CONTRACTUAL VALIDITY OF END USER LICENCE AGREEMENTS

Renée Zmurchyk

End User Licence Agreements (EULAs) specify the parameters governing the use of a product and may be found on all software. Originally, EULAs were created simply to limit product liability and a manufacturer's warranty on goods but have since evolved into extremely elaborate contracts, often containing highly restrictive terms. EULAs are typically formed with consumers who have no bargaining power, where negotiation is nonexistent, and true acceptance is frequently not required. The validity and enforceability of EULAs and, more specifically, terms within EULAs, has continued to perplex those in the software world. Even within the courts there has been considerable controversy. An exploration of the various forms in which EULAs may be presented, the terms contained therein, as well as recent case law will provide insight into the current state of these agreements.

Part I: Forms of EULAs

EULAs can take on many forms, some of which are typically known as clickwrap, browsewrap and shrinkwrap agreements. These agreements have in common a lack of negotiation, as the contract is dictated by the producer and acceptance is indicated by some act other than a written signature. This article provides a review of the current state of EULAs and the various ways in which they may be presented to the consumer.

Clickwrap Agreements

Clickwrap agreements require the user to scroll through the agreement and confirm acceptance of the terms and conditions by taking some form of positive action, such as clicking an "I accept" button, prior to use of the program. The installation or use of the software is conditional on the user accepting the agreement and thereby consenting to abide by its terms.

The use of clickwrap agreements is growing. Today, there remains no doubt that legally binding contracts between users and manufacturers may be formed online. The momentous case of *Rudder* v. *Microsoft Corporation,* [*Rudder*][1] established that clickwrap agreements are valid and legally binding contractual agreements. In *Rudder*, Microsoft filed for a permanent stay of proceedings, claiming that the plaintiffs agreed online to the exclusive jurisdiction clause stating that the State of Washington was the governing jurisdiction for any disputes. The plaintiffs argued that the online agreement should not be enforced because they did not receive specific notice of the clause and were therefore unaware of its existence. In rejecting the plaintiffs' claim, the Court noted that the plaintiffs were required to click an "I agree" button twice during the process and that the forum selection clause was no more difficult to read than any other term. The Court compared the online agreement to an agreement in writing, holding that it must be given the same enforcement.[2]

The recent 8th Circuit Court decision in *Davidson & Associates, Inc.* v. *Jung,* [*Davidson*][3] affirmed that clicking on an "I Agree" button at the end of a EULA creates a binding agreement and will be enforceable against the consumer. The Court took into account that the software packaging contained notice on the outside of the box stating that it is subject to a EULA, the defendants assented to the EULA by clicking the "I agree" button, and then proceeded to install the game. Terms of the EULA were disclosed prior to game installation and the

---

[1] (1999), 2 C.P.R. (4th) 474 (Ont. Sup. Ct.) [*Rudder*].

[2] *Supra* note 1 at para. 19.

[3] 422 F.3d 630 (8th Cir. 2005) [*Davidson*].

defendants expressly consented to those terms. These factors were found to be sufficient notice to create a binding contract.[4]

Few cases have considered the validity of clickwrap licences, however; where their validity has been challenged, the terms of the contract have ultimately been upheld.[5] It appears that future courts will find clickwrap agreements to be valid binding contracts as long as a standard of notice is met. The recent case law indicates this onus may be satisfied where the term being challenged is plainly stated within the EULA and a positive action for assent to the entire EULA is required.

Browsewrap Agreements

Browsewrap agreements set out the terms somewhere within the site but do not require the user to review or agree to the terms prior to use of the program. Uncertainty remains surrounding the enforceability of browsewrap agreements because of the lack of active consent required by the user. There are very few cases that deal directly with browsewrap agreements.

In *Register.com, Inc.* v. *Verio, Inc.,*[6] the New Jersey Superior Court Appellate Division upheld the enforceability of the browsewrap agreement on the basis of implied consent, whereby the end user had agreed to the terms simply through installation or use of the software. The browsewrap agreement was recognized based on the fact that it was designed and presented carefully. The Court noted that the terms of use were clearly posted on the Web site and that the defendant's conduct in using the site constituted agreement of the terms.

