).
[244] *See, e.g.*, BÖHME & KÖPSELL, *supra* note 231, at 2406; Masnick, *supra* note 231.
[245] Hillman, *supra* note 238, at 846 ("Llewellyn wrote that, so long as a consumer has access to standard terms, her signature constitutes an implied delegation to the drafter of the duty to draft fair and efficient boilerplate terms, even if the consumer does not read them . . . . Under Llewellyn's theory, consumers who agree to a standard-form transaction after mandatory website disclosure would have a more difficult time complaining of hollow assent.").
[246] Robert A. Hillman, *Contract Law in Context: The Case of Software Contracts*, 45 WAKE FOREST L. REV. 669, 679–80 (2010).
[247] *See* JAMES J. WHITE & ROBERT S. SUMMERS, PRINCIPLES OF SALES LAW 43 (1st ed. 2009) (implying all "judicial inquiry about the conspicuousness and clarity of form contract terms is . . . really a covert investigation of the fairness of the contract.").

the realm of private contract law, an individual might manifest assent to a form that contains unenforceable provisions.[248] If this fiction is subsumed into the criminal law, it becomes far more difficult to say that the accused "knew the law" when he or she violated a term which requires a court's judgment to determine whether it is enforceable.[249]

C. The Proposed Solution

The two easiest ways of attempting to incorporate the civil rules for clickwrap and browsewrap while avoiding the problems listed in the section above are, in large part, unsatisfactory. The easiest way of incorporating the civil rules for clickwrap and browsewrap would be to require a strict adherence to the express terms. This has the disadvantage of letting private corporations define what is and what is not illegal, dividing the criminal law into as many pieces as there are corporate networks.[250] The fact that these fundamentally contractual constraints will "also define what constitutes

[248] *See id.* at 43. *See also* CORBIN, *supra* note 98, at § 79.1.

[249] United States v. Drew, 259 F.R.D. 449, 464–66 (C.D. Cal. 2009) (discussing whether Drew should have expected to be subjected to criminal prosecution for the violation of a term in a private contract).

[250] *See* Letter from Laura W. Murphy, Director, Wash. Legislative Office, Am. Civil Liberties Union et al. to Patrick Leahy, Chairman, Senate Comm. on the Judiciary, & Charles Grassley, Ranking Member, Senate Comm. on the Judiciary 1 (Aug. 3, 2011), *available at* https://www.cdt.org/files/pdfs/CFAA_Sign-on_ltr.pdf ("[S]everal courts have used companies' network terms of use, which lay out *contractual* constraints on users' use of those networks, to also define what constitutes *criminal* behavior on those networks. The consequence is that private corporations can in effect establish what conduct violates federal criminal law when they draft such policies.").

criminal behavior on those networks"[251] should give policymakers serious pause. The alternative of adopting something like the "doctrine of reasonable expectations" would have the disadvantage of failing to overcome the problem of whether the accused "knew the law" when he or she violated a term which may or may not be enforceable.[252]

A better solution than attempting to lump all kinds of internet-based offenses into the preexisting language of the CFAA, which is already aimed at "hackers"[253] and which faces the difficult problems outlined above, is to identify the conduct the DOJ is attempting to proscribe through these controversial CFAA-based prosecutions and tailor laws to specifically proscribe that conduct. There seem to be two types of conduct the DOJ would like to proscribe: (1) conduct analogous to Lori Drew's, and (2) conduct analogous to David Nosal's. Because these are two different types of conduct, both will be discussed separately, before an argument is given for why this is a better solution than that currently advocated by the DOJ.

1. Punishing Lori Drew's Conduct

The conduct the DOJ was attempting to punish in *Drew* was Lori Drew's involvement in Megan Meier's suicide via the internet. Lori Drew created a fictitious persona on MySpace as a part of plan to integrate herself into Megan Meier's life and

---

[251] *Id.*

[252] *See Drew*, 259 F.R.D. at 464–66 (discussing whether Drew should have expected to be subjected to criminal prosecution for the violation of a term in a private contract).

