Internet Law:
Cases and Problems

James Grimmelmann
Associate Professor of Law
New York Law School

Semaphore
PRESS

www. semaphorepress.com

For my parents.

Internet Law: Cases and Problems

James Grimmelmann

Copyright and Your Rights:

We ask that you not resell or give away your copy. Please direct people who are interested in obtaining a copy to the Semaphore Press website, www.semaphorepress.com, where they can download their own copies. The resale market in the traditional casebook publishing world is part of what drives casebook prices up to $150 or more. When a publisher prices a book at $150, it is factoring in the competition and lost opportunities that the resold books embody for it. Things are different at Semaphore Press: Because anyone can get his or her own copy of a Semaphore Press book at a reasonable price, we ask that you help us keep legal casebook materials available at reasonable prices by directing anyone interested in this book to our website.

Printing A Paper Copy

If you would like to have a printed copy of the book in addition to the electronic copy, you are welcome to print out a copy of any part, or all, of the book. Please note that you will find blank pages throughout the book. We have inserted these intentionally to facilitate double-sided printing. We anticipate that students may wish to carry only portions of the book at a time. The blank pages are inserted so that each chapter begins on a fresh, top-side page.

Finding Aids and Annotations

Finally, please note that the book does not include an index, a table of cases, or other finding aids that are conventional for printed books. This is because a Semaphore Press book, in pdf form, can be searched electronically for any word or phrase in which you are interested. With the book open in Adobe Reader, simply hit control-f (or select the "find" option in the "Edit" pull-down menu) and enter the search term you want to find. We also enable Reader's commenting features in our pdf books, so you can highlight text, insert comments, and personally annotate your copy in other ways you find helpful. If your copy of Reader does not appear to permit these commenting features, please check to make sure you have the most recent version; any version numbered "8" or higher should permit you to annotate a Semaphore Press book.

INTERNET LAW: CASES AND PROBLEMS

James Grimmelmann

TABLE OF CONTENTS **BOOK PAGE #**

CHAPTER 5: ACCESS TO COMPUTERS

This chapter describes the various legal theories that owners and operators of servers can use to control how users are allowed to access those systems. A user who does what the server owner disapproves of might be breaching a contract, committing a crime, or committing a tort. Each of these three bodies of law has confronted the problem of access to computer systems by drawing on its own traditional categories, and evolved according to its own logic. It is not clear that the results are logical or consistent: what is legal behavior under one may be a serious wrong under another. Complicating matters even further, the categories draw on each other. The scope of "authorized" access under the Computer Fraud and Abuse Act, for example, may depend on the enforceability of a contract between the server owner and the user. As you read the following materials, be alert to the ways in which clever lawyers take advantage of this doctrinal ambiguity by seeking ways to frame a dispute using the legal categories that most favor their clients.

I. Contracts

Our first source of potential legal control over servers is contract law. The courts here are applying what appear at first to be standard, elementary doctrines of contract law. Read closely, though: is there anything unusual about the courts' reasoning?

A. Contracting via Computer

The mechanics of contract formation should be familiar to you from your first-year course in contract law. Rules on offer and acceptance, parol evidence, and modifications were created long before electronic computers and the Internet. The following case illustrates some of the issues involved in translating them to a new factual context.

CX Digital Media, Inc. v. Smoking Everywhere, Inc.

No. 09-62020-CIV (S.D. Fla. Mar. 23, 2011)
2011 U.S. Dist. LEXIS 29999, 2011 WL 1102782

Altonaga, District Judge: …

I. FINDINGS OF FACT

Defendant, Smoking Everywhere Inc. ("Smoking Everywhere"), sold through its website an alternative to regular cigarettes called "electronic cigarettes," "E-Cigarettes," or "E-Cigs." To generate web traffic to its site and increase sales of E-Cigs, Smoking Everywhere approached Plaintiff, CX Digital Media, Inc. ("CX Digital"), about a free-trial offer that Smoking Everywhere wanted to promote.

CX Digital provides "advertising solutions" through "affiliate marketing." More simply put, CX Digital acts as a middleman between its network of affiliates or "third-party publishers," who purchase or provide advertising on the internet ("CX [Affiliates]"), and businesses that want to advertise online ("CX Client[s]"). How this works in practice is a bit technical.

CX Digital has relationships with approximately 10,000 independent affiliates. These affiliates are typically small entrepreneurs who purchase advertising space on web sites, social media sites, or who do direct emailing. When CX Digital enters an agreement called an "insertion order" with a new Client, CX Digital may work with the Client to design a campaign and to design appropriate web pages for the campaign.

CX Digital makes the Client's campaign available to CX Affiliates, who place advertisements for the CX Client's campaign. Each of the advertisements is clickable.

When a consumer sees the ad, becomes interested in the product or service, and clicks on the advertisement [the consumer's browser loads a webpage from CX Digital's server, while also setting a cookie on the user's computer to track which CX Affiliate's ad the consumer clicked on].

Upon arriving at the CX Digital server, CX Digital records which affiliate's advertisement was clicked on by the consumer. The consumer is then redirected to the Client's "landing page," which contains the campaign offer details and a link to purchase the Client's product or service. … The completion of a Sale triggers two obligations. First, the Client owes CX Digital the unit price for a Sale, and second, CX Digital owes its referring affiliate a payment for a completed Sale. CX Digital pays its affiliates, usually on a weekly basis, even if it has not received payment from the Client.

On August 4, 2009, Nick Touris, the vice-president of advertising for Smoking Everywhere , entered an agreement, entitled Insertion Order #6921, with CX Digital on behalf of Smoking Everywhere. In the Insertion Order, Smoking Everywhere promised to pay $45.00 to CX Digital for each completed Sale of the "Gold E-Cigarette Kit Free-Trial." The term "Sale" is defined by the Insertion Order as "a consumer who accesses the content via a CX Digital link and completes a one-page registration consisting of: filling in the appropriate field of information and successful credit card submi[ssion] . . . . No further action will be required from the consumer for the [cost per action] to be payable."

During the month of August, CX Digital provided 670 Sales pursuant to the Insertion Order. CX Digital never provided more than 200 Sales on any given day in August; from August 13, 2009 until August 31, 2009, the average number of Sales per day was about 39. …

On September 2, 2011, Touris and Pedram Soltani, an account manager at CX Digital, engaged in a day-long instant-message conversation covering a number of topics … After [discussing other topics] Soltani began a conversation about increasing the number of Sales CX Digital was sending Smoking Everywhere:

> pedramcx (2:49:45 PM): A few of our big guys are really excited about the new page and they're ready to run it
>
> pedramcx (2:50:08 PM): We can do 2000 orders/day by Friday if I have your blessing
>
> pedramcx (2:50:39 PM): You also have to find some way to get the Sub IDs working
>
> pedramcx (2:52:13 PM): those 2000 leads are going to be generated by our best affiliate and he's legit
>
> nicktouris is available (3:42:42 PM): I am away from my computer right now.
>
> pedramcx (4:07:57 PM): And I want the AOR when we make your offer #1 on the network
>
> nicktouris (4:43:09 PM): NO LIMIT
>
> pedramcx (4:43:21 PM): awesome!

The same day as this conversation, the number of Sales per day that CX Digital sent to Smoking Everywhere began to increase substantially. Between September 2, 2009 and September 23, 2009, CX Digital sent an average of 1,244 Sales per day, with a peak of 2,896 Sales on September 22, 2009. …

At the end of September, CX Digital sent a second invoice for both August and September 2009. That invoice demanded that Smoking Everywhere pay a balance of $1,339,419.00 upon receipt. That figure included a price increase from $45.00 to $51.00

per Sale for 17,294 Sales between September 14 and 23, 2009.[7] CX Digital acknowledges that Smoking Everywhere paid a $5,000.00 deposit when it entered the Insertion Order. Accordingly, CX Digital asserts Smoking Everywhere owes it $1,260,805.00, which Smoking Everywhere has not yet paid. The Complaint contains one count alleging breach of contract, and in addition to compensatory damages, seeks attorney's fees pursuant to the Insertion Order.

II. Conclusions Of Law

A. The Insertion Order

Smoking Everywhere does not dispute it signed the Insertion Order and that the Insertion Order constitutes a valid contract between CX Digital and Smoking Everywhere. …

Smoking Everywhere also contends that, beginning in early September, CX Digital breached the Insertion Order by sending more than 200 Sales per day … CX Digital does not dispute it engaged in this conduct, but it argues it was performing in accordance with the modified Insertion Order. Because Smoking Everywhere's allegations of breach by CX Digital turn on whether there was an enforceable modification to the Insertion Order, these arguments are addressed below in the discussion of the alleged changes.

B. Modification of the Insertion Order

The central dispute in this case is whether the Insertion Order was modified to permit an unlimited number of leads … This raises two questions: (1) did Touris and Soltani agree to modify the Insertion Order during their September 2, 2009 instant-message conversation; and if so, (2) is their agreement to modify the contract enforceable?

1. *Agreement to Modify Insertion Order*

CX Digital contends the September 2, 2009 instant-message conversation between Touris and Soltani … eliminated the 200-Sale-per-day limit. "The manifestation of assent may be made wholly or partly by written or spoken words or by other acts or by failure to act." Restatement (Second) Contracts § 19 (1981). Under Delaware law, "overt manifestation of assent – not subjective intent – controls the formation of a contract; [and] the 'only intent of the parties to a contract which is essential is an intent to say the words or do the acts which constitute their manifestation of assent'; . . . 'the intention to accept is unimportant except as manifested.'" *Indus. Am., Inc. v. Fulton Indus., Inc.*, 285 A.2d 412, 415 (Del. 1971) (quoting Restatement § 20). …

In the "Campaign Details" section on the first page of the Insertion Order, the term "VOLUME:" appears in bold type followed by "200 leads/day." CX Digital contends Touris and Soltani agreed to remove the limit on the number of leads or Sales per day during their September 2, 2009 instant-message conversation.

After the discussion between Touris and Soltani about switching the URLs, Soltani sends an offer to Touris: "We can do 2000 orders/day by Friday if I have your blessing . . . . [a]nd I want the AOR when we make your offer number one on the network." Touris responds, "NO LIMIT." CX Digital argues that Touris accepted Soltani's offer by saying "NO LIMIT." The Court agrees a contract was formed but clarifies that Touris's response acted as a rejection and counter-offer that Soltani accepted by then replying "awesome!"

"In order to constitute an 'acceptance,' a response to an offer must be on identical terms as the offer and must be unconditional." *PAMI-LEMB I Inc. v. EMB-NHC, L.L.C.*, 857 A.2d 998, 1015 (Del. Ch. 2004). "A reply to an offer which purports to accept it but is conditional on the offeror's assent to terms additional to or different from those offered

[7] CX Digital is not seeking to recover the additional $6.00 per Sale in this litigation.

is not an acceptance but is a counter-offer." Restatement § 59; see also *PAMI-LEMB I*, 857 A.2d at 1015 n.80. "The words and conduct of the response are to be interpreted in light of all the circumstances." *PAMI-LEMB I*, 857 A.2d at 1015 n.81.

Here, Touris's response of "NO LIMIT" varies from the two specific terms Soltani offered and so acts as a counter-offer. Soltani proposed CX Digital provide 2,000 Sales per day and that CX Digital be the AOR or agent of record, a term of art meaning the exclusive provider of affiliate advertising on the advertising campaign. Touris makes a simple counter-offer that there be no limit on the number of Sales per day that CX Digital's affiliates may generate and makes no mention of the AOR term. Soltani enthusiastically accepts the counter-offer by writing, "awesome!" and by beginning to perform immediately by increasing the volume of Sales.

Touris testified he could have been responding to something other than Soltani's offer of 2,000 Sales per day when he said "NO LIMIT." Touris acknowledged that he had engaged in contract negotiations about "changing the number of leads, changing URLs, deposits, that type of thing" although he added, "we mainly spoke on the phone. A little bit of email but I had trouble receiving his emails so I mean we used Instant Messaging but you know there was a lot more than what was presented here, last court appearance." The implication of this testimony was that Touris could have been responding to something else he and Soltani had discussed by phone. But when pressed on just what else he could have been referring to when he said "NO LIMIT," Touris's memory failed him. In particular, he denied that "NO LIMIT" was some kind of personal motto.[15]

Indeed, neither Touris nor [Smoking Everywhere president Elicko] Taieb ever suggested any plausible alternative interpretation for why Touris wrote "NO LIMIT" to Soltani, nor did they explain the content of the alleged additional negotiations that took place outside of the September 2, 2009 instant messages or what effect those would have had on the apparent agreement the parties reached on September 2nd. Considering Touris's admission that he was engaged in instant-message negotiations with Soltani about changing the number of leads along with the September 2nd instant-message transcript, directs the conclusion that those negotiations, wherever and however they occurred, culminated with a modification of the Insertion Order when Touris and Soltani agreed to "NO LIMIT."

Smoking Everywhere also observes that a significant amount of time – almost two hours – passed between Soltani's offer of 2,000 Sales per day and Touris's counter-offer of "NO LIMIT," which it suggests adds uncertainty to the meaning of the conversation. However, more than an hour passes before Soltani added that he would like CX Digital to be the AOR; yet this is clearly part of Soltani's offer. It is then only thirty-four minutes later that Touris responds "NO LIMIT." Given that Touris testified he would not have approved such an increase without first discussing it with Taieb, one explanation for the time delay, if one is needed, is that Touris was doing just that – asking Taieb for approval.[16]

2. *Enforceability of the Modifications*

Smoking Everywhere contends that even if it and CX Digital agreed to modify the Insertion Order, the modification is not enforceable for several reasons. First, an oral modification of a contract must be proven with "specificity and directness." Second, the

[15] It is clear from Soltani's "awesome!" reply that Soltani interpreted Touris's statement as a direct response to the offer to increase the number of Sales. Moreover, Touris does not react to or correct Soltani's exclamation of "awesome!" in any way that would indicate confusion about the subject matter of their discussion. Indeed, the conversation reads most naturally when understood as two people negotiating and reaching a modification of an existing agreement.

[16] Moreover, anyone who has used an instant-message application in an office setting will recognize these time lags between responses as typical of the medium.

language of the Insertion Order provides that it "may be changed only by a subsequent writing signed by both parties," and Smoking Everywhere did not waive this provision. Third, "the Defendant did not give the required consideration for any modifications to the initial insertion order, thus the alleged changes to the insertion order are not enforceable." Fourth, Touris lacked the authority to bind Smoking Everywhere. Lastly, Smoking Everywhere also raises the defenses of commercial frustration, violation of the implied covenant of good faith and fair dealing, and mutual mistake. These defenses are addressed in turn.

a. Specificity and Directness

Drawing from Delaware case law, Smoking Everywhere contends "[a] party asserting an oral modification must prove the intended change with 'specificity and directness as to leave no doubt of the intention of the parties to change what they previously solemnized by formal document.'" *Cont'l Ins. Co. v. Rutledge & Co.*, 750 A.2d 1219, 1230 (Del. Ch. 2000). In particular, Smoking Everywhere relies on *Reserves Dev. LLC v. Severn Sav. Bank, FSB,* No. 2502-VCP, 2007 WL 4054231, at *10 (Del. Ch. Nov. 9, 2007). The court in that case found a series of emails in the "record [was] not sufficiently 'specific and direct' to support a conclusion that the parties orally modified an existing written contract." *Id.* Smoking Everywhere contends that in this case, the instant messages between Touris and Soltani are not specific and direct enough evidence that it agreed with CX Digital to modify the Insertion Order. …

The agreement to modify the Insertion Order to remove the limit is also supported by specific and direct evidence. As discussed, during the September 2nd instant messages, Touris made a counter-offer of "NO LIMIT" in response to Soltani's offer of 2,000 leads per day with AOR status for CX Digital. Soltani accepted the counter-offer. This modification clearly changed the "VOLUME" term in the details contract of the Insertion Order from 200 per day to unlimited. The language in the instant messages and the increase in the volume of leads that immediately follows provide specific and direct support that the change was intended.

Moreover, the *Severn Savings* case is easily distinguished from this case. … First, the scope and complexity of the modifications alleged in *Severn Savings* far exceed the narrow and straightforward changes here. The emails in *Severn Savings* showed the parties discussing potential payment arrangements on two letters of credit, but evidence of an agreement "to change the party responsible for effectuating construction of the infrastructure" was only "sketchy" and "muddled." Id. at *9–10. Reading the emails excerpted in Severn Savings, one has the impression that the parties had discussed different options orally, but never reached any agreement. The emails were a continuation of the oral negotiations that tried to pin down the details of the parties' obligations. In this case, although there may have been conversations by phone, … once the limit was removed on the number of Sales per day, CX Digital began to send more – no further negotiation was needed. The instant messages therefore, rather than showing continued debate like the emails in *Severn Savings*, show the parties had come to an agreement.