However, other courts have held that browsewrap agreements are unenforceable.[7] For example, in *Ticketmaster* v. *Tickets.com,*[8]

---

[4] See pg. 66 for further analysis of the *Davidson* case.

[5] See notes 1 and 3.

[6] 126 F. Supp. 2d 238 (S.D.N.Y. 2000).

[7] See *Specht* v. *Netscape Communications Corp* 150 F. Supp. 2d 585 (S.D.N.Y. 2001), for further discussion on browsewrap agreements. In this case the agreement was unenforceable.

[8] 2003 U.S. Dist. LEXIS 6484 (D. Cal. 2003) at 2.

Ticketmaster argued that its browsewrap agreement was analogous to a shrinkwrap agreement, where notice on the exterior packaging states that opening the package constitutes adherence to the licence agreement. Ticketmaster set forth its terms and conditions on its Web site homepage, along with a statement providing that anyone who continued using the site was deemed to have agreed to those terms. The Court was not persuaded by this argument, ruling that terms on a Web site are not necessarily obvious and may be easily missed. In finding that no implied agreement existed, the Court noted that many customers will not bother to read the fine print and therefore, it cannot be said that merely putting the terms on the Web site creates a contract with anyone using that site.

According to a recent study of precedents and scholars, it was suggested that a browsewrap agreement will likely be valid and enforceable where the following four elements are satisfied: (1) the user is given adequate notice that the terms exist; (2) the user has a meaningful opportunity to review those terms; (3) the user is given notice that taking a specified action results in assent to the specified terms; and (4) the user performs that specified action.[9]

Shrinkwrap Agreements

Shrinkwrap agreements have the terms contained on or inside the software box. Originally, shrinkwrap agreements were located on the exterior of the software packaging, allowing consumers to read the terms prior to purchase. The concept was that the licence terms were deemed to be accepted once the user opened the shrinkwrap seal on the software product. This has changed in recent years, possibly to improve the visual appearance of the box, with licences now being placed inside the packaging. Acceptance of shrinkwrap agreements is generally indicated by the use of the software and failure to return it within a specified period of time. Arguably, reading a notice inside a box is not equivalent to the degree of assent that occurs in a clickwrap agreement, where the consumer must take a positive action to agree to the terms, although the validity of shrinkwrap agreements has been upheld.

---

[9] Christina L. Kunz et al., "Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements" (Nov. 2003) 59 The Bus. Lawyer 291 (QL).

Step-Saver Data Systems Inc. v. *Wyse Technology*[10] was one of the earliest cases of significance. The 3rd Circuit Court upheld the validity of a shrinkwrap agreement between two businesses. Other courts, however, have refused to enforce shrinkwrap agreements, considering them to be invalid. In *Vault Corp.* v. *Quaid Software,* [*Vault*][11] the 5th Circuit Court refused to enforce the terms of a licence agreement because some terms of the agreement were preempted by federal copyright and patent law. At the district court level, it was stated that the shrinkwrap licence was a contract of adhesion that was only enforceable if the Louisiana statute, explicitly validating the shrinkwrap licence, was valid and not preempted by federal copyright law. The Court concluded the Louisiana statute was not valid, at least to the extent that its provisions were contrary to federal copyright policy on the prohibition of copying for any purpose and prohibition on reverse engineering.

More recently, in *ProCD, Inc.* v. *Zeidenberg,* [*ProCD*][12] it was held that a shrinkwrap licence was binding on the purchaser. In this case, the purchaser had notice of the licence terms as there was a disclaimer on the outside of the box indicating the transaction was subject to a software licence. Under the terms contained inside the box, the purchaser had a right to return the software if the terms were unacceptable. The Court noted that shrinkwrap licences are enforceable as a general matter unless their terms are objectionable on grounds applicable to contract, such as violation of a rule of positive law or unconscionability.