[253] *See* H.R. REP. NO. 98-894, at 10 (1984) *reprinted in* 1984 U.S.C.C.A.N. 3689, 3696.

drive Meier towards suicide.[254] She engaged with Meier on numerous occasions via this persona, culminating in an hour-long exchange of insults.[255] The final message Drew sent to Meier was "[t]he world would be a better place without you."[256] Meier was found in her bedroom closet by her mother a little while later.[257] Dead.[258] She had committed suicide at age thirteen.[259]

In the realm of criminal law, Drew's conduct seems most analogous to involuntary manslaughter.[260] Ordinarily, the federal government would not have jurisdiction to prosecute an involuntary manslaughter case in Missouri, so Drew could only be prosecuted by the Missouri Attorney General's Office.[261] There would seem to be room for the prosecution of people like Drew under the Missouri statute on involuntary manslaughter,[262] if only by analogy to early vehicular homicide

[254] *See* Maag, *supra* note 11.
[255] *Id.*
[256] *Id.*
[257] *Id.*
[258] *Id.*
[259] *Id.*
[260] *See* 18 U.S.C. § 1112 (2006); Mo. Ann. Stat. § 565.024 (2008).
[261] The original iterations of the CFAA seemed to strongly separate conduct that occurred among states, i.e. interstate, and conduct that occurred within a state, i.e. intrastate. *See* S. REP. NO. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.
[262] In Missouri, "[a] person commits the crime of involuntary manslaughter in the second degree if he acts with criminal negligence to cause the death of any person." Mo. Ann. Stat. § 565.024 (West 2012). "To make negligent conduct culpable or criminal and make it manslaughter, the particular negligent conduct of the defendant must have been of such a reckless or wanton character as to indicate on his part utter indifference to the life of another who is killed as a result thereof." State v. Melton, 33 S.W.2d 894, 895 (Mo. 1930).

prosecutions.[263] Before Missouri's involuntary manslaughter statute was tailored to deal with vehicular cases, it was successfully used in the prosecution of individuals who committed vehicular acts now specifically identified in the involuntary manslaughter statute.[264] Similar justifications would seem to sustain application of the same statute to what is also essentially a homicide crime.[265]

If the state court remedy is deemed insufficient, Congress might be able to design a constitutionally valid statute regulating virtually the same conduct, on the basis that it uses channels of interstate commerce to accomplish its goal.[266] An analogy might be found in the federal wire fraud statute,[267] which requires the interstate use of the wire for prosecution.[268] Designing a constitutionally valid statute would

---

[263] *See* State v. Watson, 115 S.W. 1011, 1013 (Mo. 1909) (failing to mention specific provisions of the statute dealing with vehicles); State v. Horner, 180 S.W. 873, 874 (Mo. 1915) (failing to mention specific provisions of the statute dealing with vehicles).

[264] *Compare Watson*, 115 S.W. at 1013 (failing to mention specific provisions of the statute dealing with vehicles), *and Horner*, 266 Mo. 109, 180 S.W. at 874 (failing to mention specific provisions of the statute dealing with vehicles), *with* Mo. Ann. Stat. § 565.024 (West 2012) (having several sections specifically mentioning vehicles).

[265] *See Watson*, 115 S.W. 1011; *Horner*, 180 S.W. 873.

[266] United States v. Lopez, 514 U.S. 549, 558–59 (1995) (holding Congress may regulate the channels of interstate commerce to keep them "free from immoral and injurious uses" and "activities that substantially affect interstate commerce."); United States v. Cardoza, 129 F.3d 6, 11–12 (1st Cir. 1997) (holding Congress may regulate the "intrastate sale, transfer, delivery, and possession of handguns to and by juveniles.").

[267] 18 U.S.C. § 1343 (2006).

[268] Annulli v. Panikkar, 200 F.3d 189, 200 (3d Cir. 1999); Smith v. Ayres, 845 F.2d 1360, 1366 (5th Cir. 1988). Intrastate use cannot be prosecuted federally. *Id.*

probably require Congress to charge the DOJ with specifically demonstrating that the internet communication occurred in an interstate manner, such as being routed through another state, as courts have held that, in the context of wire fraud, intrastate communications cannot be prosecuted federally.[269] This might effectively allow the federalization of what would otherwise be a state-level crime.[270]

2. Punishing David Nosal's Conduct

In contrast to the conduct the DOJ was trying to punish in *Drew*, the conduct the DOJ was trying to punish in *Nosal* actually involved a contractually based dispute, the "misappropriation" of an employer's information by current and former employees.[271] In short, Nosal set up a competing business using information owned by Korn/Ferry International, his former employer, in violation of a contractual agreement with Korn/Ferry International.[272] This conduct is very different from that alleged in *Drew*.[273]

In designing a new statute or modifying the CFAA to deal with the conduct in *Nosal*, Congress would simply be

---

[269] *Ayres*, 845 F.2d at 1366. *See also* United States v. Morrison, 529 U.S. 598, 618 (2000) ("The regulation and punishment of intrastate violence that is not directed at the instrumentalities, channels, or goods involved in interstate commerce has always been the province of the States.").