Second, the emails in *Severn Savings* were provided as evidence of an oral modification that had specific terms, not as a record of those specific terms. Here, the instant messages operate collectively as an unsigned writing containing the terms of the agreement to modify the Insertion Order. CX Digital is not alleging there are additional oral terms to the modification that are not evident from the instant messages. In fact, unlike in *Severn Savings*, Smoking Everywhere and CX Digital do not argue about what the specific terms of the alleged modification are, but about whether the modification actually occurred. As already discussed, the instant-message conversation and the parties' conduct surrounding it provide specific and direct evidence the parties agreed to modify the Insertion Order.

b. The Signed-Writing Clause

The Insertion Order provides it "may be changed only by a subsequent writing signed by both parties." Delaware follows the common law rule with respect to "no oral-modification clauses" or signed-writing clauses.[19] The common law rule is that "an oral agreement is sufficient to modify or rescind a written contract, notwithstanding a provision in the written contract purporting to require that subsequent modifications be evidenced by writing." WILLISTON ON CONTRACTS § 29.42 (4th ed. 1999). On this point, the Supreme Court of Delaware has held:

> We think, therefore, that a written agreement between contracting parties, despite its terms, is not necessarily only to be amended by formal written agreement. We agree with [*Bartlett v. Stanchfield,* 148 Mass. 394 (1889),] that a written agreement does not necessarily govern all conduct between contracting parties until it is renounced in so many words. The reason for this is that the parties have a right to renounce or amend the agreement in any way they see fit and by any mode of expression they see fit. They may, by their conduct, substitute a new oral contract without a formal abrogation of the written agreement. We think the existence of Paragraphs 16 in the plaintiffs' appointments does not prohibit the modification of making of a new agreement by conduct of the parties, despite a prohibition of Paragraphs 18 against any change except by written bilateral agreement.

Pepsi-Cola Bottling Co. of Asbury Park v. Pepsico, Inc., 297 A.2d 28, 33 (Del. 1972). In this case, the modification was not oral, but appeared in writing in an instant-message conversation. Nevertheless, the same principle applies to this informal, unsigned writing as to an oral modification. Therefore, the instant-message conversation, as an unsigned writing, suffices under Delaware law to modify the Insertion Order despite the signed-writing clause and notwithstanding the Court's preliminary observation stated during the trial.

Nevertheless, even if the instant-message conversation did not qualify as an enforceable modification under Delaware law and the signed-writing clause of the Insertion Order were enforceable, Smoking Everywhere would have waived the provision because, following the instant messages, CX Digital materially changed its position in reliance on Touris's statements. "[W]here, following the oral modification, one of the parties materially changes position in reliance on the oral modification, the courts are in general agreement that the other party will be held to have waived or be estopped from asserting the no oral modification clause." WILLISTON § 29:42.

There is no dispute that after the September 2nd instant-message conversation between Touris and Soltani, CX Digital began to send an increased number of Sales to two new URLs. CX Digital did this because it believed Touris had agreed with Soltani to modify the Insertion Order; that is, CX Digital relied on the instant messages to change the course of its performance. As discussed, Smoking Everywhere was aware of both changes and did not complain. Accordingly, Smoking Everywhere is estopped from asserting the signed- writing provision of the Insertion Order as a defense.

III. DAMAGES

CX Digital is entitled to damages pursuant to the Insertion Order as modified by the September 2nd instant messages. This includes payment for up to 600 Sales per day prior to September 2, 2009, and to an unlimited number of Sales per day after September 2, 2009. CX Digital through its affiliates, completed or caused to be

[19] The common-law rule applies because this a contract for the sale of services, not goods. Therefore, Delaware Code § 2-209, derived from the Uniform Commercial Code and permitting a signed- writing requirement, does not apply.

completed 670 Sales before September 2, 2009, and 27,459 Sales during the remainder of September 2009. CX Digital is entitled to $45.00 for each of those Sales. This totals $30,150.00 for the 670 Sales completed prior to the modification and $1,235,655.00 for the 27,459 Sales completed after the modification. Smoking Everywhere paid a $5,000 deposit toward the balance. Therefore, Smoking Everywhere owes CX Digital $1,260,805.00.

Pursuant to the Insertion Order, CX Digital is entitled to 1.5% interest per month on the $25,150.00 August 31, 2009 invoice accruing from September 15, 2009. CX Digital is also entitled to 1.5% interest per month on the balance of $1,240,655.00 accruing from October 15, 2009. (See Insertion Order ¶ 3). CX Digital is also entitled to all attorney's fees and costs related to the enforcement of the Insertion Order. (See id. ¶ 3).

Questions

1. Smoking Everywhere ends up owing $1,260,805.00, plus interest, attorneys' fees, and court costs – all based on the instant message "NO LIMIT". How much is that per character? Is this the most expensive instant message ever sent?

2. The court treats Touris's instant messages as "unsigned writings." Is that correct? Could you make an argument that they are oral communications, not writings? Could you make an argument that they are signed?

3. People conduct business in all kinds of media: in person, by letter, on the phone. What would have been the result if Touris and Soltani had their conversation in one of these other media? Which of these does an instant-message conversation most closely resemble? What result if they had exchanged emails or SMS messages instead? How much should the enforceability of contracts turn on the details of the particular medium the parties use?

4. Note that the quoted exchange consists of eight messages exchanged over the course of two hours, and one of them is an away message. Is the court's discussion of these gaps persuasive?

5. Suppose that CX Digital had *not* removed the sales limit after this conversation. Without the reliance argument, would the court have reached the same result? On the other hand, what if the conversation had been missing the final "awesome!" but CX Digital had removed the limit anyway?

6. There is an evidentiary issue lurking in the background of this case. How did CX Digital prove the contents of the conversation? What would have happened if Smoking Everywhere had alleged that the whole thing was a forgery by CX Digital?

7. This case provides a window onto the world of affiliate marketing. What is the relationship among Smoking Everywhere, CX Digital, CX Affiliates, and the websites where the ads appear? Who pays whom? Why would Smoking Everywhere use this kind of decentralized advertising, rather than, say, renting billboards or buying banner ads on popular websites directly?

8. An award of attorneys' fees to the prevailing party is unusual. Where does the court obtain the authority to provide this remedy?

B. Form Contracts

The issues posed by standardized form contracts have been well known for decades. But on the Internet, such issues are almost inescapable. Because the Internet enables near-strangers to meet and interact, it makes sense that one of the things they will do is enter into commercial relationships. Cheap and instant mass-market contracts would appear to be an obvious complement to cheap and instant communications. But for precisely the same reason, perhaps offerors will be tempted to overreach in claiming that a contract has been formed by virtue of online interactions. Keep these advantages and disadvantages in mind as you read the cases in this section.

ProCD, Inc. v. Zeidenberg

86 F. 3d 1447 (7th Cir. 1996)

Easterbrook, Circuit Judge: …

I.

ProCD, the plaintiff, has compiled information from more than 3,000 telephone directories into a computer database. We may assume that this database cannot be copyrighted … ProCD sells a version of the database, called SelectPhone™, on CD-ROM discs. (CD-ROM means "compact disc – read only memory."[)] The "shrinkwrap license" gets its name from the fact that retail software packages are covered in plastic or cellophane "shrinkwrap," and some vendors, though not ProCD, have written licenses that become effective as soon as the customer tears the wrapping from the package. Vendors prefer "end user license," but we use the more common term.) A proprietary method of compressing the data serves as effective encryption too. Customers decrypt and use the data with the aid of an application program that ProCD has written. This program, which is copyrighted, searches the database in response to users' criteria (such as "find all people named Tatum in Tennessee, plus all firms with 'Door Systems' in the corporate name"). The resulting lists (or, as ProCD prefers, "listings") can be read and manipulated by other software, such as word processing programs.

The database in SelectPhone™ cost more than $10 million to compile and is expensive to keep current. It is much more valuable to some users than to others. The combination of names, addresses, and SIC codes enables manufacturers to compile lists of potential customers. Manufacturers and retailers pay high prices to specialized information intermediaries for such mailing lists; ProCD offers a potentially cheaper alternative. People with nothing to sell could use the database as a substitute for calling long distance information, or as a way to look up old friends who have moved to unknown towns, or just as an electronic substitute for the local phone book. ProCD decided to engage in price discrimination, selling its database to the general public for personal use at a low price (approximately $150 for the set of five discs) while selling information to the trade for a higher price. …

Instead of tinkering with the product and letting users sort themselves – for example, furnishing current data at a high price that would be attractive only to commercial customers, and two-year-old data at a low price – ProCD turned to the institution of contract. Every box containing its consumer product declares that the software comes with restrictions stated in an enclosed license. This license, which is encoded on the CD-ROM disks as well as printed in the manual, and which appears on a user's screen every time the software runs, limits use of the application program and listings to non-commercial purposes.

Matthew Zeidenberg bought a consumer package of SelectPhone™ in 1994 from a retail outlet in Madison, Wisconsin, but decided to ignore the license. He formed Silken Mountain Web Services, Inc., to resell the information in the SelectPhone™ database. The corporation makes the database available on the Internet to anyone willing to pay its price – which, needless to say, is less than ProCD charges its commercial customers. Zeidenberg has purchased two additional SelectPhone™ packages, each with an updated version of the database, and made the latest information available over the World Wide Web, for a price, through his corporation. ProCD filed this suit seeking an injunction against further dissemination that exceeds the rights specified in the licenses (identical in each of the three packages Zeidenberg purchased). …

II.

Following the district court, we treat the licenses as ordinary contracts accompanying the sale of products, and therefore as governed by the common law of contracts and the Uniform Commercial Code. … Zeidenberg does argue, and the district court held, that placing the package of software on the shelf is an "offer," which the customer "accepts" by paying the asking price and leaving the store with the goods. In Wisconsin, as elsewhere, a contract includes only the terms on which the parties have agreed. One cannot agree to hidden terms, the judge concluded. So far, so good – but one of the terms to which Zeidenberg agreed by purchasing the software is that the transaction was subject to a license. Zeidenberg's position therefore must be that the printed terms on the outside of a box are the parties' contract – except for printed terms that refer to or incorporate other terms. But why would Wisconsin fetter the parties' choice in this way? Vendors can put the entire terms of a contract on the outside of a box only by using microscopic type, removing other information that buyers might find more useful (such as what the software does, and on which computers it works), or both. The "Read Me" file included with most software, describing system requirements and potential incompatibilities, may be equivalent to ten pages of type; warranties and license restrictions take still more space. Notice on the outside, terms on the inside, and a right to return the software for a refund if the terms are unacceptable (a right that the license expressly extends), may be a means of doing business valuable to buyers and sellers alike. Doubtless a state could forbid the use of standard contracts in the software business, but we do not think that Wisconsin has done so.

Transactions in which the exchange of money precedes the communication of detailed terms are common. Consider the purchase of insurance. The buyer goes to an agent, who explains the essentials (amount of coverage, number of years) and remits the premium to the home office, which sends back a policy. On the district judge's understanding, the terms of the policy are irrelevant because the insured paid before receiving them. Yet the device of payment, often with a "binder" (so that the insurance takes effect immediately even though the home office reserves the right to withdraw coverage later), in advance of the policy, serves buyers' interests by accelerating effectiveness and reducing transactions costs. Or consider the purchase of an airline ticket. The traveler calls the carrier or an agent, is quoted a price, reserves a seat, pays, and gets a ticket, in that order. The ticket contains elaborate terms, which the traveler can reject by canceling the reservation. To use the ticket is to accept the terms, even terms that in retrospect are disadvantageous. Just so with a ticket to a concert. The back of the ticket states that the patron promises not to record the concert; to attend is to agree. A theater that detects a violation will confiscate the tape and escort the violator to the exit. One could arrange things so that every concertgoer signs this promise before forking over the money, but that cumbersome way of doing things not only would lengthen queues and raise prices but also would scotch the sale of tickets by phone or electronic data service.

Consumer goods work the same way. Someone who wants to buy a radio set visits a store, pays, and walks out with a box. Inside the box is a leaflet containing some terms, the most important of which usually is the warranty, read for the first time in the comfort of home. By Zeidenberg's lights, the warranty in the box is irrelevant; every consumer gets the standard warranty implied by the UCC in the event the contract is silent; yet so far as we are aware no state disregards warranties furnished with consumer products. Drugs come with a list of ingredients on the outside and an elaborate package insert on the inside. The package insert describes drug interactions, contraindications, and other vital information – but, if Zeidenberg is right, the purchaser need not read the package insert, because it is not part of the contract.

Next consider the software industry itself. Only a minority of sales take place over the counter, where there are boxes to peruse. A customer may place an order by phone in response to a line item in a catalog or a review in a magazine. Much software is ordered over the Internet by purchasers who have never seen a box. Increasingly software arrives by wire. There is no box; there is only a stream of electrons, a collection of information that includes data, an application program, instructions, many limitations ("MegaPixel 3.14159 cannot be used with BytePusher 2.718"), and the terms of sale. The user purchases a serial number, which activates the software's features. On Zeidenberg's arguments, these unboxed sales are unfettered by terms – so the seller has made a broad warranty and must pay consequential damages for any shortfalls in performance, two "promises" that if taken seriously would drive prices through the ceiling or return transactions to the horse-and-buggy age.

According to the district court, the UCC does not countenance the sequence of money now, terms later. …

What then does the current version of the UCC have to say? We think that the place to start is § 2-204(1): "A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract." 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. And that is what happened. ProCD proposed a contract that a buyer would accept by using the software after having an opportunity to read the license at leisure. This Zeidenberg did. He had no choice, because the software splashed the license on the screen and would not let him proceed without indicating acceptance. So although the district judge was right to say that a contract can be, and often is, formed simply by paying the price and walking out of the store, the UCC permits contracts to be formed in other ways. ProCD proposed such a different way, and without protest Zeidenberg agreed. Ours is not a case in which a consumer opens a package to find an insert saying "you owe us an extra $10,000" and the seller files suit to collect. Any buyer finding such a demand can prevent formation of the contract by returning the package, as can any consumer who concludes that the terms of the license make the software worth less than the purchase price. Nothing in the UCC requires a seller to maximize the buyer's net gains. …

Some portions of the UCC impose additional requirements on the way parties agree on terms. A disclaimer of the implied warranty of merchantability must be "conspicuous." UCC § 2-316(2), incorporating UCC § 1-201(10). Promises to make firm offers, or to negate oral modifications, must be "separately signed." UCC §§ 2-205, 2-209 (2). These special provisos reinforce the impression that, so far as the UCC is concerned, other terms may be as inconspicuous as the forum-selection clause on the back of the cruise ship ticket in Carnival Lines. Zeidenberg has not located any Wisconsin case – for that matter, any case in any state – holding that under the UCC the ordinary terms found in shrinkwrap licenses require any special prominence, or otherwise are to be undercut rather than enforced. In the end, the terms of the license are conceptually identical to the contents of the package. Just as no court would dream of saying that SelectPhone™ must contain 3,100 phone books rather than 3,000, or must have data no more than 30 days old, or must sell for $100 rather than $150 – although any of these changes would be welcomed by the customer, if all other things were held constant – so, we believe, Wisconsin would not let the buyer pick and choose among terms. Terms of use are no less a part of "the product" than are the size of the database and the speed with which the software compiles listings. Competition among vendors, not judicial revision of a package's contents, is how consumers are protected in a market economy. ProCD has rivals, which may elect to compete by offering superior software, monthly updates, improved terms of use, lower price, or a better compromise among these elements. As we stressed above, adjusting terms in buyers' favor might help Matthew Zeidenberg today (he already has the software) but would lead to a response, such as a higher price, that might make consumers as a whole worse off.

Questions

1. In *ProCD*, the parties agree that putting the software on the shelf is an "offer" and that buying it is an "acceptance." Is it possible to characterize the exchange of communications differently?

2. *ProCD* upholds a contract that features "[n]otice on the outside [of the box], terms on the inside, and a right to return the software for a refund if the terms are unacceptable." Is this fair to both sides? Imagine an exchange that was missing notice but featured terms on the inside and a right to return. Would this suffice to create a valid contract? What if notice and a right to return were available, but the terms were missing? How about notice and terms, but no right to return?

3. One way of describing Zeidenberg's challenge to the purported "contract" is that he argued it was unreasonable for ProCD to treat his conduct as constituting an acceptance. This argument runs into the usual rule that the offeror is "master of his offer" and may define what conduct counts as acceptance. But how far can that rule really go? As James J. White puts it in *Contracting Under Amended 2-207*, 2004 WIS. L. REV. 723, "Suppose that your form asserts that my intentional tying my shoelaces tomorrow will be assent to all of your terms. Since I cannot tie my shoelaces unintentionally and since I have no valet, I'm stuck, not so?" How would you respond? Does your answer mean that *ProCD* was wrongly decided?

4. Is this a "computer case?" Or is this an ordinary contract case that just happens to involve the sale of computer software rather than the sale of grapes?

Specht v. Netscape Communications Corp.

306 F. 3d 17 (2d Cir. 2002)

Sotomayor, Circuit Judge: …

I. FACTS

In three related putative class actions, plaintiffs alleged that, unknown to them, their use of [the Netscape program] SmartDownload transmitted to defendants private information about plaintiffs' downloading of files from the Internet, thereby effecting an electronic surveillance of their online activities in violation of two federal statutes, the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

Specifically, plaintiffs alleged that when they first used Netscape's Communicator – a software program that permits Internet browsing – the program created and stored on each of their computer hard drives a small text file known as a "cookie" that functioned "as a kind of electronic identification tag for future communications" between their computers and Netscape. Plaintiffs further alleged that when they installed SmartDownload – a separate software "plug-in" that served to enhance Communicator's browsing capabilities – SmartDownload created and stored on their computer hard drives another string of characters, known as a "Key," which similarly functioned as an identification tag in future communications with Netscape. According to the complaints in this case, each time a computer user employed Communicator to download a file from the Internet, SmartDownload "assume[d] from Communicator the task of downloading" the file and transmitted to Netscape the address of the file being downloaded together with the cookie created by Communicator and the Key created by SmartDownload. These processes, plaintiffs claim, constituted unlawful "eavesdropping" on users of Netscape's software products as well as on Internet websites from which users employing SmartDownload downloaded files.