There remains little doubt that EULAs can be enforced by courts subject only to substantive contract law. An agreement may be unenforceable if it breaches the established rules of contract law, such as unconscionability.[13] Clearly, questions remain about the enforceability of properly drafted shrinkwrap, clickwrap and browsewrap agreements, although many jurisdictions have upheld their enforcement. For the time being, browsewrap and shrinkwrap

---

[10] 939 F.2d 91 (3rd Cir. 1991).

[11] 847 F.2d 255 (5th Cir. 1988) [*Vault*].

[12] 86 F.3d 1447 (7th Cir. 1996) [*ProCD*].

agreements should be used cautiously. Historically, shrinkwrap agreements have not been upheld, but since the *ProCD* decision they are more likely to be endorsed by the courts. Future cases will determine whether *ProCD* has set precedence for upholding the contractual validity of shrinkwrap agreements. Since the *ProCD* decision in 1996, a similar case has yet to be tried. Ultimately, clickwrap agreements should be the preferred method wherever possible to ensure the EULA creates a binding online contract.

In the marketplace, clickwrap agreements are currently limited to online software programs. In the near future, it is likely there will be a shift to an increasing use of clickwrap agreements. Based on recent case law and the enforceability of this form of agreement, companies will expand their use. It is foreseeable that technology will be designed for game consoles and software computer games that require users to actively assent to the terms of EULAs. In order to maximize enforceability of EULAs, companies may continue usage of browsewrap and shrinkwrap agreements, but will also require end users to assent to a clickwrap agreement before using their products.

Part 2: How EULAs Are Limiting End User Rights

EULAs often contain extensive terms that attempt to highly limit consumer rights. For example, common EULAs prohibit consumers from criticizing products publicly or from reverse engineering a product. Many EULAs include terms that provide for automatic software updates and installations, while disclaiming any liability for faulty products or products that do not operate as advertised. Manufacturers also commonly reserve the right to change their EULA, without notice to the consumer, deeming that continued use of the product constitutes acceptance of the additional terms. Not only are consumers required to agree to all the onerous terms listed, but also agree to any contractual terms that may be added in the future. These terms directly conflict with many legal rights including freedom of speech, product liability, privacy rights, security rights and intellectual property rights.

There continues to be considerable debate and uncertainty amongst the legal community about what terms will be enforced by the courts. The following review of current law will provide some insight into the validity and enforceability of two specific provisions found within EULAs: unilateral change to the EULA and reverse engineering.

Unilateral Change to the EULA

Many EULAs contain a term providing that the user consents to all future changes in the agreement including any new rules, policies, terms or conditions on use of service. Furthermore, the user's continued use of the product constitutes acceptance of these new terms, regardless of whether he or she has received notice. By agreeing to this provision, users are agreeing to any future terms that may appear in the agreement, which amounts to a unilateral alteration to the contract.

The Ontario Superior Court, in *Kanitz* v. *Rogers Cable Inc.*,[14] affirmed that unilateral changes to the service agreement were valid and binding on the user. The plaintiffs commenced a class action prompted by service difficulties they experienced with their high-speed Internet access. Prior to installation of service, customers were required to sign a user agreement, which included a provision providing that the agreement could be amended at any time and that customers would be notified of changes on the defendant's Web site, through e-mail or by post. Rogers argued that the class action should be dismissed because the user agreement provided for arbitration as the exclusive dispute resolution mechanism. The original online user agreement did not state that disputes must be resolved through arbitration but had been updated to include this clause. The change was posted on the Web site within the EULA, along with a notice that the agreement had been amended. The plaintiffs argued that the amending provision amounted to a unilateral imposition of terms, which the Court should not sanction. They also argued that they did not have sufficient notice of the revised terms because Rogers did not provide notice by e-mail or postal mail and therefore, it should not be binding on the subscribers. The Court concluded that adequate notice was provided and they were bound by the terms when they continued to use the defendant's service.