[270] *See generally* Craig M. Bradley, *Racketeering and the Federalization of Crime*, 22 AM. CRIM. L. REV. 213 (1984) (discussing the evolution of legislation prohibiting racketeering from its origins at the state level through federalization of nearly all aspects of racketeering).

[271] United States v. Nosal, 642 F.3d 781, 783 *rev'd en banc granted*, 661 F.3d 1180 (9th Cir. 2011).

[272] *Id.*

[273] *Compare id.* at 783, *with* Drew, 259 F.R.D. at 452.

proscribing the use of an internet connected computer to violate specific contractual provisions, such as non-compete clauses or agreements not to misappropriate employer-owned information. Congress can overcome concerns about whether employees would be on notice that the violations of certain provisions in their employment contracts could result in criminal prosecution.[274] Congress could include language specifying which contractual provisions could result in criminal prosecution, similar to the way in which U.C.C. § 2-316 contemplates how implied warranties may be disclaimed.[275] The statute would also require the disclosure of the possibility of criminal prosecution in the employment contracts.[276] Inserting such language would clearly convey Congressional intent to criminalize the conduct of individuals like Nosal and provide employers (and prosecutors) easy access to language that clearly indicates that violations can result in criminal prosecution.[277]

---

[274] *See* United States v. Drew, 259 F.R.D. 449, 464–65 (C.D. Cal. 2009). (discussing whether Drew should have expected to be subjected to criminal prosecution for the violation of a term in a private contract).

[275] This insertion may be necessary in order to avoid the concern that nonstandard language could be too ambiguous for an employee to have fair notice of the possibility of criminal prosecution.

[276] This would be analogous to the disclosure requirements of the American Law Institute's Principles of the Law of Software Contracts. *See, e.g.*, Robert A. Hillman & Maureen O'Rourke, *Defending Disclosure in Software Licensing*, 78 U. CHI. L. REV. 95, 103–04 (2011) (arguing that even if parties to form contracts do not read them those contracts should still be enforced).

[277] United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012) ("If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.").

3. A Better Solution?

Designing two new statutes—one narrowly tailored to proscribe conduct like Drew's and one narrowly tailored to proscribe conduct like Nosal's—rather than just broadening the definition of "exceeds authorized access," is a better solution. Two new statutes work better not only for the empirical reasons outlined in Part V.B, but also because they avoid a *United States v. Kozminski* problem.[278] In *Kozminski*, the Court refused to adopt the DOJ's interpretation of "involuntary servitude" because doing so would "criminalize a broad range of day-to-day activity."[279] Adopting the DOJ's interpretation would allow (1) prosecutors and juries, rather than legislatures, to determine what constitutes a crime, (2) individuals to be subject to discriminatory prosecutions and convictions, and (3) ordinary people to be deprived of fair notice of what activities are criminal.[280] The concern with the great power this construction gives prosecutors was reiterated by the court in *Nosal*, specifically in the context of abuses of that power when "tempting target[s]," like Drew, come within a prosecutor's sights.[281] Narrowly tailored statutes, specifically aimed at conduct like Drew's and Nosal's, will prevent the stretching of

[278] 487 U.S. 931 (1988).
[279] *Id.* at 932.
[280] *Id.* ("That interpretation . . . would delegate to prosecutors and juries the inherently legislative task of determining what type of coercive activities are so morally reprehensible that they should be punished as crimes; would subject individuals to the risk of arbitrary or discriminatory prosecution and conviction; and would make the type of coercion prohibited depend entirely on the victim's state of mind, thereby depriving ordinary people of fair notice of what is required of them.").
[281] *Nosal*, 676 F.3d at 862.

a statute originally aimed at "hackers" to encompass individuals like Drew and Nosal.[282]

Further, narrowly tailoring two separate statutes will prevent lengthy discussions of the "rule of leniency" and whether it is doubtful that Congress meant to include within the scope of its prohibition the conduct of people like Drew and Nosal.[283] This is something that blends into the empirical problem discussed in Part V.B because, while ignorance of the law alone will not be sufficient to invoke the "rule of leniency," it can trigger a court's skepticism, leading to narrower constructions of statutory language than would ordinarily occur.[284] Indeed, the chief complaint of the dissent in *Nosal* is not that the majority's colorful hypotheticals are

[282] *See id.* at 862–63 (indicating that the CFAA's language should be construed as narrowly as possible in light of its original purpose, prohibiting hacking, especially since Congress makes criminal law and not the courts).