In the time period relevant to this litigation, Netscape offered on its website various software programs, including Communicator and SmartDownload, which visitors to the site were invited to obtain free of charge. …

Each of these plaintiffs allegedly arrived at a Netscape webpage captioned "SmartDownload Communicator" that urged them to "Download With Confidence Using SmartDownload!" At or near the bottom of the screen facing plaintiffs was the prompt "Start Download" and a tinted button labeled "Download." By clicking on the button, plaintiffs initiated the download of SmartDownload. Once that process was complete, SmartDownload, as its first plug-in task, permitted plaintiffs to proceed with downloading and installing Communicator, an operation that was accompanied by the clickwrap display of Communicator's license terms...

The signal difference between downloading Communicator and downloading SmartDownload was that no clickwrap presentation accompanied the latter operation. Instead, once plaintiffs Gibson, Gruber, Kelly, and Weindorf had clicked on the "Download" button located at or near the bottom of their screen, and the downloading of SmartDownload was complete, these plaintiffs encountered no further information about the plug-in program or the existence of license terms governing its use. The sole reference to SmartDownload's license terms on the "SmartDownload Communicator" webpage was located in text that would have become visible to plaintiffs only if they had scrolled down to the next screen.

Had plaintiffs scrolled down instead of acting on defendants' invitation to click on the "Download" button, they would have encountered the following invitation: "Please review and agree to the terms of the Netscape SmartDownload software license agreement before downloading and using the software." Plaintiffs Gibson, Gruber, Kelly, and Weindorf averred in their affidavits that they never saw this reference to the SmartDownload license agreement when they clicked on the "Download" button. They also testified during depositions that they saw no reference to license terms when they clicked to download SmartDownload, although under questioning by defendants' counsel, some plaintiffs added that they could not "remember" or be "sure" whether the screen shots of the SmartDownload page attached to their affidavits reflected precisely what they had seen on their computer screens when they downloaded SmartDownload. …

Even for a user who, unlike plaintiffs, did happen to scroll down past the download button, SmartDownload's license terms would not have been immediately displayed. … Instead, if such a user had seen the notice of SmartDownload's terms and then clicked on the underlined invitation to review and agree to the terms, a hypertext link would have taken the user to a separate webpage entitled "License & Support Agreements." The first paragraph on this page read, in pertinent part:

> The use of each Netscape software product is governed by a license agreement. You must read and agree to the license agreement terms BEFORE acquiring a product. Please click on the appropriate link below to review the current license agreement for the product of interest to you before acquisition. For products available for download, you must read and agree to the license agreement terms BEFORE you install the software. If you do not agree to the license terms, do not download, install or use the software.

Below this paragraph appeared a list of license agreements, the first of which was "License Agreement for Netscape Navigator and Netscape Communicator Product Family (Netscape Navigator, Netscape Communicator and Netscape SmartDownload)." If the user clicked on that link, he or she would be taken to yet another webpage that contained the full text of a license agreement that … granted the user a nonexclusive license to use and reproduce the software, subject to certain terms:

> BY CLICKING THE ACCEPTANCE BUTTON OR INSTALLING OR USING NETSCAPE COMMUNICATOR, NETSCAPE NAVIGATOR, OR NETSCAPE SMARTDOWNLOAD SOFTWARE (THE "PRODUCT"), THE INDIVIDUAL OR ENTITY LICENSING THE PRODUCT ("LICENSEE") IS CONSENTING TO BE BOUND BY AND IS BECOMING A PARTY TO THIS AGREEMENT. IF LICENSEE DOES NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THE BUTTON INDICATING NON-ACCEPTANCE MUST BE SELECTED, AND LICENSEE MUST NOT INSTALL OR USE THE SOFTWARE.

Among the license terms was a provision requiring virtually all disputes relating to the agreement to be submitted to arbitration:

> Unless otherwise agreed in writing, all disputes relating to this Agreement (excepting any dispute relating to intellectual property rights) shall be subject to final and binding arbitration in Santa Clara County, California, under the auspices of JAMS/EndDispute, with the losing party paying all costs of arbitration. …

II. Proceedings Below

In the district court, defendants moved to compel arbitration and to stay court proceedings pursuant to the Federal Arbitration Act ("FAA"), 9 U.S.C. § 4, arguing that the disputes reflected in the complaints, like any other dispute relating to the SmartDownload license agreement, are subject to the arbitration clause contained in that agreement. Finding that Netscape's webpage, unlike typical examples of clickwrap, neither adequately alerted users to the existence of SmartDownload's license terms nor required users unambiguously to manifest assent to those terms as a condition of downloading the product, the court held that the user plaintiffs had not entered into the SmartDownload license agreement. …

Defendants took this timely appeal pursuant to 9 U.S.C. § 16, and the district court stayed all proceedings in the underlying cases pending resolution of the appeal. …

Discussion

I. Standard of Review and Applicable Law

A district court's denial of a motion to compel arbitration is reviewed de novo. The determination of whether parties have contractually bound themselves to arbitrate a dispute – a determination involving interpretation of state law – is a legal conclusion also subject to de novo review. The findings upon which that conclusion is based, however, are factual and thus may not be overturned unless clearly erroneous.

If a court finds that the parties agreed to arbitrate, it should then consider whether the dispute falls within the scope of the arbitration agreement. …

III. Whether the User Plaintiffs Had Reasonable Notice of and Manifested Assent to the SmartDownload License Agreement

Whether governed by the common law or by Article 2 of the Uniform Commercial Code ("UCC"), a transaction, in order to be a contract, requires a manifestation of agreement between the parties. Mutual manifestation of assent, whether by written or spoken word or by conduct, is the touchstone of contract. Although an onlooker observing the disputed transactions in this case would have seen each of the user plaintiffs click on the SmartDownload "Download" button, a consumer's clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms. California's common law is clear that "an offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious."

Arbitration agreements are no exception to the requirement of manifestation of assent. …

A. The Reasonably Prudent Offeree of Downloadable Software

Defendants argue that plaintiffs must be held to a standard of reasonable prudence and that, because notice of the existence of SmartDownload license terms was on the next scrollable screen, plaintiffs were on "inquiry notice" of those terms. We disagree with the proposition that a reasonably prudent offeree in plaintiffs' position would necessarily have known or learned of the existence of the SmartDownload license agreement prior to acting, so that plaintiffs may be held to have assented to that agreement with constructive notice of its terms. It is true that "[a] party cannot avoid the terms of a contract on the ground that he or she failed to read it before signing." *Marin Storage & Trucking*, 89 Cal. App. 4th at 1049. But courts are quick to add: "An exception to this general rule exists when the writing does not appear to be a contract and the terms are not called to the attention of the recipient. In such a case, no contract is formed with respect to the undisclosed term."

Most of the cases cited by defendants in support of their inquiry-notice argument are drawn from the world of paper contracting. …

As the foregoing cases suggest, receipt of a physical document containing contract terms or notice thereof is frequently deemed, in the world of paper transactions, a sufficient circumstance to place the offeree on inquiry notice of those terms. "Every person who has actual notice of circumstances sufficient to put a prudent man upon inquiry as to a particular fact, has constructive notice of the fact itself in all cases in which, by prosecuting such inquiry, he might have learned such fact." Cal. Civ.Code § 19. These principles apply equally to the emergent world of online product delivery, pop-up screens, hyperlinked pages, clickwrap licensing, scrollable documents, and urgent admonitions to "Download Now!". What plaintiffs saw when they were being invited by defendants to download this fast, free plug-in called SmartDownload was a screen containing praise for the product and, at the very bottom of the screen, a "Download" button. Defendants argue that under the principles set forth in the cases cited above, a "fair and prudent person using ordinary care" would have been on inquiry notice of SmartDownload's license terms.

We are not persuaded that a reasonably prudent offeree in these circumstances would have known of the existence of license terms. Plaintiffs were responding to an offer that did not carry an immediately visible notice of the existence of license terms or require unambiguous manifestation of assent to those terms. Thus, plaintiffs' "apparent manifestation of . . . consent" was to terms "contained in a document whose contractual nature [was] not obvious." *Windsor Mills*, 25 Cal. App. 3d at 992, 101 Cal. Rptr. at 351. Moreover, the fact that, given the position of the scroll bar on their computer screens, plaintiffs may have been aware that an unexplored portion of the Netscape webpage remained below the download button does not mean that they reasonably should have concluded that this portion contained a notice of license terms. In their deposition testimony, plaintiffs variously stated that they used the scroll bar "[o]nly if there is something that I feel I need to see that is on – that is off the page," or that the elevated position of the scroll bar suggested the presence of "mere[ ] formalities, standard lower banner links" or "that the page is bigger than what I can see." Plaintiffs testified, and defendants did not refute, that plaintiffs were in fact unaware that defendants intended to attach license terms to the use of SmartDownload.

We conclude that in circumstances such as these, where consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms. … Internet users may have, as defendants put it, "as much time as they need[ ]" to scroll through multiple screens on a webpage, but there is no reason to assume that viewers will scroll down to subsequent screens simply because screens are there. When products are "free" and users are invited to download them in the absence of reasonably conspicuous notice that they are about to bind themselves to contract terms, the transactional circumstances cannot be fully analogized to those in the paper world of arm's-length bargaining. In the next two sections, we discuss case law and other legal authorities that have addressed the circumstances of computer sales, software licensing, and online transacting. Those authorities tend strongly to support our conclusion that plaintiffs did not manifest assent to SmartDownload's license terms. …

Cases in which courts have found contracts arising from Internet use do not assist defendants, because in those circumstances there was much clearer notice than in the present case that a user's act would manifest assent to contract terms. *See*, *e.g.*, … *Caspi v. Microsoft Network, L.L.C.*, 323 N.J.Super. 118 (App. Div. 1999) (upholding forum selection clause where subscribers to online software were required to review license terms in scrollable window and to click "I Agree" or "I Don't Agree"); *Barnett v. Network Solutions, Inc.*, 38 S.W.3d 200, 203-04 (Tex. App. 2001) (upholding forum selection clause in online contract for registering Internet domain names that required users to scroll through terms before accepting or rejecting them); *cf. Pollstar v. Gigmania, Ltd.*, 170 F.Supp. 2d 974, 981-82 (E.D. Cal.2000) (expressing concern that notice of license terms had appeared in small, gray text on a gray background on a linked webpage, but concluding that it was too early in the case to order dismissal).

After reviewing the California common law and other relevant legal authority, we conclude that under the circumstances here, plaintiffs' downloading of SmartDownload did not constitute acceptance of defendants' license terms. Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility. We hold that a reasonably prudent offeree in plaintiffs' position would not have known or learned, prior to acting on the invitation to download, of the reference to SmartDownload's license terms hidden below the "Download" button on the next screen. We affirm the district court's conclusion that the user plaintiffs, including Fagan, are not bound by the arbitration clause contained in those terms.

Questions

1. In *Specht*, what is the purported "offer?" What is the purported "acceptance?" Is there any other way to characterize the exchange of communications?

2. How were the proposed license terms presented to downloaders of SmartDownload? Compare this to how the proposed license terms in *ProCD* were presented to purchasers of SelectPhone. Would a "reasonably prudent offeree" in Zeidenberg's shoes have been aware of the existence of the terms?

3. Why did Netscape include an arbitration clause?

4. Reconsider the FloodZone problem in Chapter 2, *supra*. The contract in *ProCD* is an example of an enforceable "shrinkwrap" license; the contract in *Specht* is an example of an unenforceable "browsewrap" license; the FloodZone contract is an example of "clickwrap." Based on *ProCD* and *Specht*, are clickwrap contracts enforceable?

5. Ada reprograms her web browser so that whenever it request a web page from a server, it sends the following text to the server: "By responding to this HTTP request, you accept legal responsibility for any resulting harm." (Technically, the browser send the text as the "User-Agent string," which would ordinarily tell the server, for example, whether she is using Internet Explorer, Firefox, or Safari. The standard that defines the HTTP protocol neither requires her to use nor forbids her from using the User-Agent string in this way.) If Charles's server sends her back a page with malware that crashes Ada's computer, can she sue the site for damages? What if the site has its own browsewrap terms of service disclaiming such liability?

Bragg v. Linden Research, Inc.

487 F. Supp. 2d 593 (E.D. Pa. 2007)

Robreno, District Judge: …

I. Background

A. Second Life

The defendants in this case, Linden Research Inc. ("Linden") and its Chief Executive Officer, Philip Rosedale, operate a multiplayer role-playing game set in the virtual world known as "Second Life." Participants create avatars to represent themselves, and Second Life is populated by hundreds of thousands of avatars, whose interactions with one another are limited only by the human imagination. According to Plaintiff, many people "are now living large portions of their lives, forming friendships with others, building and acquiring virtual property, forming contracts, substantial business relationships and forming social organizations" in virtual worlds such as Second Life. Owning property in and having access to this virtual world is, moreover, apparently important to the plaintiff in this case. …

C. Plaintiffs' Participation in Second Life

In 2005, Plaintiff Marc Bragg, Esq., signed up and paid Linden to participate in Second Life. …

The dispute ultimately at issue in this case arose on April 30, 2006, when Bragg acquired a parcel of virtual land named "Taessot" for $300. Linden sent Bragg an email advising him that Taessot had been improperly purchased through an "exploit." Linden took Taesot away. It then froze Bragg's account, effectively confiscating all of the virtual property and currency that he maintained on his account with Second Life.

Bragg brought suit against Linden and Rosedale in the Court of Common Pleas of Chester County, Pennsylvania, on October 3, 2006. Linden and Rosedale removed the case to this Court and then, within a week, moved to compel arbitration. …

III. Motion to Compel Arbitration

Defendants have also filed a motion to compel arbitration that seeks to dismiss this action and compel Bragg to submit his claims to arbitration according to the Rules of the International Chamber of Commerce ("ICC") in San Francisco.

A. Relevant Facts

Before a person is permitted to participate in Second Life, she must accept the Terms of Service of Second Life (the "TOS") by clicking a button indicating acceptance of the TOS. Bragg concedes that he clicked the "accept" button before accessing Second Life. Included in the TOS are a California choice of law provision, an arbitration provision, and forum selection clause. Specifically, located in the fourteenth line of the thirteenth paragraph under the heading "GENERAL PROVISIONS," and following provisions regarding the applicability of export and import laws to Second Life, the following language appears:

> Any dispute or claim arising out of or in connection with this Agreement or the performance, breach or termination thereof, shall be finally settled by binding arbitration in San Francisco, California under the Rules of Arbitration of the International Chamber of Commerce by three arbitrators appointed in accordance with said rules. . . . Notwithstanding the foregoing, either party may apply to any court of competent jurisdiction for injunctive relief or enforcement of this arbitration provision without breach of this arbitration provision.

TOS § 13.

B. Legal Standards

1. *Federal law applies*

The Federal Arbitration Act ("FAA") requires that the Court apply federal substantive law here because the arbitration agreement is connected to a transaction involving interstate commerce. …

2. *The Legal Standard Under the FAA*

Under the FAA, on the motion of a party, a court must stay proceedings and order the parties to arbitrate the dispute if the court finds that the parties have agreed in writing to do so. 9 U.S.C. §§ 3, 4, 6. A party seeking to compel arbitration must show (1) that a valid agreement to arbitrate exists between the parties and (2) that the specific dispute falls within the scope of the agreement. …

In determining whether a valid agreement to arbitrate exists between the parties, the Third Circuit has instructed district courts to give the party opposing arbitration "the benefit of all reasonable doubts and inferences that may arise," or, in other words, to apply the familiar Federal Rule of Civil Procedure 56(c) summary judgment standard. … While there is a presumption that a particular dispute is within the scope of an arbitration agreement,*Volt Info. Scis., Inc. v. Bd. of Trustees*, 489 U.S. 468, 475 (1989), there is no such "presumption" or "policy" that favors the existence of a valid agreement to arbitrate. …

C. Application

1. *Unconscionabilty of the Arbitration Agreement*

Bragg resists enforcement of the TOS's arbitration provision on the basis that it is "both procedurally and substantively unconscionable and is itself evidence of defendants' scheme to deprive Plaintiff (and others) of both their money and their day in court."

Section 2 of the FAA provides that written arbitration agreements "shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." 9 U.S.C. § 2. Thus, "generally applicable contract defenses, such as fraud, duress, or unconscionability, may be applied to invalidate arbitration agreements without contravening § 2." *Doctor's Assocs. v. Casarotto,* 517 U.S. 681, 687 (1996). When determining whether such defenses might apply to any purported agreement to arbitrate the dispute in question, "courts generally . . . should apply ordinary state-law principles that govern the formation of contracts." *First Options of Chicago, Inc. v. Kaplan*, 514 U.S. 938, 944, (1995). Thus, the Court will apply California state law to determine whether the arbitration provision is unconscionable.

Under California law, unconscionability has both procedural and substantive components. … The procedural component can be satisfied by showing (1) oppression through the existence of unequal bargaining positions or (2) surprise through hidden terms common in the context of adhesion contracts. *Comb* [*v. Paypal, Inc.*], 218 F.Supp. 2d [1165,] 1172. The substantive component can be satisfied by showing overly harsh or one-sided results that "shock the conscience." *Id.* The two elements operate on a sliding scale such that the more significant one is, the less significant the other need be. … However, a claim of unconscionability cannot be determined merely by examining the face of the contract; there must be an inquiry into the circumstances under which the contract was executed, and the contract's purpose, and effect.