There will always be exceptions to this finding and each future case will be evaluated on its own merits, although this decision regarding an amending provision places onerous obligations on users to frequently check the Web site for any changes or amendments. Where a user agreement provides that it may be amended at any time, continued use of service after posting the amendment will normally

---

[14] (2002), 58.O.R. (3d) 299 (Ont. Sup. Ct.) [*Kanitz*].

constitute deemed acceptance of that amendment, despite absence of an express agreement to the unilateral change.

Reverse Engineering

Reverse engineering is the process of beginning with a finished product and working backwards to figure out how the product was made and how it operates. The fair use doctrine[15] is an aspect of Canadian[16] and American[17] copyright law that provides for the use of copyrighted material in another author's work.[18] Section 107 of the US *Copyright Act* states that "the fair use of a copyrighted work, including such use by reproduction in copies … for purposes such as criticism, comment, new reporting, teaching, scholarship or research, is not an infringement of copyright".[19] Copyright law is aimed at protecting an author's expression. It does not confer unlimited protection and privileges, but is designed to reward individuals for their creation, in order to benefit the public as a whole. Copyright will protect creativity in video games and software but will not extend protection to all

---

[15] The fair use doctrine is known as the fair dealings defence in Canada. The Canadian fair dealing defence is substantially similar to the American fair use doctrine. See Robert G. Howell, "Reformulation of Copyright by the Supreme Court of Canada: *Théberge, CCH* and *Tariff 22*" (Paper presented at the Intellectual Property Law symposia in Vancouver, BC, June 2004) [unpublished] for further discussion on the similarities between American and Canadian fair use/dealing exceptions.

[16] *Copyright Act*, R.S. 1985, c. C-42, s. 29.

[17] *Copyright Act*, 17 U.S.C. § 107.

[18] The Supreme Court of Canada recently established the application of the fair dealing exception in Canadian copyright law in *CCH Canadian Ltd.* v. *Law Society of Upper Canada,* 2004 SCC 13. The Supreme Court of Canada did not address the scope of the fair dealings defence in relation to reverse engineering. The most recent case law on reverse engineering and copyright protection is from the United States. Therefore, given the similarities between the copyright Acts in Canada and in the United States, this paper will focus on the application of the fair use doctrine in American case law.

[19] *Supra* note 17.

functional aspects of those products. Reverse engineering has been widely accepted as a legal fair use of copyrighted material.[20]

To prove copyright infringement, the plaintiff must show ownership of a valid copyright and that copying of protected expression took place. The fair use defence allows courts to maneuver around the strict application of copyright laws. Fair use has been defined as a "privilege in others than the owner of the copyright to use the copyrighted material in a reasonable manner without his consent."[21] This defence provides for creativity, which copyright laws are designed to foster. Courts must decide the applicability of the fair use defence on a case-by-case basis in light of the purpose of that doctrine and the *Copyright Act*.

The *Sega* v. *Accolade,* [*Sega*][22] and *Sony* v. *Connectix Corporation,* [*Sony*][23] decisions clearly show that reverse engineering is considered fair use so long as that use is aimed at understanding the technology in order to facilitate further technological advancement. The issue raised in *Sony* was whether the intermediate copying of software during the reverse engineering process should be considered fair use under the *Copyright Act* when the final product contains no infringing code. It was determined that the intermediate copying was necessary. The Court found that Connectix reverse engineered a product that would be compatible with games designed for the Sony PlayStation and that purpose was legitimate under the first statutory factor of the fair use analysis. The Court also concluded that the end product did not contain any code that infringed on Sony's copyright (although it noted that this factor is of little weight). The final factor was the effect on the market for the Sony PlayStation. Connectix's game console was a new platform for PlayStation games. It was likely that Sony would sustain economic losses on the sale of their PlayStation consoles,

---

[20] This was affirmed in *Sega* v. *Accolade* U.S. App. LEXIS 78 (9th Cir. 1993) and *Sony* v. *Connectix Corporation* 203 F.3d 596 (9th Cir. 2000).

