

209 On the Trail of the Cybercriminal—The Role of In-house Counsel

Michael Finn

Vice President & General Counsel
Sideware Corporation

Jay Monahan

Associate General Counsel, Intellectual Property
eBay Inc.

Charles A.B. Moore

Associate Counsel
Federated Department Stores, Inc.

Christopher M.E. Painter

Deputy Chief of the Computer Crime and Intellectual Property Section
Department of Justice

Faculty Biographies

Michael Finn

Michael Finn is general counsel and vice president of business affairs for Sideware Corporation, a web collaboration software company. Mr. Finn has specialized in technology, telecommunications, and ecommerce transactions and policy matters.

Mr. Finn previously worked at Teligent Inc., Willkie Farr and Gallagher, and the general counsel's office of the Federal Communications Commissions. He clerked for Judge Frank M. Johnson, Jr. on the 11th Circuit and for Chief Bankruptcy Judge (EDNY) Conrad B. Duberstein.

Mr. Finn received his JD from New York University School of Law.

Jay Monahan

Jay Monahan is associate general counsel, intellectual property for eBay Inc., the leading internet online trading community. He manages worldwide intellectual property matters for the company, including the Verified Rights Owner (VeRO) Program (infringing items), copyright, patent and trademark prosecutions, domain registrations and enforcement, and other IP enforcement matters, spam, and litigation concerning unauthorized robots and other access to the eBay site.

Prior to joining eBay, Mr. Monahan was vice president, worldwide antipiracy for Walt Disney Pictures & Television. He also has been a high technology IP litigator with Brown & Bain in Palo Alto, California, and a general litigator with the Los Angeles office of Morrison & Foerster.

Mr. Monahan is a graduate of the University of California, Hastings College of Law, where he has editor in chief of *COMMENT*, The Hastings Journal of Communications and Entertainment Law. He also graduated Phi Beta Kappa from the University of California at Berkeley.

Charles A.B. Moore

Charles A.B. Moore is associate counsel with Federated Department Stores in Atlanta, Georgia. His responsibilities include electronic commerce, technology, commercial contracts, and regulatory matters.

Prior to joining Federated, Mr. Moore was transactional counsel for United Parcel Service in Atlanta and in private practice in Connecticut.

Mr. Moore has been a member of ACCA for more than 10 years. He currently serves as cochair of ACCA's eCommerce Committee and is a nominee to ACCA's board of directors. Mr. Moore is president of ACCA's Georgia Chapter and is chair of the Chapter's

eCommerce Committee as well. He is a member of the Computer Law Association and a frequent speaker on eCommerce issues. Most recently, Mr. Moore has been featured in the *ACCA Docket* issue on eCommerce and coauthored an article on internet taxation for the *ACCA Docket*. Mr. Moore is a member of the board of directors for the Carrie Steele-Pitts Home in Atlanta, which provides a secure home for neglected and abused children.

Mr. Moore is a graduate of Trinity College and received his JD from Vermont Law School.

Christopher M.E. Painter

Christopher M.E. Painter is a deputy chief of the computer crime and intellectual property section at the Department of Justice. In that position he supervises the section's case and policy efforts concerning computer network intrusions, intellectual property matters, legislative, and other issues.

Prior to his work at the Department of Justice, Mr. Painter was a criminal prosecutor in the U.S. Attorney's Office for the Central District of California (Los Angeles). During his tenure in Los Angeles, Mr. Painter specialized in the investigation and prosecution of high-tech, intellectual property, and computer crimes and served as a computer crime and internet fraud coordinator for his office. He subsequently clerked for the Honorable Betty Fletcher of the U.S. Court of Appeals for the Ninth Circuit before practicing law at the Washington, DC law firm of Arnold and Porter.

Mr. Painter serves on several Department of Justice and interagency working groups relating to computer hackers, internet fraud investigations and prosecutions, electronic evidence, intellectual property crimes, and thefts of trade secrets. He is also cochair of an ABA White Collar Crime Subcommittee on Computer Crime. He has lectured extensively and has appeared on 60 minutes, CNN, CBS Morning News, the BBC, and has testified before Congress concerning computer crime issues.

Mr. Painter received his BA from Cornell University and JD from Stanford Law School. He was a senior editor of the *Stanford Law Review* and graduated Order of the Coif.

Anonymous Chat-Board Postings: An Overview

Michael F. Finn
General Counsel &
VP Business Affairs
Sideware Corp.
1810 Samuel Morse Drive
Reston, VA 20190
703.437.9002
mfinn@bellatlantic.net

Anonymous Chat-Board Postings:

An Overview

Today, most companies have official Web sites dedicated to providing information about their products, services, background, and management team. There are also numerous "unofficial" Web sites and chat boards which permit individuals (including company employees) to post anonymously information that may or may not be true and which may or may not be competitively sensitive. Postings that are anonymous and derogatory are known as "cybersmears."