(a) Procedural Unconscionability

A contract or clause is procedurally unconscionable if it is a contract of adhesion. … A contract of adhesion, in turn, is a "standardized contract, which, imposed and drafted by the party of superior bargaining strength, relegates to the subscribing party only the opportunity to adhere to the contract or reject it." … Under California law, "the critical factor in procedural unconscionability analysis is the manner in which the contract or the disputed clause was presented and negotiated." *Nagrampa v. MailCoups, Inc.*, 469 F.3d 1257, 1282 (9th Cir. 2006). "When the weaker party is presented the clause and told to 'take it or leave it' without the opportunity for meaningful negotiation, oppression, and therefore procedural unconscionability, are present." *Id.* …

The TOS are a contract of adhesion. Linden presents the TOS on a take-it-or-leave-it basis. A potential participant can either click "assent" to the TOS, and then gain entrance to SecondLife's virtual world, or refuse assent and be denied access. Linden also clearly has superior bargaining strength over Bragg. Although Bragg is an experienced attorney, who believes he is expert enough to comment on numerous industry standards and the "rights" or participants in virtual worlds, he was never presented with an opportunity to use his experience and lawyering skills to negotiate terms different from the TOS that Linden offered. …

(b) Substantive Unconscionability

Even if an agreement is procedurally unconscionable, "it may nonetheless be enforceable if the substantive terms are reasonable." *Id.* at 1173 (citing *Craig v. Brown & Root, Inc.*, 84 Cal. App. 4th 416 (2000) (finding contract of adhesion to arbitrate disputes enforceable)). Substantive unconscionability focuses on the one-sidedness of the contract terms. *Armendariz* [*v. Foundation Health Psychcare Services, Inc.*], 99 Cal. Rptr. 2d 745 (2000),. Here, a number of the TOS's elements lead the Court to conclude that Bragg has demonstrated that the TOS are substantively unconscionable.

(i) Mutuality

Under California law, substantive unconscionability has been found where an arbitration provision forces the weaker party to arbitrate claims but permits a choice of forums for the stronger party. … In other words, the arbitration remedy must contain a "modicum of bilaterality." *Armendariz* [*v. Foundation Health Psychcare Services, Inc.*, 99 Cal. Rptr. 2d 745, 769 (2000)]. This principle has been extended to arbitration provisions that allow the stronger party a range of remedies before arbitrating a dispute, such as self-help, while relegating to the weaker party the sole remedy of arbitration.

In *Comb*, for example, the court found a lack of mutuality where the user agreement allowed PayPal "at its sole discretion" to restrict accounts, withhold funds, undertake its own investigation of a customer's financial records, close accounts, and procure ownership of all funds in dispute unless and until the customer is "later determined to be entitled to the funds in dispute." 218 F. Supp. 2d at 1173–74. Also significant was the fact that the user agreement was "subject to change by PayPal without prior notice (unless prior notice is required by law), by posting of the revised Agreement on the PayPal website." *Id.*

Here, the TOS contain many of the same elements that made the PayPal user agreement substantively unconscionable for lack of mutuality. The TOS proclaim that "Linden has the right at any time for any reason or no reason to suspend or terminate your Account, terminate this Agreement, and/or refuse any and all current or future use of the Service without notice or liability to you." Whether or not a customer has breached the Agreement is "determined in Linden's sole discretion." Linden also reserves the right to return no money at all based on mere "suspicions of fraud" or other violations of law. Finally, the TOS state that "Linden may amend this Agreement . . . at any time in its sole discretion by posting the amended Agreement [on its website]."

In effect, the TOS provide Linden with a variety of one-sided remedies to resolve disputes, while forcing its customers to arbitrate any disputes with Linden. This is precisely what occurred here. When a dispute arose, Linden exercised its option to use self-help by freezing Bragg's, account, retaining funds that Linden alone determined were subject to dispute, and then telling Bragg that he could resolve the dispute by initiating a costly arbitration process. The TOS expressly authorized Linden to engage in such unilateral conduct. As in *Comb*, "[f]or all practical purposes, a customer may resolve disputes only after [Linden] has had control of the disputed funds for an indefinite period of time," and may only resolve those disputes by initiating arbitration. 218 F.Supp. 2d at 1175.

Linden's right to modify the arbitration clause is also significant. "The effect of [Linden's] unilateral right to modify the arbitration clause is that it could . . . craft precisely the sort of asymmetrical arbitration agreement that is prohibited under California law as unconscionable." *Net Global Mktg.* [*v. Dialtone, Inc.*, 217 Fed. Appx. 598, 602 (9th Cir. 2007)]. This lack of mutuality supports a finding of substantive unconscionability.

(ii) Costs of Arbitration and Fee-Sharing

… Here, even taking Defendants characterization of the fees to be accurate, the total estimate of costs and fees would be $7,500, which would result in Bragg having to advance $3,750 at the outset of arbitration. The court's own estimates place the amount that Bragg would likely have to advance at $8,625, but they could reach as high as $13,687.50. Any of these figures are significantly greater than the costs that Bragg bears by filing his action in a state or federal court. Accordingly, the arbitration costs and fee-splitting scheme together also support a finding of unconscionability.

(iii) Venue

The TOS also require that any arbitration take place in San Francisco, California. In *Comb*, the Court found that a similar forum selection clause supported a finding of substantive unconscionability, because the place in which arbitration was to occur was unreasonable, taking into account "the respective circumstances of the parties." 218 F.Supp.2d at 1177. As in *Comb*, the record in this case shows that Linden serves millions of customers across the United States and that the average transaction through or with Second Life involves a relatively small amount. In such circumstances, California law dictates that it is not "reasonable for individual consumers from throughout the country to travel to one locale to arbitrate claims involving such minimal sums." *Id.* Indeed, "[l] imiting venue to [Linden's] backyard appears to be yet one more means by which the arbitration clause serves to shield [Linden] from liability instead of providing a neutral forum in which to arbitrate disputes." *Id.* …

(c) Conclusion

When a dispute arises in Second Life, Linden is not obligated to initiate arbitration. Rather, the TOS expressly allow Linden, at its "sole discretion" and based on mere "suspicion," to unilaterally freeze a participant's account, refuse access to the virtual and real currency contained within that account, and then confiscate the participant's virtual property and real estate. A participant wishing to resolve any dispute, on the other hand, after having forfeited its interest in Second Life, must then initiate arbitration in Linden's place of business. To initiate arbitration involves advancing fees to pay for no less than three arbitrators at a cost far greater than would be involved in litigating in the state or federal court system. Moreover, under these circumstances, the confidentiality of the proceedings helps ensure that arbitration itself is fought on an uneven field by ensuring that, through the accumulation of experience, Linden becomes an expert in litigating the terms of the TOS, while plaintiffs remain novices without the benefit of learning from past precedent.

Taken together, the lack of mutuality, the costs of arbitration, the forum selection clause, and the confidentiality provision that Linden unilaterally imposes through the TOS demonstrate that the arbitration clause is not designed to provide Second Life participants an effective means of resolving disputes with Linden. Rather, it is a one-sided means which tilts unfairly, in almost all situations, in Linden's favor. As in *Comb*, through the use of an arbitration clause, Linden "appears to be attempting to insulate itself contractually from any meaningful challenge to its alleged practices." 218 F.Supp. 2d at 1176. …

Finding that the arbitration clause is procedurally and substantively unconscionable, the Court will refuse to enforce it. …

Questions

1. Linden got its offer-acceptance process right, didn't it? So what was wrong with their arbitration clause? Do the terms the court found objectionable seem "unconscionable" to you?

2. As Linden's lawyer, would you advise trying to salvage the arbitration term, and if so, how, or should you just give up on it?

3. Look at the Central Pacific Railroad Photographic History Museum website at http://cprr.org, including its User Agreement at http://cprr.org/Museum/legal.html. Are these terms enforceable? All of them? Against whom? What's going on here?

4. Under *Bragg*, were the terms in *ProCD* unconscionable?

SeaSells Problem

You are counsel to SeaSells.com, an e-commerce startup that is creating an online marketplace for seashell collectors to show off their favorite shells and trade with each other. User accounts are free, and are required to post, but not to view the site. SeaSells takes a 10% commission plus a $1.00 listing fee on any sale. As SeaSells adds new site features, such as new payment options, new forums, and new technology partnerships, you expect to revise your terms and conditions to take into account these new features. You also expect that you will want to revise the terms and conditions to respond to shifts in the legal landscape. Design a process – both technical and legal – to ensure that any future changes to the terms will be enforceable. Your proposal will need to be approved by the CEO, and you will need to be prepared to respond to any objections from Marketing and Operations that your process makes the site harder to use.

II. Computer Misuse Statutes

Although computer intrusions were initially prosecuted under existing common-law or statutory theft laws, the field is now primarily defined by special-purpose computer misuse statutes. The federal Computer Fraud and Abuse Act (CFAA) has been the leading model here, but every state has its own statute, most of which parallel the CFAA in their essentials.

The details of these statutes and their interpretation vary enormously, and the CFAA itself has been frequently amended, so the materials in this section don't focus on the exact structure of any particular statute. Instead, they consider a number of common interpretive questions that arise under any of this family of statutes. The general scheme of the CFAA and related statutes is that they prohibit "intentional" "access" to a computer "without authorization." In many such statutes additional elements, such as causing "damage or loss" above a certain threshold, increase the gravity of the offense. The materials in this section consider some of the ambiguities those phrases create.

State v. Allen

260 Kan. 107 (1996)

Larson, Justice.:

In this first impression case, we are presented with the question of whether a person's telephonic connections that prompt a computer owner to change its security systems constitute felony computer crime in violation of K.S.A. 21-3755(b).

The charges against Anthony A. Allen arose from several telephonic connections he made with Southwestern Bell Telephone Company's computers in early 1995. After preliminary hearing, the trial court dismissed the complaint, finding no probable cause existed to believe Allen had committed any crime.

The State has appealed pursuant to K.S.A. 22-3602(b)(1). We affirm the trial court. …

Allen admitted to Detective Kent Willnauer that he had used his computer, equipped with a modem, to call various Southwestern Bell computer modems. The telephone numbers for the modems were obtained by random dialing. If one of Allen's calls were completed, his computer determined if it had been answered by voice or another computer. These were curiosity calls of short duration.

The State presented no evidence which showed that Allen ever had entered any Southwestern Bell computer system. Detective Willnauer was unable to state that Allen had altered any programs, added anything to the system, used it to perform any functions, or interfered with its operation. Willnauer specifically stated he had no evidence that the Southwestern Bell computer system had been damaged.

Ronald W. Knisley, Southwestern Bell's Regional Security Director, testified Allen had called two different types of Southwestern Bell computer equipment – SLC-96 system environmental controls and SMS-800 database systems. …

Testimony confirmed Allen also called and connected 28 times with the SMS-800 systems at several different modem numbers. Each call but two was under 1 minute. Upon connection with this system, a person would see a log on request and a "banner." The banner identifies the system that has answered the incoming call and displays that it is Southwestern Bell property and that access is restricted. Entry into the system itself then requires both a user ID and a password which must agree with each other. No evidence indicated Allen went beyond this banner or even attempted to enter a user ID or password.

Knisley testified that if entry into an SMS-800 system were accomplished and proper commands were given, a PBX system could be located which would allow unlimited and nonchargeable long distance telephone calls. There was no evidence this occurred, nor was it shown that Allen had damaged, modified, destroyed, or copied any data.

James E. Robinson, Function Manager responsible for computer security, testified one call to an SMS-800 system lasted 6 minutes and 35 seconds. Although the system should have retained information about this call, it did not, leading to speculation the record-keeping system had been overridden. Robinson speculated Allen had gained entry into the system but admitted he had no evidence that Allen's computer had done anything more than sit idle for a few minutes after calling a Southwestern Bell modem number.

Robinson testified that Southwestern Bell was unable to document any damage to its computer equipment or software as a result of Allen's activities. However, as a result of its investigation, Southwestern Bell decided that prudence required it to upgrade its password security system to a more secure "token card" process. It was the cost of this investigation and upgrade that the State alleges comprises the damage caused by Allen's actions. Total investigative costs were estimated at $4,140. The cost of developing deterrents was estimated to be $1,656. The cost to distribute secure ID cards to employees totaled $18,000. Thus, the total estimated damage was $23,796. …

The legal standard to be applied in a preliminary hearing is clear. If it appears from the evidence presented that a crime has been committed and there is probable cause to believe the defendant committed it, K.S.A. 22-2902(3) requires that the defendant be bound over for trial. … If there is not sufficient evidence, the defendant must be discharged. … From the evidence presented, the trial court must draw the inferences favorable to the prosecution, and the evidence need only establish probable cause. … "Probable cause at a preliminary hearing signifies evidence sufficient to cause a person of ordinary prudence and caution to conscientiously entertain a reasonable belief of the accused's guilt." …

Allen was charged with a violation of K.S.A. 21-3755(b)(1), with the second amended complaint alleging that he

> "did then and there intentionally and without authorization gain access and damage a computer, computer system, computer network or other computer property which caused a loss of the value of at least $500.00 but less than $25,000.00, a severity level 9 non-person felony."

Felony computer crime as it is charged in this case under K.S.A. 21-3755(b)(1) required the State to prove three distinct elements: (1) intentional and unauthorized access to a computer, computer system, computer network, or any other property … ; (2) damage to a computer, computer system, computer network, or any other property; and (3) a loss in value as a result of such crime of at least $500 but less than $25,000. The trial court found that the State failed to show probable cause as to each of these elements.

Did the trial court err in ruling there was insufficient evidence to show Allen gained "access" to Southwestern Bell's computers?

After finding the evidence showed Allen had done nothing more than use his computer to call unlisted telephone numbers, the trial court ruled there was insufficient evidence to show Allen had gained access to the computer systems. Although a telephone connection had been established, the evidence showed Allen had done nothing more. The trial court reasoned that unless and until Allen produced a password that permitted him to interact with the data in the computer system, he had not "gained access" as the complaint required.

The State argues the trial court's construction of the statute ignores the fact that "access" is defined in the statute, K.S.A. 21-3755(a)(1), as "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system or computer network." By this definition, the State would lead us to believe that any kind of an "approach" is criminal behavior sufficient to satisfy a charge that Allen did in fact "gain access" to a computer system.

The problem with the State's analysis is that K.S.A. 21-3755(b)(1) does not criminalize "accessing" (and, thus, "approaching") but rather "gaining or attempting to gain access." If we were to read "access" in this context as the equivalent of "approach," the statute would criminalize the behavior of "attempting to gain approach" to a computer or computer system. …

The United States Department of Justice has commented about the use of "approach" in a definition of "access" in this context: "The use of the word 'approach' in the definition of 'access,' if taken literally, could mean that any unauthorized physical proximity to a computer could constitute a crime." National Institute of Justice, Computer Crime: Criminal Justice Resource Manual, p. 84 (2d ed. 1989). …

Webster's defines "access" as "freedom or ability to obtain or make use of." Webster's New Collegiate Dictionary, p. 7 (1977). This is similar to the construction used by the trial court to find that no evidence showed that Allen had gained access to Southwestern Bell's computers. Until Allen proceeded beyond the initial banner and entered appropriate passwords, he could not be said to have had the ability to make use of Southwestern Bell's computers or obtain anything. Therefore, he cannot be said to have gained access to Southwestern Bell's computer systems as gaining access is commonly understood. The trial court did not err in determining the State had failed to present evidence showing probable cause that Allen had gained access to Southwestern Bell's computer system.

Did the trial court err in ruling that no evidence showed Allen had damaged any computer, computer system, computer network, or any other property?

The State acknowledges it cannot meet the damage element of the crime it has charged by any means other than evidence showing Allen's actions resulted in expenditures of money by Southwestern Bell. It is crystal clear there is absolutely no evidence Allen modified, altered, destroyed, copied, disclosed, or took possession of anything. The State's evidence clearly shows Allen did not physically affect any piece of computer equipment or software by his telephone calls. All the State was able to show was that Southwestern Bell made an independent business judgment to upgrade its security at a cost of $23,796. The State argues this is sufficient.

The State's argument is clearly flawed. The trial court reasoned by a fitting analogy that the State is essentially saying that a person looking at a no trespassing sign on a gate causes damage to the owner of the gate if the owner decides as a result to add a new lock. The trial court has clearly pointed to the correct analysis of this issue.

The State's circular theory is that if someone incurs costs to investigate whether an activity is criminal, it becomes criminal because investigative costs were incurred. Although computer crime is not, for obvious reasons, a common-law crime, it nevertheless has a common-law predicate which helps us to understand the legislature's intent. K.S.A. 21-3755 was not designed to update criminal trespass or malicious mischief statutes to the computer age but "to address inadequacies in the present theft statute related to prosecution of computer related crimes. Specifically, present theft statutes make prosecution difficult among crimes in which the computer owner was not actually deprived of the computer or its software." Kansas Legislature Summary of Legislation 1985, p. 80.

Theft, as defined in K.S.A. 21-3701, is not concerned with mere occupation, detention, observation, or tampering, but rather requires permanent deprivation. The intent required for theft is an "intent to deprive the owner permanently of the possession, use, or benefit of the owner's property." K.S.A. 21-3701(a). One may have wrongful intent, such as intent to trespass, without having the intent required for a theft. In addition, at common law, the thing of which the victim was deprived had to be something of value. The second element of computer crime mirrors this common-law requirement of the deprivation of something of value in a larceny action. As in a larceny action, the extent of the deprivation determines the severity level of the crime. This element of computer crime, as with other theft statutes, cannot be satisfied where there is no deprivation as in this case. . . .

Southwestern Bell's computer system was not "damaged" in the sense the statute requires. Southwestern Bell was not deprived of property in the manner required to support a criminal charge. The fact an independent business judgment that Southwestern Bell's computer systems might be accessible was made after Allen's conduct was discovered does not support the second and third elements of the crime charged. The trial court correctly determined the State failed to meet its probable cause burden on these issues as well.

Affirmed.