[21] Derek Prestin, "Where to Draw the Line Between Reverse Engineering and Infringement: Sony Computer Entertainment, Inc v. Connectix Corp." (2002) 3 Minn. Intell. Rep. Rev. 137 (citing H. Ball, *Law of Copyright and Literary Property* 260 (1944)).

[22] 1993 U.S. App. LEXIS 78 (9th Cir. 1993) [*Sega*].

[23] 203 F.3d 596 (9th Cir. 2000) [*Sony*].

although it could actually increase sales for Sony games. This was insufficient to compel a finding that the fair use doctrine should not be applied. In *Sega*, it was determined that where there is a legitimate reason for a developer to study or examine unprotected functional aspects of a copyrighted program and where there are no other means to do so, the disassembly of the program is considered a fair use under the fair use doctrine.

The recent 8th Circuit Court decision in *Davidson*[24] established that EULAs can override protections under federal copyright law, including the fair use doctrine. An in-depth analysis of this decision evidences how far courts are willing to go to protect the sanctity of EULAs. *Davidson* dealt with the right to reverse engineer in order to build an open-source network game emulator. In order to play many popular Blizzard video games over the Internet (such as Diablo and Starcraft), gamers must connect through Blizzard's proprietary Battle.net service. The Battle.net mode of operation allows Blizzard games to be played online, using their servers. Dissatisfied with the occasional difficulties in Battle.net service, a group of independent programmers created a functional alternative to the plaintiff's online gaming service, known as bnetd. In order to design bnetd, the programmers created their own servers and reverse engineered Blizzard games and protocol from Battle.net to figure out how to get Blizzard games to operate on their servers. This information was used to give players access to the bnetd server. Battle.net servers contained a proprietary mechanism, which was not incorporated into the bnetd servers, that prevented pirated copies of Blizzard games from being played online. Yet once users began to play the game, there was no discernible difference from the standpoint of the participants in the online game. Blizzard sued the creators of bnetd for reverse engineering their products, claiming the programmers were in violation of the EULA.

The *Davidson* case differs from *Sega* and *Sony* because of the existence of a EULA. Blizzard's EULA contained a term expressly prohibiting reverse engineering of their products. The defendants in *Davidson* argued that even if the EULA is enforceable under contract law, it should not be enforced because it prohibits the fair use of Blizzard software. Their main argument was that reverse engineering is a fair

---

[24] *Supra* note 3.

use under copyright law and that copyright law overrides Blizzard's EULA. In *Davidson*, the Court concluded that contractual agreements that waive the right for users to reverse engineer products are valid and, therefore, the defendants waived their statutory rights by assenting to the EULA.

The *Davidson* case found that EULAs can override established intellectual property rights. This is not an astounding revelation. It is nothing new in the world of contracts that two parties can contract out of their legal rights. Parties have long been able to sign a contract that removes a privilege or right they otherwise would have had. For example, free speech can be explicitly contracted away through a gag order, or implicitly by doctors and lawyers. Courts have always been reluctant to set aside a contract created between two competent parties. Where rational, competent parties create a contract prohibiting reverse engineering, courts will not override that provision simply on the basis that it removes rights.

Debatably, this case was really more about issues of contract law rather than copyright law. According to the decisions in *Sega* and *Sony*, if there was no EULA, the programmers likely would not have been liable because the fair use defence would have been upheld. The problem was that the defendants in *Davidson* accepted the explicit agreement of terms, including the prohibition on reverse engineering. Arguably, the Court was essentially bound to uphold the sanctity of the EULA as an enforceable contract despite the defendant's attempts to circumvent it.

In reaching its decision, the Court reviewed the following cases. In *Vault*,[25] the District Court refused to enforce the terms of a licence agreement, ruling that the state *Software Licence Enforcement Act*, which prohibited reverse engineering, was preempted by federal law. In a more recent case, the Federal Circuit held in *Bowers* v. *Baystate Technologies, Inc.*[26] that a broad prohibition on reverse engineering in a shrinkwrap licence was enforceable and not preempted by the federal *Copyright Act*. The Court adopted the analysis of *ProCD*[27] in holding

---

[25] *Supra* note 11.