[283] *See, e.g.*, *id.* at 863 (quoting United States v. Cabaccang, 332 F.3d 622, 635 n.22 (9th Cir. 2003)) (internal quotations omitted) (alterations in original) ("If there is any doubt about whether Congress intended [the CFAA] to prohibit the conduct in which [Nosal] engaged, then 'we must choose the interpretation least likely to impose penalties unintended by Congress.'").

[284] *See, e.g.*, *id.* at 859 ("While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer.").

wrong,[285] but that the majority's construction of "exceeds authorized access" is too narrow.[286]

Adopting the two-statute solution proposed above not only has the benefit of bypassing the empirical difficulties identified in Part V.B and the *Kozominski* problem, but will also help narrowly target the DOJ's efforts, potentially avoiding years of wasted efforts, as occurred with the NET Act,[287] and reinforces the DOJ's effort to prosecute those cases with the largest deterrent effect.[288] Since, as with the NET Act, the DOJ does not have the resources to prosecute every case,[289] adopting a two-statute solution will allow the DOJ to identify and prosecute those cases with the largest deterrent effect and the greatest likelihood of winning.[290] Further, adopting a two-statute solution will increase the deterrent effect because

[285] *Id.* at 867 (Silverman, Cir. J., dissenting) ("[E]ven if an imaginative judge can conjure up far-fetched hypotheticals producing federal prison terms for accessing word puzzles, jokes, and sports scores while at work, well, . . . that is what an as-applied challenge is for.").

[286] *Id.* at 864 (Silverman, Cir. J., dissenting) ("The majority also takes a plainly written statute and parses it in a hyper-complicated way that distorts the obvious intent of Congress.").

[287] *See* Bason, *supra* note 211 (discussing the DOJ's efforts to pursue NET Act violations against Megaupload); Gross, *supra* note 211 (discussing the DOJ's shift towards pursuing infringing domains, rather than individuals in NET Act prosecutions).

[288] U.S. DEP'T OF JUSTICE, *supra* note 207, at 9-71.010 (discussing deterrent effects and noting that "[a]n unsuccessful prosecution may be counterproductive not only in terms of allocation of resources, but also with respect to deterrence.").

[289] McCullagh, *supra* note **Error! Bookmark not defined.**.

[290] U.S. DEP'T OF JUSTICE, *supra* note 207, at 9-71.010 (discussing deterrent effects and noting that "[a]n unsuccessful prosecution may be counterproductive not only in terms of allocation of resources, but also with respect to deterrence.").

deterrent effect is correlated with certainty of punishment, and the prohibitions included in the two-statute solution will target very specific conduct, making it more certain that those engaged in that conduct will be punished.[291]

VI. CONCLUSION

If the DOJ's interpretation of the CFAA is adopted and prosecutions for violations of websites' terms of service are allowed to proceed, effectively subsuming private contract law into criminal law, there will be serious empirical and legal hurdles to overcome. Additionally, the history of the NET Act indicates that there is some reason to give second thought to the DOJ's proposed course of action.

The solution proposed in Part V has the advantage of targeting both kinds of conduct the DOJ wants to be able to prosecute without really having to confront the uncomfortable issue of subsuming the private contract law into the criminal law. It avoids the possibility of a prosecution based upon the viewing of a publically available website, such as 27b/6, or a prosecution based upon lying on an interactive website, such as Facebook, unless those lies directly contribute to the death of another person. It also avoids the problems associated with any attempt to determine whether the accused had sufficient notice of the illegality of his or her actions. And, perhaps most

[291] *See* Higgins, Wilson, & Fell, *supra* note 208, at 166 ("The findings from the analysis showed that certainty and not severity was important in reducing software piracy.").

importantly, it avoids criminalizing conduct, such as lying, that the vast majority of people engage in.[292]

[292] MARK TWAIN, ON THE DECAY OF THE ART OF LYING (1885), *available at* http://www.gutenberg.org/cache/epub/2572/pg2572.html. *See also* DAVID SHORE, HOUSE: UNTITLED DAVID SHORE PROJECT PILOT 11 (2004), *available at* http://leethomson.myzen.co.uk/House/House_1x01_-%20_Pilot.pdf.