Questions

1. Why do computer misuse statutes exist at all? Prosecutors used to (and sometimes still do) charge defendants like Allen with ordinary theft crimes. Suppose he had been able to use Southwestern Bell's computers to change several people's phone numbers, look through a local politician's billing records, zero out his own account balance, and download confidential Southwestern Bell documents. Which of these actions, if any, would constitute larceny? Fraud? Embezzlement? What problems arise when trying to apply the elements of these crimes to computer misuse?

2. What did Allen do, and why did the court hold that it didn't constitute "access?" Note that Allen did cause the SMS-800 to transmit information to him. Why doesn't that count as "access?" Suppose you were Allen's lawyer and it appeared that the court was likely to rule against you on the access issue. Could you argue that his limited use of the SMS-800 was "authorized?"

3. The second issue *Allen* raises is the nature of harm required. The Kansas statute refers to "damage." In what sense did Allen damage or not damage the SMS-800? Did it burst into flames? Did it become unusable? Did it require programming time to repair? Did it require programming time to investigate whether it needed to be repaired? The court calls the state's argument on this point "circular." Do you agree?

4. The CFAA defines "computer" as:

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

18 U.S.C. § 1030(e)(1). Under this definition, is a cell phone a "computer?" An abacus? A USB thumb drive? A power cable?

United States v. Morris

928 F. 2d 504 (2d Cir. 1991)

Newman, Circuit Judge:

In the fall of 1988, [Robert Tappan] Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise. When Morris entered Cornell, he was given an account on the computer at the

Computer Science Division. This account gave him explicit authorization to use computers at Cornell. …

In October 1988, Morris began work on a computer program, later known as the INTERNET "worm" or "virus." The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered. … Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network. Morris released the worm into INTERNET, which is a group of national networks that connect university, governmental, and military computers around the country. The network permits communication and transfer of information between computers on the network.

Morris sought to program the INTERNET worm to spread widely without drawing attention to itself. The worm was supposed to occupy little computer operation time, and thus not interfere with normal use of the computers. Morris programmed the worm to make it difficult to detect and read, so that other programmers would not be able to "kill" the worm easily.

Morris also wanted to ensure that the worm did not copy itself onto a computer that already had a copy. [Due to programming and mathematical mistakes, Morris's safeguard failed, leading the worm to install thousands of copies of itself on each computer it reached.]

Morris identified four ways in which the worm could break into computers on the network:

> (1) through a "hole" or "bug" (an error) in SENDMAIL, a computer program that transfers and receives electronic mail on a computer;
>
> (2) through a bug in the "finger demon" program, a program that permits a person to obtain limited information about the users of another computer;
>
> (3) through the "trusted hosts" feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and
>
> (4) through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform.

On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discovered that the worm was replicating and reinfecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around the country either crashed or became "catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000.

Morris was found guilty, following a jury trial, of violating 18 U.S.C. § 1030(a)(5)(A). He was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.

Discussion

I. The intent requirement in section 1030(a)(5)(A)

Section 1030(a)(5)(A), covers anyone who

> (5) *intentionally accesses* a Federal interest computer without authorization, *and* by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or *prevents authorized use* of any such computer or information, *and thereby*
>
> > (A) *causes loss* to one or more others of a value aggregating $1,000 or more during any one year period; . . . [emphasis added].

The District Court concluded that the intent requirement applied only to the accessing and not to the resulting damage. Judge Munson found recourse to legislative history unnecessary because he considered the statute clear and unambiguous. However, the Court observed that the legislative history supported its reading of section 1030(a)(5)(A).

Morris argues that the Government had to prove not only that he intended the unauthorized access of a federal interest computer, but also that he intended to prevent others from using it, and thus cause a loss. The adverb "intentionally," he contends, modifies both verb phrases of the section. The Government urges that since punctuation sets the "accesses" phrase off from the subsequent "damages" phrase, the provision unambiguously shows that "intentionally" modifies only "accesses." Absent textual ambiguity, the Government asserts that recourse to legislative history is not appropriate. ...

With some statutes, punctuation has been relied upon to indicate that a phrase set off by commas is independent of the language that followed. ... However, we have been advised that punctuation is not necessarily decisive in construing statutes, ... , and with many statutes, a mental state adverb adjacent to initial words has been applied to phrases or clauses appearing later in the statute without regard to the punctuation or structure of the statute. ... In the present case, we do not believe the comma after "authorization" renders the text so clear as to preclude review of the legislative history. ...

First, the 1986 amendments changed the scienter requirement in section 1030(a)(2) from "knowingly" to "intentionally." *See* Pub.L. No. 99-474, section 2(a)(1). ...

According to the Senate Judiciary Committee, Congress changed the mental state requirement in section 1030(a)(2) for two reasons. Congress sought only to proscribe intentional acts of unauthorized access, not "mistaken, inadvertent, or careless" acts of unauthorized access. S.Rep. No. 99-432, 99th Cong., 2d Sess. 5 (1986), *reprinted in* 1986 U.S.Code Cong. & Admin.News 2479, 2483 [hereinafter Senate Report].

Also, Congress expressed concern that the "knowingly" standard "might be inappropriate for cases involving computer technology." *Id.* The concern was that a scienter requirement of "knowingly" might encompass the acts of an individual "who inadvertently 'stumble[d] into' someone else's computer file or computer data," especially where such individual was authorized to use a particular computer. *Id.* at 6. The Senate Report concluded that "[t]he substitution of an 'intentional' standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." *Id.* ...

This use of a mens rea standard to make sure that inadvertent accessing was not covered is also emphasized in the Senate Report's discussion of section 1030(a)(3) and section 1030(a)(5), under which Morris was convicted. Both subsections were designed to target "outsiders," individuals without authorization to access any federal interest computer. Senate Report at 10, U.S.Code Cong. & Admin.News at 2488. The rationale for the *mens rea* requirement suggests that it modifies only the "accesses" phrase, which was the focus of Congress's concern in strengthening the scienter requirement. …

Despite some isolated language in the legislative history that arguably suggests a scienter component for the "damages" phrase of section 1030(a)(5)(A), the wording, structure, and purpose of the subsection, examined in comparison with its departure from the format of its predecessor provision persuade us that the "intentionally" standard applies only to the "accesses" phrase of section 1030(a)(5)(A), and not to its "damages" phrase.

II. THE UNAUTHORIZED ACCESS REQUIREMENT IN SECTION 1030(A)(5)(A)

Section 1030(a)(5)(A) penalizes the conduct of an individual who "intentionally accesses a Federal interest computer without authorization." … Morris argues that there was insufficient evidence to convict him of "unauthorized access," …

We assess the sufficiency of the evidence under the traditional standard. Morris was authorized to use computers at Cornell, Harvard, and Berkeley, all of which were on INTERNET. As a result, Morris was authorized to communicate with other computers on the network to send electronic mail (SENDMAIL), and to find out certain information about the users of other computers (finger demon). The question is whether Morris's transmission of his worm constituted … accessing without authorization. …

The evidence permitted the jury to conclude that Morris's use of the SENDMAIL and finger demon features constituted access without authorization. … Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.

Moreover, the jury verdict need not be upheld solely on Morris's use of SENDMAIL and finger demon. As the District Court noted, in denying Morris' motion for acquittal,

> Although the evidence may have shown that defendant's initial insertion of the worm simply exceeded his authorized access, the evidence also demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program. Moreover, there was also evidence that the worm was designed to gain access to computers at which he had no account by guessing their passwords. Accordingly, the evidence did support the jury's conclusion that defendant accessed without authority as opposed to merely exceeding the scope of his authority.

In light of the reasonable conclusions that the jury could draw from Morris's use of SENDMAIL and finger demon, and from his use of the trusted hosts feature and password guessing, his challenge to the sufficiency of the evidence fails.

Questions

1. *Morris* confronts the most vexing issue in the CFAA caselaw: the the nature of "unauthorized" access. The court's first theory of authorization has to do with the "intended function" of the programs Morris used. How does a user (or a court) determine what the "intended function" of a computer program is? Have you ever used a program for something other than its intended function?

2. Is sending spam an "intended function" of an email program? Is logging in using a guessed password "authorized" under this test?

3. The court's second theory of authorization has to do with Morris's lack of an account on various systems. Have you ever used a computer on which you didn't have an

account? Does one always need an account to use a computer with permission? Is there a way to modify this test to make it more persuasive?

4. *Morris* also examines the *mens rea* requirement in the CFAA. The statute says "intentional," but does that mean only that the "access" must be intentional, or does the intentional mental state also apply to the lack of authorization, the resulting loss, etc.? How does *Morris* answer this question?

5. Where does *Morris* look for evidence to help it decide this question? Why does the court consider the placement of a comma potentially significant? In terms of legislative history, the court looks to the "Senate Report." What is that, who wrote it, and where would you look it up?

United States v. Drew

259 F.R.D. 449 (C.D. Cal. 2009)

Wu, District Judge: …

II. Background

A. Indictment

… The Indictment included, inter alia, the following allegations (not all of which were established by the evidence at trial). Drew, a resident of O'Fallon, Missouri, entered into a conspiracy in which its members agreed to intentionally access a computer used in interstate commerce without (and/or in excess of) authorization in order to obtain information for the purpose of committing the tortious act of intentional infliction of emotional distress upon "M.T.M.," subsequently identified as Megan Meier ("Megan"). Megan was a 13 year old girl living in O'Fallon who had been a classmate of Drew's daughter Sarah. Pursuant to the conspiracy, on or about September 20, 2006, the conspirators registered and set up a profile for a fictitious 16 year old male juvenile named "Josh Evans" on the www.MySpace.com website ("MySpace"), and posted a photograph of a boy without that boy's knowledge or consent. Such conduct violated MySpace's terms of service. The conspirators contacted Megan through the MySpace network (on which she had her own profile) using the Josh Evans pseudonym and began to flirt with her over a number of days. On or about October 7, 2006, the conspirators had "Josh" inform Megan that he was moving away. On or about October 16, 2006, the conspirators had "Josh" tell Megan that he no longer liked her and that "the world would be a better place without her in it." Later on that same day, after learning that Megan had killed herself, Drew caused the Josh Evans MySpace account to be deleted.

B. Verdict

[The jury deadlocked on a conspiracy charge and acquitted Drew on three felony counts. It did, however, convict Drew of a misdemeanor charge of "accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information."]

C. MySpace.com

… MySpace is a "social networking" website where members can create "profiles" and interact with other members. Anyone with Internet access can go onto the MySpace website and view content which is open to the general public such as a music area, video section, and members' profiles which are not set as "private." However, to create a profile, upload and display photographs, communicate with persons on the site, write "blogs," and/or utilize other services or applications on the MySpace website, one must be a "member." Anyone can become a member of MySpace at no charge so long as they meet a minimum age requirement and register.

In 2006, to become a member, one had to go to the sign-up section of the MySpace website and register by filling in personal information (such as name, email address, date of birth, country/state/postal code, and gender) and creating a password.

In addition, the individual had to check on the box indicating that "You agree to the MySpace **Terms of Service** and **Privacy Policy**." The terms of service did not appear on the same registration page that contained this "check box" for users to confirm their agreement to those provisions. In order to find the terms of service, one had (or would have had) to proceed to the bottom of the page where there were several "hyperlinks" including one entitled "Terms." … A person could become a MySpace member without ever reading or otherwise becoming aware of the provisions and conditions of the MySpace terms of service by merely clicking on the "check box" and then the "Sign Up" button without first accessing the "Terms" section.

As used in its website, "terms of service" refers to the "MySpace.com Terms of Use Agreement" ("MSTOS"). The MSTOS in 2006 stated, inter alia:

> This Terms of Use Agreement ("Agreement") sets forth the legally binding terms for your use of the Services. By using the Services, you agree to be bound by this Agreement, whether you are a "Visitor" (which means that you simply browse the Website) or you are a "Member" (which means that you have registered with Myspace.com). The term "User" refers to a Visitor or a Member. You are only authorized to use the Services (regardless of whether your access or use is intended) if you agree to abide by all applicable laws and to this Agreement. Please read this Agreement carefully and save it. If you do not agree with it, you should leave the Website and discontinue use of the Services immediately. If you wish to become a Member, communicate with other Members and make use of the Services, you must read this Agreement and indicate your acceptance at the end of this document before proceeding. …
>
> By using the Services, you represent and warrant that (a) all registration information you submit is truthful and accurate; (b) you will maintain the accuracy of such information; (c) you are 14 years of age or older; and (d) your use of the Services does not violate any applicable law or regulation.

The MSTOS prohibited the posting of a wide range of content on the website including (but not limited to) material that: a) "is potentially offensive and promotes racism, bigotry, hatred or physical harm of any kind against any group or individual"; b) "harasses or advocates harassment of another person"; c) "solicits personal information from anyone under 18"; d) "provides information that you know is false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous"; e) "includes a photograph of another person that you have posted without that person's consent"; f) "involves commercial activities and/or sales without our prior written consent"; g) "contains restricted or password only access pages or hidden pages or images"; or h) "provides any phone numbers, street addresses, last names, URLs or email addresses. . . ." MySpace also reserved the right to take appropriate legal action (including reporting the violating conduct to law enforcement authorities) against persons who engaged in "prohibited activity" which was defined as including, *inter alia*: a) "criminal or tortious activity", b) "attempting to impersonate another Member or person", c) "using any information obtained from the Services in order to harass, abuse, or harm another person", d) "using the Service in a manner inconsistent with any and all applicable laws and regulations", e) "advertising to, or solicitation of, any Member to buy or sell any products or services through the Services", f) "selling or otherwise transferring your profile", or g) "covering or obscuring the banner advertisements on your personal profile page …" The MSTOS warned users that "information provided by other MySpace.com Members (for instance, in their Profile) may contain inaccurate, inappropriate, offensive or sexually explicit material, products or services, and MySpace.com assumes no responsibility or liability for this material." Further, MySpace was allowed to unilaterally modify the terms of service, with such modifications taking effect upon the posting of notice on its website. Thus, members would have to review the

MSTOS each time they logged on to the website, to ensure that they were aware of any updates in order to avoid violating some new provision of the terms of service. Also, the MSTOS provided that "any dispute" between a visitor/member and MySpace "arising out of this Agreement must be settled by arbitration" if demanded by either party.

At one point, MySpace was receiving an estimated 230,000 new accounts per day and eventually the number of profiles exceeded 400 million with over 100 million unique visitors worldwide. "Generally speaking," MySpace would not monitor new accounts to determine if they complied with the terms of service except on a limited basis, mostly in regards to photographic content. Sung testified that there is no way to determine how many of the 400 million existing MySpace accounts were created in a way that violated the MSTOS. The MySpace website did have hyperlinks labelled "Safety Tips" (which contained advice regarding personal, private and financial security vis-a-vis the site) and "Report Abuse" (which allowed users to notify MySpace as to inappropriate content and/or behavior on the site). MySpace attempts to maintain adherence to its terms of service. It has different teams working in various areas such as "parent care" (responding to parents' questions about this site), handling "harassment/cyberbully cases, impostor profiles," removing inappropriate content, searching for underage users, etc. As to MySpace's response to reports of harassment:

> It varies depending on the situation and what's being reported. It can range from … letting the user know that if they feel threatened to contact law enforcement, to us removing the profile, and in rare circumstances we would actually contact law enforcement ourselves.

Once a member is registered and creates his or her profile, the data is housed on computer servers which are located in Los Angeles County. Members can create messages which can be sent to other MySpace members, but messages cannot be sent to or from other Internet service providers such as Yahoo!. All communications among MySpace members are routed from the sender's computer through the MySpace servers in Los Angeles. …

III. Applicable Law

A. F.R.Crim.P. 29(c)

A motion for judgment of acquittal under F.R.Crim.P. 29(c) may be made by a defendant seeking to challenge a conviction on the basis of the sufficiency of the evidence, … , or on other grounds including ones involving issues of law for the court to decide. … Where the Rule 29(c) motion rests in whole or in part on the sufficiency of the evidence, the evidence must be viewed "in the light most favorable to the government" … , with circumstantial evidence and inferences drawn in support of the jury's verdict. …

B. The CFAA

In 2006, the CFAA (18 U.S.C. § 1030) provided in relevant part that:

> (a) Whoever –
>
> * * * *
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –
>
> …
>
> (C) information from any protected computer if the conduct involved an interstate or foreign communication;
>
> shall be punished as provided in subsection (c) of this section. …

As used in the CFAA … [t]he term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . . ." *Id.* § 1030(e)(6). …

IV. Discussion

A. The Misdemeanor 18 U.S.C. § 1030(a)(2)(C*)* Crime Based on Violation of a Website's Terms of Service

… [T]he primary question here is whether any conscious violation of an Internet website's terms of service will cause an individual's contact with the website via computer to become "intentionally access[ing] . . . without authorization" or "exceeding authorization." …

In this particular case, as conceded by the Government, the only basis for finding that Drew intentionally accessed MySpace's computer/servers without authorization and/or in excess of authorization was her and/or her co-conspirator's violations of the MSTOS by deliberately creating the false Josh Evans profile, posting a photograph of a juvenile without his permission and pretending to be a sixteen year old O'Fallon resident for the purpose of communicating with Megan. …

There is nothing in the way that the undefined words "authorization" and "authorized" are used in the CFAA (or from the CFAA's legislative history) which indicates that Congress intended for them to have specialized meanings. As delineated in *Webster's New World Dictionary* at 92, to "authorize" ordinarily means "to give official approval to or permission for. . . ."