[26] 68 Fed. Appx. 966 (Fed. Cir. 2003).

[27] *Supra* note 12.

that parties may contract out of the rights provided in the *Copyright Act*.[28] The Court in *Davidson* distinguished the ruling in *Vault*, finding that it simply stood for the fact that a state law prohibiting all copying is preempted by the *Copyright Act* and therefore does not apply to this situation. The Court found that the issue in this case was not one of conflicting laws, but rather involved contractual agreements.[29]

Many commentators have taken the *Davidson* ruling to stand for the fact that any reverse engineering of software and video games is now illegal. For example, Jason Schultz, a staff attorney for EFF who worked on the case, stated that "[the ruling] essentially shuts down any competitor's add-on innovation that customers could enjoy with their legitimately purchased products".[30] Members of the gaming community have suggested that the Court's decision makes it unlawful in most cases to reverse engineer any commercial software program, thus making it unfeasible to create new programs that interoperate with older ones. Future cases will dictate the accuracy of these opinions, although a close review of the judgment in *Davidson* seems to suggest this criticism may be overstated.

There was much more involved in this situation than simply the creation of an add-on innovation. Most importantly, the defendants reverse engineered protocols after expressly agreeing not to through acceptance of the EULA. They disassembled a Blizzard game to figure out how to implement password protections when creating an account in Battle.net mode, made an unauthorized copy of a Blizzard game to test the interoperability of their creation, redirected protocol, looked into Blizzard client files and performed data dumps. They also used a program to figure out how Blizzard games displayed ad banners so that people running the bnetd emulator could display ads in the same format and they took approximately 50 icons and symbols from the Battle.net site and built them into their server. Not only

---

[28] There was a strongly worded dissent in this case, arguing that shrinkwrap licences that override the fair use defence should be preempted by the US *Copyright Act*.

[29] *Supra* note 3 at 14.

[30] "Federal Court Slams Door on Add-On Innovation", September 1, 2005, online: EFF <http://www.eff.org/news/archives/2005_09.php>. (last accessed September 20, 2005).

were the Blizzard games designed to connect to Battle.net servers but once game play began, a user perceives no noticeable difference between Battle.net and bnetd. The programmers attempted to mirror all of the user-visible features of Battle.net, including online discussion forums and access to the programs computer code for others to copy and modify. The end result was that individuals using Blizzard games could play their game over the Internet via bnetd rather than Battle.net.[31] It is also important to note that the defendants were not average gamers. They were sophisticated programmers and, therefore, were not as likely to be subjected to an inequality in bargaining power. All of this may suggest that the average gamer who creates a game modification will not be prosecuted by game companies and, if they were, arguably the court would not reach the same conclusion.

The fact remains that the widespread use of EULAs today may essentially ban the use of reverse engineering to design new and improved products. It is not easily disputed that courts should protect the sanctity of contracts when entered into by two competent parties. Subsequently, if reverse engineering is an important tool, there must be another way to ensure its continued use. For example, legislation could be introduced to prohibit some of the terms found in EULAs, although this should only be done if the value of reverse engineering is greater than the value lost by not upholding private contracting.

A tension exists between the benefits and downfalls of reverse engineering, although it is a broad and important social interest. Technological innovation must be supported, but obviously game creators see value in prohibiting reverse engineering. If reverse engineering were allowed, game creators would spend more resources to protect their technology against use by others. This would increase overall costs, which would be passed on to the consumer. Conversely, reverse engineering has tremendous value and the ban of it results in negative consequences to society. Reverse engineering increases creativity, innovation and competition. Banning reverse engineering hinders technical innovation. Reverse engineering provides new and enhanced products for consumers. It also ensures that competitors

---

[31] Hear audio recordings of the oral arguments before the 8th Circuit Court of Appeals, online: EFF <http://www.eff.org/IP/Emulation/Blizzard_v_bnetd> (last accessed November 15, 2005).

are able to enter into the market. The effect of prohibiting all reverse engineering goes well beyond game publishers. It has clear positive outcomes for the economy, but for the meantime, it appears that courts are bound to uphold private contracts unless they are willing to strike down these onerous terms, possibly through a finding of unconscionability. The tension between reverse engineering and contracts must be balanced by the courts and the government. Future cases and potential legislation will determine the outcome.