It cannot be considered a stretch of the law to hold that the owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access to information, services and/or applications which are available on the website. … Nor can it be doubted that the owner can relay and impose those limitations/restrictions/conditions by means of written notice such as terms of service or use provisions placed on the home page of the website. … While issues might be raised in particular cases as to the sufficiency of the notice and/or sufficiency of the user's assent to the terms, … , and while public policy considerations might in turn limit enforcement of particular restrictions, the vast majority of the courts (that have considered the issue) have held that a website's terms of service/use can define what is (and/or is not) authorized access vis-a-vis that website.

Here, the MSTOS defined "services" as including "the MySpace.com Website . . ., the MySpace.com instant messenger, and any other connection with the Website. . . ." It further notified the public that the MSTOS "sets forth the legally binding terms for your use of the services." Visitors and members were informed that "you are only authorized to use the Services . . . if you agree to abide by all applicable laws and to this Agreement." Moreover, to become a MySpace member and thereby be allowed to communicate with other members and fully utilize the MySpace Services, one had to click on a box to confirm that the user had agreed to the MySpace Terms of Service. Clearly, the MSTOS was capable of defining the scope of authorized access of visitors, members and/or users to the website.

B. Contravention of the Void-for-Vagueness Doctrine

1. *Applicable Law*

Justice Holmes observed that, as to criminal statutes, there is a "fair warning" requirement. As he stated in *McBoyle v. United States,* 283 U.S. 25, 27, (1931):

> Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.

… To avoid contravening the void-for-vagueness doctrine, the criminal statute must contain "relatively clear guidelines as to prohibited conduct" and provide "objective criteria" to evaluate whether a crime has been committed. …

However, a "difficulty in determining whether certain marginal offenses are within the meaning of the language under attack as vague does not automatically render a statute unconstitutional for indefiniteness . . . . Impossible standards of specificity are not required." *Jordan v. De George,* 341 U.S. 223, 231 (1951). "What renders a statute vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved; but rather the indeterminacy of precisely what that fact is." *United States v. Williams,* 553 U.S. 285 (2008). …

2. *Definitional/Actual Notice Deficiencies*

The pivotal issue herein is whether basing a CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine. This Court concludes that it does primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies.

As discussed in Section IV(A) above, terms of service which are incorporated into a browsewrap or clickwrap agreement can, like any other type of contract, define the limits of authorized access as to a website and its concomitant computer/server(s). However, the question is whether individuals of "common intelligence" are on notice that a breach of a terms of service contract can become a crime under the CFAA. Arguably, they are not.

First, an initial inquiry is whether the statute, as it is written, provides sufficient notice. Here, the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has "criminalized breaches of contract" in the context of website terms of service. Normally, breaches of contract are not the subject of criminal prosecution. … Thus, while "ordinary people" might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties. … This would especially be the case where the services provided by MySpace are in essence offered at no cost to the users and, hence, there is no specter of the users "defrauding" MySpace in any monetary sense.

Second, if a website's terms of service controls what is "authorized" and what is "exceeding authorization" – which in turn governs whether an individual's accessing information or services on the website is criminal or not, section 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will. For example, in the present case, MySpace's terms of service prohibits a member from engaging in a multitude of activities on the website, including such conduct as "criminal or tortious activity," "gambling," "advertising to . . . any Member to buy or sell any products," "transmit[ting] any chain letters," "covering or obscuring the banner advertisements on your personal profile page," "disclosing your password to any third party," etc. The MSTOS does not specify which precise terms of service, when breached, will result in a termination of MySpace's authorization for the visitor/member to access the website. If any violation of any term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement.[25]

Third, by utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime, that approach makes the website owner – in essence – the party

[25] Another uncertainty is whether, once a user breaches a term of service, is every subsequent accessing of the website by him or her without authorization or in excess of authorization.

who ultimately defines the criminal conduct. This will lead to further vagueness problems. The owner's description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers. For example, the MSTOS prohibits members from posting in "band and filmmaker profiles . . . sexually suggestive imagery or any other unfair . . . [c]ontent intended to draw traffic to the profile." It is unclear what "sexually suggestive imagery" and "unfair content" mean. Moreover, website owners can establish terms where either the scope or the application of the provision are to be decided by them *ad hoc* and/or pursuant to undelineated standards. For example, the MSTOS provides that what constitutes "prohibited content" on the website is determined "in the sole discretion of MySpace.com. . . ." Additionally, terms of service may allow the website owner to unilaterally amend and/or add to the terms with minimal notice to users. …

V. CONCLUSION

For the reasons stated above, the Defendant's motion under F.R.Crim.P. 29(c) is GRANTED.

Questions

1. What did Drew do that was in violation of the MySpace terms of service? Did she know that she was in violation? Would the MySpace terms of service be enforceable as a contract?

2. The government's theory is that using a site in violation of its terms of service is access "without authorization." Compare this theory to the theories relied on by the *Morris* court.

3. The court agrees: violation of the terms of service is use without authorization. So Drew accessed MySpace's computers without authorization. But the court grants her motion for acquittal nonetheless. Why?

4. Another common scenario is the disloyal employee. Suppose that Samir has been given a password to log on to the Initech server and network for company business. One day, however, frustrated with a recalcitrant printer, he decides to jump ship for Initech's rival, Intertrode. He logs onto the Initech server and downloads the last year's worth of financial data, then resigns. Three months later, the Initech IT department is auditing its records and discovers what Samir has done. Initech refers the case to the local U.S. Attorney. Has Samir "exceeded authorized access?"

5. The federal CFAA also provides victims with a civil remedy. It gives "any person who suffers damage or loss by reason of a violation of this section" a civil action against the violator. Under the most commonly used prong, the CFAA has a $5,000 "loss" threshold and is limited to economic damages. *See* 18 U.S.C. § 1030(g). Does Myspace have a valid cause of action against Drew under this provision?

6. Is the CFAA a good fit for what Drew did? Why or why not? Has she committed any other crimes?

Armenian Computer Misuse Problem

Your law school classmate Noubar Akelian is now working as a criminal defense lawyer in his native Armenia. He has recently taken on a case that involves Armenia's computer-misuse statute, which is modeled on the United States's CFAA. Since there are very few Armenian precedents explaining the meaning of the terms used in the Armenian statute, he has asked you for guidance based on U.S. cases. Here are the facts as he explained them to you:

> His client is Linda Torosian. Her sister-in-law, Isabel, owned a computer. Isabel gave Linda an account on the computer, one that had no technical restrictions on what it could do. Isabel also told her that she could do anything she wanted with the computer *excep*t look in the Secret001 folder. One day,

> while Isabel was out of town, Linda looked inside the folder and discovered that Isabel had a secret collection of Justin Bieber MP3s.
>
> Isabel and Linda had a falling-out later that month. Isabel discovered that the Secret001 folder had been opened. One thing led to another, and Linda was charged with a violation of the computer misuse statute.

The Armenian statute reads, in relevant part:

> (a)
>
> > (1) Whoever recklessly and without authorization accesses a computer and thereby causes damage to said computer shall be punished in accordance with [the Armenian criminal code].
> >
> > (2) Whoever intentionally and without authorization accesses a computer and thereby obtains any thing of value shall be punished in accordance with [the Armenian criminal code]
>
> (b) If the damage as described in paragraph (1) of section (b) exceeds $5,000 to any victim or victims or the value of the thing obtained as described in paragraph (2) of section (b) exceeds $5,000, such offense shall be punished as a felony of the third degree. In all other cases it shall be punished as a misdemeanor of the fourth degree.
>
> (c) As used in this section –
>
> > …
> >
> > (6) The term "computer" shall mean an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, a portable hand-held calculator, or a similar device which is non-programmable or which does not contain any data storage facility.
> >
> > (7) "damage" shall mean any impairment to a computer or the integrity or availability of data, a program or system, or information, that causes loss to any person of $5,000 or more; modifies or impairs the medical examination, diagnosis, treatment or care of any person; causes or threatens physical injury or death to any person; or threatens public health or public safety.

At trial, Isabel testified that on her return, she noticed that two of the MP3s, which she purchased from Amazon's MP3 store for 89 cents each, were missing. Isabel spent $6,000 hiring a computer consultant to discover who had been using the computer and trying (without success) to recover the deleted MP3s. She claimed that no one besides herself and Linda had physical access to the computer. Linda admitted using the computer and looking inside the folder, but she denied playing the MP3s, deleting them, or doing anything else with them. Linda was then found guilty of violating both section (a)(1) and (a)(2) of the statute, and is to be sentenced for a felony violation of the act.

Noubar Akelian, your colleague, would like your advice on possible challenges to the conviction that he could raise on appeal.

III. Trespass to Chattels

Our final source of law for control over servers comes from the borderline between property law and tort law. If I use your computer without permission and cause it to burst into flames, it's generally accepted that you will have a valid lawsuit against me for trespass to chattels. The harder, more controversial questions arise when your use of the computer doesn't cause physical damage, but only some form of intangible trouble: deleted data, a slowed-down computer, or, perhaps, no visible harm at all.

Restatement (Second) of Torts

§ 158: Liability for Intentional Intrusions on Land

One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally

(a) enters land in the possession of the other, or causes a thing or a third person to do so, or

(b) remains on the land, or

(c) fails to remove from the land a thing which he is under a duty to remove.

§ 218: *Liability to Person in Possession*

One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,

(a) he dispossesses the other of the chattel, or

(b) the chattel is impaired as to its condition, quality, or value, or

(c) the possessor is deprived of the use of the chattel for a substantial time, or

(d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.

Question

In 2007, a group of Harvard students created a website named CrimsonReading.org, which allowed students to comparison-shop for textbooks. In order to make a list of the books for the upcoming semester, they visited the Coop, a local bookstore where most professors place their book orders, to copy down courses, book names, and ISBNs.[*] The Coop, which has a policy against copying down ISBNs, objected and asked the students to leave, eventually calling the police. It is undisputed that the ISBNs themselves are not copyrightable and that the Coop has no rights over the numbers themselves. Can the Coop use tort law to keep CrimsonReading at bay?

eBay, Inc. v. Bidder's Edge, Inc.

100 F. Supp. 2d 1058 (N.D. Cal. 2000)

Whyte, District Judge:

Plaintiff eBay, Inc.'s ("eBay") motion for preliminary injunction was heard by the court on April 14, 2000. The court has read the moving and responding papers and heard the argument of counsel. For the reasons set forth below, the court preliminarily enjoins defendant Bidder'sEdge, Inc. ("BE") from accessing eBay's computer systems by use of any automated querying program without eBay's written authorization.

[*] Short for International Standard Book Number, a 10- or 13-digit number that uniquely identifies an edition of a book.

I. BACKGROUND

eBay is an Internet-based, person-to-person trading site. eBay offers sellers the ability to list items for sale and prospective buyers the ability to search those listings and bid on items. The seller can set the terms and conditions of the auction. The item is sold to the highest bidder. The transaction is consummated directly between the buyer and seller without eBay's involvement. A potential purchaser looking for a particular item can access the eBay site and perform a key word search for relevant auctions and bidding status. eBay has also created category listings that identify items in over 2500 categories, such as antiques, computers, and dolls. Users may browse these category listing pages to identify items of interest.

Users of the eBay site must register and agree to the eBay User Agreement. Users agree to the seven page User Agreement by clicking on an "I Accept" button located at the end of the User Agreement. The current version of the User Agreement prohibits the use of "any robot, spider, other automatic device, or manual process to monitor or copy our web pages or the content contained herein without our prior expressed written permission." It is not clear that the version of the User Agreement in effect at the time BE began searching the eBay site prohibited such activity, or that BE ever agreed to comply with the User Agreement.

eBay currently has over 7 million registered users. Over 400,000 new items are added to the site every day. Every minute, 600 bids are placed on almost 3 million items. Users currently perform, on average, 10 million searches per day on eBay's database. Bidding for and sales of items are continuously ongoing in millions of separate auctions.

A software robot is a computer program which operates across the Internet to perform searching, copying and retrieving functions on the web sites of others. A software robot is capable of executing thousands of instructions per minute, far in excess of what a human can accomplish. Robots consume the processing and storage resources of a system, making that portion of the system's capacity unavailable to the system owner or other users. Consumption of sufficient system resources will slow the processing of the overall system and can overload the system such that it will malfunction or "crash." A severe malfunction can cause a loss of data and an interruption in services.

The eBay site employs "robot exclusion headers." A robot exclusion header is a message, sent to computers programmed to detect and respond to such headers, that eBay does not permit unauthorized robotic activity. Programmers who wish to comply with the Robot Exclusion Standard design their robots to read a particular data file, "robots.txt," and to comply with the control directives it contains.

To enable computers to communicate with each other over the Internet, each is assigned a unique Internet Protocol ("IP") address. When a computer requests information from another computer over the Internet, the requesting computer must offer its IP address to the responding computer in order to allow a response to be sent. These IP addresses allow the identification of the source of incoming requests. eBay identifies robotic activity on its site by monitoring the number of incoming requests from each particular IP address. Once eBay identifies an IP address believed to be involved in robotic activity … eBay may attempt to ignore ("block") any further requests from that IP address. Attempts to block requests from particular IP addresses are not always successful. …

Outgoing requests from remote users can be routed through … proxy servers and appear to originate from the proxy server. Incoming responses are then received by the proxy server and routed to the remote user. Information requests sent through such proxy servers cannot easily be traced back to the originating IP address and can be used to circumvent attempts to block queries from the originating IP address. Blocking queries from innocent third party proxy servers is both inefficient, because it creates an endless game of hide-and-seek, and potentially counterproductive, as it runs a substantial risk of blocking requests from legitimate, desirable users who use that proxy server.

BE is a company with 22 employees that was founded in 1997. The BE web site debuted in November 1998. BE does not host auctions. BE is an auction aggregation site designed to offer on-line auction buyers the ability to search for items across numerous on-line auctions without having to search each host site individually. As of March 2000, the BE web site contained information on more that five million items being auctioned on more than one hundred auction sites. BE also provides its users with additional auction-related services and information. The information available on the BE site is contained in a database of information that BE compiles through access to various auction sites such as eBay. When a user enters a search for a particular item at BE, BE searches its database and generates a list of every item in the database responsive to the search, organized by auction closing date and time. Rather than going to each host auction site one at a time, a user who goes to BE may conduct a single search to obtain information about that item on every auction site tracked by BE. It is important to include information regarding eBay auctions on the BE site because eBay is by far the biggest consumer to consumer on-line auction site. …

In early 1998, eBay gave BE permission to include information regarding eBay-hosted auctions for Beanie Babies and Furbies in the BE database. In early 1999, BE added to the number of person-to-person auction sites it covered and started covering a broader range of items hosted by those sites, including eBay. On April 24, 1999, eBay verbally approved BE crawling the eBay web site for a period of 90 days. The parties contemplated that during this period they would reach a formal licensing agreement. They were unable to do so. …

On November 9, 1999, eBay sent BE a letter reasserting that BE's activities were unauthorized, insisting that BE cease accessing the eBay site, alleging that BE's activities constituted a civil trespass and offering to license BE's activities. eBay and BE were again unable to agree on licensing terms. As a result, eBay attempted to block BE from accessing the eBay site; by the end of November, 1999, eBay had blocked a total of 169 IP addresses it believed BE was using to query eBay's system. BE elected to continue crawling eBay's site by using proxy servers to evade eBay's IP blocks. …

It appears that major Internet search engines, such as Yahoo!, Google, Excite and AltaVista, respect the Robot Exclusion Standard.

eBay now moves for preliminary injunctive relief preventing BE from accessing the eBay computer system …

II. Legal Standard

To obtain preliminary injunctive relief, a movant must demonstrate "either a likelihood of success on the merits and the possibility of irreparable injury, or that serious questions going to the merits were raised and the balance of hardships tips sharply in its favor." *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1517 (9th Cir. 1992) (citations omitted). …

III. Analysis

A. Balance of Harm

… According to eBay, the load on its servers resulting from BE's web crawlers represents between 1.11% and 1.53% of the total load on eBay's listing servers. eBay alleges both economic loss from BE's current activities and potential harm resulting from the total crawling of BE and others. In alleging economic harm, eBay's argument is that eBay has expended considerable time, effort and money to create its computer system, and that BE should have to pay for the portion of eBay's system BE uses. eBay attributes a pro rata portion of the costs of maintaining its entire system to the BE activity.

However, eBay does not indicate that these expenses are incrementally incurred because of BE's activities, nor that any particular service disruption can be attributed to BE's activities. eBay provides no support for the proposition that the pro rata costs of obtaining an item represent the appropriate measure of damages for unauthorized use. In contrast, California law appears settled that the appropriate measure of damages is the actual harm inflicted by the conduct: …

eBay's allegations of harm are based, in part, on the argument that BE's activities should be thought of as equivalent to sending in an army of 100,000 robots a day to check the prices in a competitor's store. This analogy, while graphic, appears inappropriate. Although an admittedly formalistic distinction, unauthorized robot intruders into a "brick and mortar" store would be committing a trespass to real property. There does not appear to be any doubt that the appropriate remedy for an ongoing trespass to business premises would be a preliminary injunction. More importantly, for the analogy to be accurate, the robots would have to make up less than two out of every one-hundred customers in the store, the robots would not interfere with the customers' shopping experience, nor would the robots even be seen by the customers. Under such circumstances, there is a legitimate claim that the robots would not pose any threat of irreparable harm. However, eBay's right to injunctive relief is also based upon a much stronger argument.

If BE's activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses. BE does not appear to seriously contest that reduced system performance, system unavailability or data loss would inflict irreparable harm on eBay consisting of lost profits and lost customer goodwill. Harm resulting from lost profits and lost customer goodwill is irreparable because it is neither easily calculable, nor easily compensable and is therefore an appropriate basis for injunctive relief. Where, as here, the denial of preliminary injunctive relief would encourage an increase in the complained of activity, and such an increase would present a strong likelihood of irreparable harm, the plaintiff has at least established a possibility of irreparable harm. …

BE correctly observes that there is a dearth of authority supporting a preliminary injunction based on an ongoing to trespass to chattels. In contrast, it is black letter law in California that an injunction is an appropriate remedy for a continuing trespass to real property. If eBay were a brick and mortar auction house with limited seating capacity, eBay would appear to be entitled to reserve those seats for potential bidders, to refuse entrance to individuals (or robots) with no intention of bidding on any of the items, and to seek preliminary injunctive relief against non-customer trespassers eBay was physically unable to exclude. The analytic difficulty is that a wrongdoer can commit an ongoing trespass of a computer system that is more akin to the traditional notion of a trespass to real property, than the traditional notion of a trespass to chattels, because even though it is ongoing, it will probably never amount to a conversion. The court concludes that under the circumstances present here, BE's ongoing violation of eBay's fundamental property right to exclude others from its computer system potentially causes sufficient irreparable harm to support a preliminary injunction. …

B. Likelihood of Success

… The court finds that eBay has established a sufficient likelihood of prevailing on the trespass claim to support the requested injunctive relief. …

1. *Trespass*

Trespass to chattels "lies where an intentional interference with the possession of personal property has proximately cause injury." *Thrifty-Tel v. Bezenek*, 46 Cal. App.4th 1559, 1566 (1996). Trespass to chattels "although seldom employed as a tort theory in

California" was recently applied to cover the unauthorized use of long distance telephone lines.Id. Specifically, the court noted "the electronic signals generated by the [defendants'] activities were sufficiently tangible to support a trespass cause of action." *Id.* at n. 6. Thus, it appears likely that the electronic signals sent by BE to retrieve information from eBay's computer system are also sufficiently tangible to support a trespass cause of action.

In order to prevail on a claim for trespass based on accessing a computer system, the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff. *See Thrifty-Tel*, 46 Cal.App.4th at 1566, 54 Cal.Rptr.2d 468; Here, eBay has presented evidence sufficient to establish a strong likelihood of proving both prongs and ultimately prevailing on the merits of its trespass claim.

a. BE's Unauthorized Interference

eBay argues that BE's use was unauthorized and intentional. eBay is correct. BE does not dispute that it employed an automated computer program to connect with and search eBay's electronic database. BE admits that, because other auction aggregators were including eBay's auctions in their listing, it continued to "crawl" eBay's web site even after eBay demanded BE terminate such activity.

BE argues that it cannot trespass eBay's web site because the site is publicly accessible. BE's argument is unconvincing. eBay's servers are private property, conditional access to which eBay grants the public. eBay does not generally permit the type of automated access made by BE. In fact, eBay explicitly notifies automated visitors that their access is not permitted. …

Even if BE's web crawlers were authorized to make individual queries of eBay's system, BE's web crawlers exceeded the scope of any such consent when they began acting like robots by making repeated queries. Moreover, eBay repeatedly and explicitly notified BE that its use of eBay's computer system was unauthorized. The entire reason BE directed its queries through proxy servers was to evade eBay's attempts to stop this unauthorized access. The court concludes that BE's activity is sufficiently outside of the scope of the use permitted by eBay that it is unauthorized for the purposes of establishing a trespass. …

b. Damage to eBay's Computer System

A trespasser is liable when the trespass diminishes the condition, quality or value of personal property. The quality or value of personal property may be "diminished even though it is not physically damaged by defendant's conduct." *Id.* at 1022. The Restatement offers the following explanation for the harm requirement:

> The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected. … Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.

Restatement (Second) of Torts § 218 cmt. e (1977).

eBay is likely to be able to demonstrate that BE's activities have diminished the quality or value of eBay's computer systems. BE's activities consume at least a portion of plaintiff's bandwidth and server capacity. Although there is some dispute as to the percentage of queries on eBay's site for which BE is responsible, BE admits that it sends some 80,000 to 100,000 requests to plaintiff's computer systems per day. Although eBay does not claim that this consumption has led to any physical damage to eBay's computer system, nor does eBay provide any evidence to support the claim that it may have lost revenues or customers based on this use, eBay's claim is that BE's use is appropriating eBay's personal property by using valuable bandwidth and capacity, and necessarily compromising eBay's ability to use that capacity for its own purposes.

BE argues that its searches represent a negligible load on plaintiff's computer systems, and do not rise to the level of impairment to the condition or value of eBay's computer system required to constitute a trespass. However, it is undisputed that eBay's server and its capacity are personal property, and that BE's searches use a portion of this property. Even if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property. Accordingly, BE's actions appear to have caused injury to eBay and appear likely to continue to cause injury to eBay. If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value. California law does not require eBay to wait for such a disaster before applying to this court for relief. The court concludes that eBay has made a strong showing that it is likely to prevail on the merits of its trespass claim, and that there is at least a possibility that it will suffer irreparable harm if preliminary injunctive relief is not granted. eBay is therefore entitled to preliminary injunctive relief. …

Questions

1. What is eBay's commercial interest in keeping Bidder's Edge from accessing its servers? What is Bidder's Edge's interest in accessing them? Does this context influence how the court approaches the trespass to chattels issue?

2. If Bidder's Edge had caused eBay's computers to burst into flames, which tort or torts could eBay have used? Trespass? Trespass to chattels?

3. Bidder's Edge didn't cause obvious physical harm. What *did* it do to eBay's computers? In what sense did it cause harm? Be as precise as you can. Are you convinced by the court's reasoning on this point? Do you think the court reached a fair and just overall result?

4. Describe, as precisely as you can, what a "robot" or a "spider" is. How does the "Robot Exclusion Standard" keep unwanted robots off of a web site? Is it easier for a search engine to ignore the Robot Exclusion Standard or to comply with its requests? In light of the Contracts section, *supra*, is a robots.txt file a valid contract?

5. When Bidder's Edge chose to ignore eBay's robots.txt file, eBay started blocking Bidder's Edge's IP address. How? And how did Bidder's Edge respond? Is law more or less necessary in a world in which both sides have access to these self-help techniques?

Intel v. Hamidi

71 P. 3d 296 (Cal. 2003)

Werdegar, Justice.:

Intel Corporation (Intel) maintains an electronic mail system, connected to the Internet, through which messages between employees and those outside the company can be sent and received, and permits its employees to make reasonable nonbusiness use of this system. On six occasions over almost two years, Kourosh Kenneth Hamidi, a former Intel employee, sent e-mails criticizing Intel's employment practices to numerous current employees on Intel's electronic mail system. Hamidi breached no computer security barriers in order to communicate with Intel employees. He offered to, and did, remove from his mailing list any recipient who so wished. Hamidi's communications to individual Intel employees caused neither physical damage nor functional disruption to the company's computers, nor did they at any time deprive Intel of the use of its computers. The contents of the messages, however, caused discussion among employees and managers.

On these facts, Intel brought suit, claiming that by communicating with its employees over the company's e-mail system Hamidi committed the tort of trespass to chattels. The trial court granted Intel's motion for summary judgment and enjoined Hamidi from any further mailings. A divided Court of Appeal affirmed.

After reviewing the decisions analyzing unauthorized electronic contact with computer systems as potential trespasses to chattels, we conclude that under California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property itself. … The consequential economic damage Intel claims to have suffered, i.e., loss of productivity caused by employees reading and reacting to Hamidi's messages and company efforts to block the messages, is not an injury to the company's interest in its computers – which worked as intended and were unharmed by the communications – any more than the personal distress caused by reading an unpleasant letter would be an injury to the recipient's mailbox, or the loss of privacy caused by an intrusive telephone call would be an injury to the recipient's telephone equipment. …

Factual and Procedural Background

We review a grant of summary judgment de novo; we must decide independently whether the facts not subject to triable dispute warrant judgment for the moving party as a matter of law. … The pertinent undisputed facts are as follows.

Hamidi, a former Intel engineer, together with others, formed an organization named Former and Current Employees of Intel (FACE-Intel) to disseminate information and views critical ofIntel's employment and personnel policies and practices. FACE-Intel maintained a Web site (which identified Hamidi as Webmaster and as the organization's spokesperson) containing such material. In addition, over a 21-month period Hamidi, on behalf of FACE-Intel, sent six mass e-mails to employee addresses on Intel's electronic mail system. The messages criticized Intel's employment practices, warned employees of the dangers those practices posed to their careers, suggested employees consider moving to other companies, solicited employees' participation in FACE-Intel, and urged employees to inform themselves further by visiting FACE-Intel's Web site. The messages stated that recipients could, by notifying the sender of their wishes, be removed from FACE-Intel's mailing list; Hamidi did not subsequently send messages to anyone who requested removal.

Each message was sent to thousands of addresses (as many as 35,000 according to FACE-Intel's Web site), though some messages were blocked by Intel before reaching employees. Intel's attempt to block internal transmission of the messages succeeded only in part; Hamidi later admitted he evaded blocking efforts by using different sending computers. When Intel, in March 1998, demanded in writing that Hamidi and FACE-Intel stop sending e-mails to Intel's computer system, Hamidi asserted the organization had a right to communicate with willing Intel employees; he sent a new mass mailing in September 1998.

The summary judgment record contains no evidence Hamidi breached Intel's computer security in order to obtain the recipient addresses for his messages; indeed, internal Intel memoranda show the company's management concluded no security breach had occurred. Hamidi stated he created the recipient address list using an Intel directory on a floppy disk anonymously sent to him. Nor is there any evidence that the receipt or internal distribution of Hamidi's electronic messages damaged Intel's computer system or slowed or impaired its functioning. Intel did present uncontradicted evidence, however, that many employee recipients asked a company official to stop the messages and that staff time was consumed in attempts to block further messages from FACE-Intel. According to the FAC-Intel Web site, moreover, the messages had prompted discussions between "[e]xcited and nervous managers" and the company's human resources department.

Intel sued Hamidi and FACE-Intel, pleading causes of action for trespass to chattels and nuisance, and seeking both actual damages and an injunction against further e-mail messages. Intel later voluntarily dismissed its nuisance claim and waived its demand for damages. …

I. Current California Tort Law

Dubbed by Prosser the "little brother of conversion," the tort of trespass to chattels allows recovery for interferences with possession of personal property "not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered." (Prosser & Keeton, Torts (5th ed. 1984) § 14, pp. 85-86.)

Though not amounting to conversion, the defendant's interference must, to be actionable, have caused some injury to the chattel or to the plaintiffs rights in it. …

The Restatement, too, makes clear that some actual injury must have occurred in order for a trespass to chattels to be actionable. Under section 218 of the Restatement Second of Torts, dispossession alone, without further damages, is actionable (*see id.*, par. (a) & com. d, pp. 420-421), but other forms of interference require some additional harm to the personal property or the possessor's interests in it. (*Id.*, pars, (b)-(d).) "The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. *Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c).* Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference." (*Id.*, com. e, pp. 421-422.) …

Intel suggests that the requirement of actual harm does not apply here because it sought only injunctive relief, as protection from future injuries. But as Justice Kolkey, dissenting below, observed, "[t]he fact the relief sought is injunctive does not excuse a showing of injury, whether actual or threatened." Indeed, in order to obtain injunctive relief the plaintiff must ordinarily show that the defendant's wrongful acts threaten to cause irreparable injuries, ones that cannot be adequately compensated in damages. …

The dispositive issue in this case, therefore, is whether the undisputed facts demonstrate Hamidi's actions caused or threatened to cause damage to Intel's computer system, or injury to its rights in that personal property, such as to entitle Intel to judgment as a matter of law. To review, the undisputed evidence revealed no actual or threatened damage to Intel's computer hardware or software and no interference with its ordinary and intended operation. Intel was not dispossessed of its computers, nor did Hamidi's messages prevent Intel from using its computers for any measurable length of time. Intel presented no evidence its system was slowed or otherwise impaired by the burden of delivering Hamidi's electronic messages. Nor was there any evidence transmission of the messages imposed any marginal cost on the operation of Intel's computers. In sum, no evidence suggested that in sending messages through Intel's Internet connections and internal computer system Hamidi used the system in any manner in which it was not intended to function or impaired the system in any way. Nor does the evidence show the request of any employee to be removed from FACE-Intel's mailing list was not honored. The evidence did show, however, that some employees who found the messages unwelcome asked management to stop them and that Intel technical staff spent time and effort attempting to block the messages. A statement on the FACE-Intel Web site, moreover, could be taken as an admission that the messages had caused "[e]xcited and nervous managers" to discuss the matter with Intel's human resources department.

Relying on a line of decisions, most from federal district courts, applying the tort of trespass to chattels to various types of unwanted electronic contact between computers, Intel contends that, while its computers were not damaged by receiving Hamidi's messages, its interest in the "physical condition, quality or value" (Rest.2d Torts, § 218, com. e, p. 422) of the computers was harmed. We disagree. The cited line of decisions does not persuade us that the mere sending of electronic communications that assertedly cause injury only because of their contents constitutes an actionable trespass to a computer system through which the messages are transmitted. Rather, the decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' functioning.

In *Thrifty-Tel, Inc. v. Bezenek*, *supra*, 46 Cal. App. 4th at pages 1566-1567 (*Thrifty-Tel*), the California Court of Appeal held that evidence of automated searching of a telephone carrier's system for authorization codes supported a cause of action for trespass to chattels. The defendant's automated dialing program "overburdened the [plaintiffs] system, denying some subscribers access to phone lines" (*Id.*, at p. 1564), showing the requisite injury.

Following *Thrifty-Tel*, a series of federal district court decisions held that sending UCE through an ISP's equipment may constitute trespass to the ISP's computer system. The lead case, *CompuServe, Inc. v. Cyber Promotions, Inc.*, *supra*, 962 F.Supp. 1015, 1021-1023 (*CompuServe*), was followed by *Hotmail Corp. v. Van$ Money Pie, Inc.* (N.D. Cal., Apr. 16, 1998, No. C 98-20064 JW) 1998 WL 388389, page *7, *America Online, Inc. v. IMS* (E.D. Va. 1998) 24 F. Supp. 2d 548, 550-551, and *America Online, Inc. v. LCGM, Inc.* (E.D. Va.1998) 46 F. Supp. 2d 444, 451-452.

In each of these spamming cases, the plaintiff showed, or was prepared to show, some interference with the efficient functioning of its computer system. In *CompuServe*, the plaintiff ISP's mail equipment monitor stated that mass UCE mailings, especially from nonexistent addresses such as those used by the defendant, placed "a tremendous burden" on the ISP's equipment, using "disk space and draining] the processing power," making those resources unavailable to serve subscribers. (*Compu-Serve*, *supra*, 962 F.

Supp. at p. 1022.) Similarly, in *Hotmail Corp. v. Van$ Money Pie, Inc.*, *supra*, 1998 WL 388389 at 7, the court found the evidence supported a finding that the defendant's mailings "fill[ed] up Hotmail's computer storage space and threatened to damage Hotmail's ability to service its legitimate customers." …

In the leading case, *eBay*, the defendant Bidder's Edge (BE), operating an auction aggregation site, accessed the eBay Web site about 100,000 times per day, accounting for between 1 and 2 percent of the information requests received by eBay and a slightly smaller percentage of the data transferred by eBay. (*eBay*, *supra*, 100 F. Supp. 2d at pp. 1061, 1063.) The district court rejected eBay's claim that it was entitled to injunctive relief because of the defendant's unauthorized presence alone, or because of the incremental cost the defendant had imposed on operation of the eBay site, but found sufficient proof of *threatened* harm in the potential for others to imitate the defendant's activity: "If BE's activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses." (*Id.* at p. 1066.) Again, in addressing the likelihood of eBay's success on its trespass to chattels cause of action, the court held the evidence of injury to eBay's computer system sufficient to support a preliminary injunction: "If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value." (*Id.* at pp. 1071-1072.) …

That Intel does not claim the type of functional impact that spammers and robots have been alleged to cause is not surprising in light of the differences between Hamidi's activities and those of a commercial enterprise that uses sheer quantity of messages as its communications strategy. Though Hamidi sent thousands of copies of the same message on six occasions over 21 months, that number is minuscule compared to the amounts of mail sent by commercial operations. The individual advertisers sued in *America Online, Inc. v. IMS*, *supra*, 24 F. Supp. 2d at page 549, and *America Online, Inc. v. LCGM, Inc.*, *supra*, 46 F. Supp. 2d at page 448, were alleged to have sent more than 60 million messages over 10 months and more than 92 million messages over seven months, respectively. Collectively, UCE has reportedly come to constitute about 45 percent of all e-mail. (Hansell, *Internet Is Losing Ground in Battle Against Spam*, N.Y. Times (Apr. 22, 2003) p. A1, col. 3.) The functional burden on Intel's computers, or the cost in time to individual recipients, of receiving Hamidi's occasional advocacy messages cannot be compared to the burdens and costs caused ISP's and their customers by the ever-rising deluge of commercial e-mail.