Unconscionability

The defendants in *Davidson* argued that even if the EULA was a binding contract, it was an unconscionable contract and was therefore unenforceable.[32] One concern arising from the *Davidson* case was a potential inequality of bargaining power between the two parties. It was purported that the EULA was a contract of adhesion because it does not square with the reasonable expectations of the parties, as no member of the public would expect to pay for a game and then be unable to use it simply because they did not agree to the licence terms. No reasonable person would expect to be barred from installing a game unless he or she complied with the EULA.

The basic test applied for unconscionability is "whether, in light of the general background and the needs of a particular case, the clauses involved are so one-sided as to be unconscionable under the circumstances existing at the time of the making of the contract".[33] In the context of standard form contracts, unconscionability is characterized by the "absence of meaningful choice on the part of one party due to one-sided contract provisions, together with terms which are so oppressive that no reasonable person would make them and no fair and honest person would accept them".[34] In order to find the existence of unconscionability, both a procedural and a substantial element must be present. A sliding scale is used in applying these two elements, which allows for a greater degree of one element and a lesser degree of the other to result in a finding of unconscionability.

---

[32] This was argued in the District Court but was not at issue at the 8th Circuit level. See *Davidson* v. *Internet Gateway*, 334 F. Supp. 2d 1164 (D. Mo. 2004).

[33] Cal. Code 1670.5 (2004) Legis. Comm. Cmt. (1). Cited at 21 of *Davidson*.

[34] *Fanning* v. *Fritz's Pontiac-Cadillac-Buick*, 322 S.C. 399 (S.C. 1996).

Substantive unconscionability looks to the actual terms of the agreement, while procedural unconscionability focuses on the manner in which the contract was negotiated and the circumstances of the parties at the time of formation. Procedural unconscionability may be shown by either an inequality in bargaining power or unfair surprise. This may be evidenced by terms that are unreasonably favourable to one party, terms hidden in the contract, or where one party has substantially lower education levels. Substantive unconscionability may be shown by an overly harsh allocation of risks or unjustifiable costs or a great price disparity. Where a court finds that a contract or clause is unconscionable at the time it was made, it can refuse to enforce the contract or limit the application of that clause to avoid an unconscionable result.

The Court in *Davidson* ruled that the contract was neither procedurally nor substantially unconscionable. Unfortunately, a finding of unconscionability depends heavily upon the subjective preferences of individual courts. In concluding that the agreement was not procedurally unconscionable, the Court did not clearly explain its reasoning. It found unequal bargaining power between the parties but decided that there was no procedural unconscionability because there was no element of surprise surrounding the contract terms. The defendants were not "unwitting members of the general public", but were computer programmers and administrators familiar with the language used in the contract.[35] The Court affirmed its reasoning by stating that the defendants had the right to agree to the terms and play the game, return the game for a refund, or they could have selected a different game. However, the fact that other products are available on the market does not represent a meaningful choice for the defendants or any consumer, because almost all games contain a EULA with similar terms. If the defendants in this case were unwitting members of the general public, it is easy to conceive of them being surprised by the onerous terms of the EULA and the Court may have found the existence of procedural unconscionability.

The Court further failed to address why the contract was not substantively unconscionable, only stating that the EULA did not impose harsh or oppressive terms. According to the Court's definition of substantive unconscionability, the contract did not impose a one-

---

[35] *Supra* note 32 at 22.

sided result. It is undisputed that the EULA protects the economic and intellectual investments of the drafter. The creator of the EULA benefits from the agreement while binding the user to a number of strict terms, which are clearly not created for the benefit of that user.

Part III: Future Possibilities

Since the *Davidson* decision, the issue is no longer whether prohibition on reverse engineering can be a term of a contract in a EULA, as it clearly can be, but rather how far courts will go to uphold the rights of publishers in a EULA and where, if ever, they will find the agreement to be unconscionable. Consumers often do not understand how limiting EULAs are on their rights. Undoubtedly, online agreements are valid contractual agreements and parties are free to contract out of legal rights, but at what point will the courts see that consumers have no other option but to agree to the contract? In today's marketplace, if consumers wish to use software, there is no real meaningful choice; they must assent to the terms of the EULA, and in their current state, these agreements are severely limiting consumers' rights.

It should be noted that the *Davidson* Court may have lacked a true understanding of the gaming community. The Court disproved of the fact that bnetd was not created for commercial purposes since the defendants did not attempt to profit financially from their creation.[36] The defendant's goal is common in the gaming world; they created a product to improve the gaming experience. They were simply frustrated with the poor service provided on the Blizzard server. It was not mentioned in the case, but the decision seems to infer that since there was no commercial purpose, the defendants were engaged in a malicious act directed towards Blizzard in an attempt to cut into their market share. That seems to be the only logical explanation as to why the Court would even point out the fact that the server was not created for commercial purposes. This appears to be one example of how out of touch the Court was with the video game world and the purpose of creating modifications. Viewed from another standpoint, this leaves open the possibility that future cases may be decided differently, providing more protection to the end user, as the legal

---

[36] *Supra* note 3 at 18.

community increases their understanding of modifications and the gaming community as a whole.

The *Davidson* ruling also seems to leave open some possibility that future cases may hold certain terms of a EULA to be unconscionable, particularly where the user is an "unwitting member of the general public".[37] In most situations, the EULA will not affect average consumers or influence their purchasing decisions, nor will it have any lasting effect on their lives. This presents the current problem that publishers can use EULAs to suppress minority rights, such as the right to reverse engineer, and only a limited number of people will be affected. Ideally, as the general public learns more about EULAs and how they are being used to deprive consumers of basic rights they may take for granted, future challenges may well become more common. As one article analogized,

> [m]any people treat EULAs with the same reverence they do the tags on mattresses that say, '*Do not remove this tag under penalty of law.*' They scoff at the idea that anyone could enforce such a bizarre rule. Increasingly, however, we are seeing consumers and software developers threatened with lawsuits for engaging in the digital equivalent of ripping tags off a mattress.[38]

The question remains: How will the seminal outcome in *Davidson* affect the software world?[39] Predictably, we will see an increase in the use of clickwrap agreements to present EULAs, as *Davidson* has authenticated their validity. Perhaps this case will not have a long-term negative impact on the ability of gamers to create new game innovations from existing products. Rather, it may represent the need for more certainty and parameters around the use of EULAs. Reverse

---

[37] *Supra* note 32 at 22.

[38] Annalee Newitz, "Dangerous Terms: A User's Guide to EULAs", online: EFF <http://www.eff.org/wp/eula.php> (last accessed October 20, 2005).

[39] For an interesting audio discussion of what the Blizzard decision means for open-source programmers, technologists and consumers, see the following link for a radio recording with University of Pittsburgh law professor Michael Madison and programmer Seth Finkelstein. Online: IT Conversations <http://www.itconversations.com/shows/detail259.html> (last accessed Nov. 15, 2005).

engineering is a vital function. This is clearly recognized by the legislators, as it was found to be an important use and, therefore, was not prohibited by intellectual property laws. It appears the Court in *Davidson* was essentially bound to uphold the entrenched laws of contract. So now it is up to the legislator and end users to respond.

Little doubt remains that EULAs are enforceable in virtually all domains of commercial activity. These agreements form contracts of adhesion; they heavily restrict one party while leaving the other party free. The result is a decrease in end user rights, where the actions a user may take are severely limited. In the meantime, it appears as though publishers have extensive protection on their products and can use EULAs to prohibit any activity related to the software platform that they have not specifically authorized. Future cases and possible legislation will bring further clarity to the scope of EULAs. For now, consumers and programmers should be aware of the importance and possible consequences of consenting to EULAs.