Intel relies on language in the eBay decision suggesting that unauthorized use of another's chattel is actionable even without any showing of injury: "Even if, as [defendant] BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property." (*eBay*, *supra*,100 F. Supp. 2d at p. 1071.) But as the eBay court went on immediately to find that the defendant's conduct, if widely replicated, would likely impair the functioning of the plaintiffs system, we do not read the quoted remarks as expressing the court's complete view of the issue. In isolation, moreover, they would not be a correct statement of California or general American law on this point. While one may have no right temporarily to use another's personal property, such use is actionable as a trespass only if it "has proximately caused injury." (*Thrifty-Tel*, *supra*, 46 Cal.App. 4th at p. 1566, 54 Cal. Rptr. 2d 468.) … That Hamidi's messages temporarily used some portion of the Intel computers' processors or storage is, therefore, not enough; Intel must, but does not, demonstrate some measurable loss from the use of its computer system. …

This theory of "impairment by content" (Burk, *The Trouble with Trespass*, *supra*, 4 J. Small & Emerging Bus.L. at p. 37) threatens to stretch trespass law to cover injuries far afield from the harms to possession the tort evolved to protect. Intel's theory would expand the tort of trespass to chattels to cover virtually any unconsented-to communication that, solely because of its content, is unwelcome to the recipient or intermediate transmitter. As the dissenting justice below explained, "'Damage' of this nature – the distraction of reading or listening to an unsolicited communication – is not within the scope of the injury against which the trespass-to-chattel tort protects, and indeed trivializes it. After all, '[t]he property interest protected by the old action of trespass was that of possession; and this has continued to affect the character of the action.' (Prosser & Keeton on Torts, *supra*, § 14, p. 87.) Reading an e-mail transmitted to equipment designed to receive it, in and of itself, does not affect the possessory interest in the equipment. Indeed, if a chattel's receipt of an electronic communication constitutes a trespass to that chattel, then not only are unsolicited telephone calls and faxes trespasses to chattel, but unwelcome radio waves and television signals also constitute a trespass to chattel every time the viewer inadvertently sees or hears the unwanted program." We agree. While unwelcome communications, electronic or otherwise, can cause a variety of injuries to economic relations, reputation and emotions, those interests are protected by other branches of tort law; in order to address them, we need not create a fiction of injury to the communication system.

Nor may Intel appropriately assert a property interest in its employees' time. "The Restatement test clearly speaks in the first instance to the impairment of the chattel.… But employees are not chattels (at least not in the legal sense of the term)." (Burk, *The Trouble with Trespass*, *supra*, 4 J. Small & Emerging Bus.L. at p. 36.) Whatever interest Intel may have in preventing its employees from receiving disruptive communications, it is not an interest in personal property, and trespass to chattels is therefore not an action that will lie to protect it. Nor, finally, can the fact Intel staff spent time attempting to block Hamidi's messages be bootstrapped into an injury to Intel's possessory interest in its computers. To quote, again, from the dissenting opinion in the Court of Appeal: "[I]t is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage. Injury can only be established by the completed tort's consequences, not by the cost of the steps taken to avoid the injury and prevent the tort; otherwise, we can create injury for every supposed tort."

Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable. Hamidi did nothing but use the e-mail system for its intended purpose – to communicate with employees. The system worked as designed, delivering the messages without any physical or functional harm or disruption. These occasional transmissions cannot reasonably be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.

II. Proposed Extension of California Tort Law

We next consider whether California common law should be extended to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents are objectionable. We decline to so expand California law. Intel, of course, was not the recipient of Hamidi's messages, but rather the owner and possessor of computer servers used to relay the messages, and it bases this tort action on that ownership and possession. The property rule proposed is a rigid one, under which the sender of an electronic message would be strictly liable to the owner of equipment through which the communication passes – here, Intel – for any consequential injury flowing from the contents of the communication. The arguments of amici curiae and academic writers on this topic, discussed below, leave us highly doubtful whether creation of such a rigid property rule would be wise.

Writing on behalf of several industry groups appearing as amici curiae, Professor Richard A. Epstein of the University of Chicago urges us to excuse the required showing of injury to personal property in cases of unauthorized electronic contact between computers, "extending the rules of trespass to real property to all interactive Web sites and servers." The court is thus urged to recognize, for owners of a particular species of personal property, computer servers, the same interest in inviolability as is generally accorded a possessor of land. In effect, Professor Epstein suggests that a company's server should be its castle, upon which any unauthorized intrusion, however harmless, is a trespass.

Epstein's argument derives, in part, from the familiar metaphor of the Internet as a physical space, reflected in much of the language that has been used to describe it: "cyberspace," "the information superhighway," e-mail "addresses," and the like. Of course, the Internet is also frequently called simply the "Net," a term, Hamidi points out, "evoking a fisherman's chattel." A major component of the Internet is the World Wide "Web," a descriptive term suggesting neither personal nor real property, and "cyberspace" itself has come to be known by the oxymoronic phrase "virtual reality," which would suggest that any real property "located" in "cyberspace" must be "virtually real" property. Metaphor is a two-edged sword.

Indeed, the metaphorical application of real property rules would not, by itself, transform a physically harmless electronic intrusion on a computer server into a trespass. That is because, under California law, intangible intrusions on land, including electromagnetic transmissions, are not actionable as trespasses (though they may be as nuisances) unless they cause physical damage to the real property. … Since Intel does not claim Hamidi's electronically transmitted messages physically damaged its servers, it could not prove a trespass to land even were we to treat the computers as a type of real property. Some further extension of the conceit would be required, under which the electronic signals Hamidi sent would be recast as tangible intruders, perhaps as tiny messengers rushing through the "hallways" of Intel's computers and bursting out of employees' computers to read them Hamidi's missives. But such fictions promise more confusion than clarity in the law. …

More substantively, Professor Epstein argues that a rule of computer server inviolability will, through the formation or extension of a market in computer-to-computer access, create "the right social result." In most circumstances, he predicts, companies with computers on the Internet will continue to authorize transmission of information through e-mail, Web site searching, and page linking because they benefit by that open access. When a Web site owner does deny access to a particular sending, searching, or linking computer, a system of "simple one-on-one negotiations" will arise to provide the necessary individual licenses.

Other scholars are less optimistic about such a complete propertization of the Internet. Professor Mark Lemley of the University of California, Berkeley, writing on behalf of an amici curiae group of professors of intellectual property and computer law, observes that under a property rule of server inviolability, "each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel." The consequence for e-mail could be a substantial reduction in the freedom of electronic communication, as the owner of each computer through which an electronic message passes could impose its own limitations on message content or source. As Professor Dan Hunter of the University of Pennsylvania asks rhetorically: "Does this mean that one must read the 'Terms of Acceptable Email Usage' of every email system that one emails in the course of an ordinary day? If the University of Pennsylvania had a policy that sending a joke by email would be an unauthorized use of their system, then under the logic of [the lower court decision in this case], you commit 'trespass' if you emailed me a . . . cartoon." (Hunter, *Cyberspace as Place, and the Tragedy of the Digital Anticommons* (2003) 91 Cal. L.Rev. 439, 508-509.)

Web site linking, Professor Lemley further observes, "would exist at the sufferance of the linked-to party, because a Web user who followed a 'disapproved' link would be trespassing on the plaintiffs server, just as sending an e-mail is trespass under the [lower] court's theory." … A leading scholar of Internet law and policy, Professor Lawrence Lessig of Stanford University, has criticized Professor Epstein's theory of the computer server as quasi-real property, previously put forward in the *eBay* case, on the ground that it ignores the costs to society in the loss of network benefits: "eBay benefits greatly from a network that is open and where access is free. It is this general feature of the Net that makes the Net so valuable to users and a source of great innovation. And to the extent that individual sites begin to impose their own rules of exclusion, the value of the network as a network declines. If machines must negotiate before entering any individual site, then the costs of using the network climb." (Lessig, The Future of Ideas: The Fate of the Commons in a Connected World (2001) p. 171; …

We discuss this debate among the amici curiae and academic writers only to note its existence and contours, not to attempt its resolution. …

The Legislature has already adopted detailed regulations governing UCE. … It may see fit in the future also to regulate noncommercial e-mail, such as that sent by Hamidi, or other kinds of unwanted contact between computers on the Internet, such as that alleged in *eBay, supra*. But we are not persuaded that these perceived problems call at present for judicial creation of a rigid property rule of computer server inviolability. We therefore decline to create an exception, covering Hamidi's unwanted electronic messages to Intel employees, to the general rule that a trespass to chattels is not actionable if it does not involve actual or threatened injury to the personal property or to the possessor's legally protected interest in the personal property. No such injury having been shown on the undisputed facts, Intel was not entitled to summary judgment in its favor. …

Kennard, Justice, concurring: …

Intel has my sympathy. Unsolicited and unwanted bulk e-mail, most of it commercial, is a serious annoyance and inconvenience for persons who communicate electronically through the Internet, and bulk e-mail that distracts employees in the workplace can adversely affect overall productivity. But, as the majority persuasively explains, to establish the tort of trespass to chattels in California, the plaintiff must prove either damage to the plaintiffs personal property or actual or threatened impairment of the plaintiffs ability to use that property. Because plaintiff Intel has not shown that defendant Hamidi's occasional bulk e-mail messages to Intel's employees have damaged Intel's computer system or impaired its functioning in any significant way, Intel has not established the tort of trespass to chattels.

This is not to say that Intel is helpless either practically or legally. As a practical matter, Intel need only instruct its employees to delete messages from Hamidi without reading them and to notify Hamidi to remove their workplace e-mail addresses from his mailing lists. Hamidi's messages promised to remove recipients from the mailing list on request, and there is no evidence that Hamidi has ever failed to do so. From a legal perspective, a tort theory other than trespass to chattels may provide Intel with an effective remedy if Hamidi's messages are defamatory or wrongfully interfere with Intel's economic interests. Additionally, the Legislature continues to study the problems caused by bulk e-mails and other dubious uses of modern communication technologies and may craft legislation that accommodates the competing concerns in these sensitive and highly complex areas.

Accordingly, I join the majority in reversing the Court of Appeal's judgment.

Brown, Justice, dissenting:

Candidate A finds the vehicles that candidate B has provided for his campaign workers, and A spray paints the water soluble message, "Fight corruption, vote for A" on the bumpers. The majority's reasoning would find that notwithstanding the time it takes the workers to remove the paint and the expense they incur in altering the bumpers to prevent further unwanted messages, candidate B does not deserve an injunction unless the paint is so heavy that it reduces the cars' gas mileage or otherwise depreciates the cars' market value. Furthermore, candidate B has an obligation to permit the paint's display, because the cars are driven by workers and not B personally, because B allows his workers to use the cars to pick up their lunch or retrieve their children from school, or because the bumpers display B's own slogans. I disagree.

Intel has invested millions of dollars to develop and maintain a computer system. It did this not to act as a public forum but to enhance the productivity of its employees. Kourosh Kenneth Hamidi sent as many as 200,000 e-mail messages to Intel employees. The time required to review and delete Hamidi's messages diverted employees from productive tasks and undermined the utility of the computer system. "There may . . . be situations in which the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition." (Rest.2d Torts, § 218, com. h, p. 422.) This is such a case.

The majority repeatedly asserts that Intel objected to the hundreds of thousands of messages solely due to their content, and proposes that Intel seek relief by pleading content-based speech torts. This proposal misses the point that Intel's objection is directed not toward Hamidi's message but his use of Intel's property to display his message. Intel has not sought to prevent Hamidi from expressing his ideas on his Web site, through private mail (paper or electronic) to employees' homes, or through any other means like picketing or billboards. But as counsel for Intel explained during oral argument, the company objects to Hamidi's using Intel's property to advance his message.

Of course, Intel deserves an injunction even if its objections are based entirely on the e-mail's content. Intel is entitled, for example, to allow employees use of the Internet to check stock market tables or weather forecasts without incurring any concomitant obligation to allow access to pornographic Web sites. A private property owner may choose to exclude unwanted mail for any reason, including its content. …

Mosk, Justice, dissenting:

The majority hold that the California tort of trespass to chattels does not encompass the use of expressly unwanted electronic mail that causes no physical damage or impairment to the recipient's computer system. They also conclude that because a computer system is not like real property, the rules of trespass to real property are also inapplicable to the circumstances in this case. Finally, they suggest that an injunction to preclude mass, noncommercial, unwelcome e-mails may offend the interests of free communication.

I respectfully disagree and would affirm the trial court's decision. In my view, the repeated transmission of bulk e-mails by appellant Kourosh Kenneth Hamidi (Hamidi) to the employees of Intel Corporation (Intel) on its proprietary confidential email lists, despite Intel's demand that he cease such activities, constituted an actionable trespass to chattels. The majority fail to distinguish open communication in the public "commons" of the Internet from unauthorized intermeddling on a private, proprietary intranet. Hamidi is not communicating in the equivalent of a town square or of an unsolicited "junk" mailing through the United States Postal Service. His action, in crossing from the public Internet into a private intranet, is more like intruding into a private office mailroom, commandeering the mail cart, and dropping off unwanted broadsides on 30,000 desks. Because Intel's security measures have been circumvented by Hamidi, the majority leave Intel, which has exercised all reasonable self-help efforts, with no recourse unless he causes a malfunction or systems "crash." Hamidi's repeated intrusions did more than merely "prompt[ ] discussions between '[e]xcited and nervous managers' and the company's human resource department" (maj. opn., ante); they also constituted a misappropriation of Intel's private computer system contrary to its intended use and against Intel's wishes.

Questions

1. What harms did Hamidi cause to Intel, if any? Which of these is trespass to chattels intended to defend against? Which of them "count" in deciding whether Hamdi committed an actionable tort? Are you convinced that this case is consistent with *Bidder's Edge*? Are there any other differences in their facts that might help explain their divergent results?

2. The dissents in *Hamidi* ask pointed questions about the majority's reasoning. Explain Justice Brown's campaign-cars analogy and Justice Mosk's mail-cart analogy. How persuasive are they?

3. One of the policy angles discussed in Part II of *Hamidi* is the extent to which physical metaphors for online activity should drive the legal analysis. How persuasive do you find the court's treatment of the idea of cyberspace as a place? Have your views on this issue changed since the start of this section? This chapter? This book?

4. The other major policy angle is whether the actual damage rule will have good consequences for the Internet and society. Can you explain the basis of the dispute between Richard Epstein and Mark Lemley?

5. After *Hamidi*, is a trespass to chattels a viable way to claim misuse of a computer server in California? Elsewhere in the United States? Does a contract claim or a Computer Fraud and Abuse Act civil claim provide computer owners with an effective substitute? Is *Hamidi* a landmark in Internet law or an irrelevancy?

Wireless Router Problem

You are associate general counsel for the FixPoint Corporation, which makes consumer and enterprise networking equipment. You have recently become aware of an issue with your company's WX11N series of home wireless routers. Once daily, each router connects to a "time server" to reset its internal clock. Each router ships with a list of roughly 100 different time servers. Each time they check what time it is, they pick a random server from the list. The goal is to spread the burden of checking what time it is across a large number of servers, so that none of them bears an excessive burden.

Unfortunately, due to a bug in the WX11N's software, the random-number generator always returns "16" when it picks which time server to consult. That means that the roughly three million WX11Ns in consumers' homes are all querying the same time server at the University of Helsinki. Worse, due to another bug, they all do it at 2:00 AM local time. This leads to a flood of hundreds of thousands of queries to the time server at the University of Helsinki, which has caused it to crash on multiple occasions. The University is threatening to file suit and possibly also to deactivate it entirely.

Evaluate the legal risk the FixPoint Corporation faces. You have a meeting scheduled with the engineering team later today. Are there any questions you would want to ask them, either to evaluate the legal risks or to consider possible mitigation strategies?

LineJump Problem

National Airlines (whom you may remember from the PsychoTravel problem in Chapter 2, *supra*) has another problem with its website. National has an egalitarian boarding policy. It has no first-class or business-class seats, and boarding passes do not come with assigned seats. Instead, it has a "cattle call" at boarding; passengers pick their own seats on a first-come, first-served basis.

The only differentiation among passengers is that each boarding pass is printed with the letter "A," "B," or "C." Passengers in the A group board first, followed by the Bs, and the the Cs. The letters are assigned based on when the passengers checked in on National's website. The earlier passengers receive A passes, the middle passengers receive B passes, and the last passengers to check in receive C passes. To check in online, a passenger must go to nationalair.com and click on a tab marked "Check in." A window then opens in which the customer inputs his or her name and flight number. National's computers then retrieve the reservation and display s an image of the boarding pass for printing. Online checkin opens 24 hours before each flight.

LineJump's only line of business is assisting National passengers to secure A boarding passes so they can be among the first on the plane. Passengers holding National tickets log on to the linejump.com website and supply their names, flight numbers, and credit card information, and authorize LineJump to act as their agents. Once a passenger's boarding pass becomes available for checkin, a BoardFirst employee manually uses the "Check in" feature on National's website, then emails the passenger an image of the boardingpass to print. LineJump charges $5 per pass, and serves about 100 National passengers per day. It typically succeeds in obtaining A passes for 95 or more of them; it gives a full refund to any passenger for whom it is unable to obtain an A pass.

National believes that LineJump's use of its website violates its terms and conditions. The National homepage states in small black print at the bottom of each page that "use of the National website constitutes acceptance of our Terms and Conditions." The words "Terms and conditions" are in blue; they are a hyperlink which takes the user to the Terms and Conditions page on nationalair.com. In relevant part, the terms read:

> National's websites and any Company Information is available to you only to learn about, evaluate, or purchase National services and products. Unless you are an approved National travel agent, you may use the National website only for personal, non-commercial purposes. For example, third parties may not use the National web sites for the purpose of checking Customers in online or attempting to obtain for them a boarding pass in any certain boarding group.
>
> As a condition of your use of the National website, you promise that you will not use the National website for any purpose that is unlawful or prohibited by these terms and conditions.

On December 20, 2010, National sent a cease-and-desist letter to LineJump stating that National's terms and conditions prohibited the use of nationalair.com for commercial purposes and that LineJump's activities breached the Terms. When LineJump's use did not stop, National filed suit on May 17, 2011. Its complaint includes claims for breach of contract, trespass to chattels, and violation of the Computer Fraud and Abuse Act. National and LineJump have filed cross motions for summary judgment. How should the court rule?