Cybersmears often involve derogatory comments about members of senior management or the company's business plans, etc. When confronted with an anonymous cybersmear, many companies have chosen to file a "John Doe" lawsuit and to seek discovery on the true identity of the anonymous poster. Such lawsuits are often grounded on defamation or, if the John Doe is alleged to be an employee, breach of confidentiality agreements.

As in-house counsel, it is critical that you ensure that any such "John Doe" suits be filed for legitimate reasons and not simply to unmask an anonymous employee in order to discipline them for legally-permitted speech, *i.e.*, stating that the CEO is an idiot. Several John Does have been able to quash subpoenas and even to receive their legal fees because the underlying complaint brought by the company did not state a claim upon which relief could be granted.

A. Filing a "John Doe" Lawsuit

Below is the kind of message one might find on BizBoards about the fictitious company Buonomo Corp. and its equally fictitious Chief Executive Officer, Nick Hearmore.:

Author: A Goodfriend of Buonomo

Re: Nick Hearmore is a fool

Nick Hearmore has shown no skills at running this company whatsoever. From what I hear from employees, he simply sits around all day playing computer basketball. Yeah, he better get to the gym. From the picture on the Web site, he has been eating a few too many jelly doughnuts. The guy looks like he swallowed a horse....wonder what his wife thinks. Bet she doesn't go near the big turkey.

Seriously folks, we are due for a real drop in price. I learned from employees that Hearmore's chief deputy, James Butty, has left the company. James was the one who did all the heavy lifting and really built and ran operations. People, confidence, and our stock price will definitely drop.

Assuming Buonomo Corp. decided to file a lawsuit against the poster, known as "A Goodfriend of Buonomo", the case most likely would occur in the following procedural manner.

1. Buonomo Corp. files a complaint against "John Doe"
2. Issuance of subpoena to the company running the chat board. In this example, it is BizBoards. In the real world, it could be Yahoo!, Motley Fool, AOL, CNBC, etc.
3. The chat board companies generally have nothing more than the actual email account of the person posting on the board. Thus, in response to the subpoena in our example, BizBoards might respond as follows: The identity of "A Goodfriend of Buonomo" corresponds to the following email address: cap12xx@yahoo.com.
4. With the above information in hand, a second subpoena would issue to Yahoo! for the identity of cap12xx@yahoo.com. If Yahoo! had information to identify the person and complied with the subpoena, you would then learn the poster's actual identity.
5. The complaint would be amended to the actual person's name.

Several of the chat boards and internet service providers will provide their members with notice that a subpoena has been filed seeking disclosure of the member's true identity and will allow a reasonable time for the member to file a motion to quash the subpoena prior complying. Consequently, it is possible that prior to compliance with step 3 or step 4, a motion to quash will be filed by the John Doe. The motion to quash may be filed and defended on an anonymous basis, i.e., the plaintiff will not learn the identity of the John Doe.

B. Caselaw

As shown below, case law on the rights of anonymous speech with respect to cybersmears is unsettled. Some cases favor a review of a complaint's merits by the court prior to unmasking a John Does. Others have permitted the subpoena without any type of prior review by the court.

1. Cases Favoring John Doe

One of the strongest cases supporting a John Doe's right to anonymous online criticism is Dendrite International Inc. v. John Does, et. al., 2001 N.J. Super. LEXIS 300 (Sup. Ct. N.J. App. Div. July 11, 2001). There, the appellate court upheld the lower court's denial of Dendrite International's motion to conduct discovery for the purpose of ascertaining the identify of certain John Does who posted chat messages alleging that Dendrite's CEO had manipulated revenue recognition to bolster earnings and that the company was for sale. The court held that prior to permitting discovery:

the plaintiff must:

- (i) set forth the exact statements which it alleges are actionable;
 - (ii) attempt to notify the anonymous posters that they are subject to a subpoena; and
 - (iii) provide a reasonable opportunity for such posters to oppose the subpoena;
- and

the trial court must determine:

- (i) whether the plaintiff has set forth a prima facie cause of action against the anonymous defendants such that the complaint on its face can survive a motion to dismiss for failure to state a claim;
- (ii) whether sufficient evidence on a prima facie basis exists for each element of the plaintiff's cause of action; and
- (iii) assuming (i) and (ii) are present, the trial court must then balance the anonymous defendant's First Amendment rights of anonymous free speech against the strength of the prima facie case presented and the necessity for disclosure of the anonymous defendant's identity

Applying the above principles, the court found that John Doe's statements about revenue recognition or the company being for sale -- which identified specific companies that purportedly had turned down the purchase -- had not been shown to have been false or to have harmed Dendrite. The court noted that stock analysts had questioned Dendrite's revenue recognition and that Dendrite had not shown that its stock price fell due to the postings.

Another strong case for John Does is Global Telemedia Int. v. Doe, 132 F. Supp. 2d 1261 (C.D. Cal. 2001). There, the plaintiff Global Telemedia was ordered to pay \$55,000 of Doe's attorneys fees because the court found that the complaint lacked merit and was designed to stifle lawful speech under California's Strategic Lawsuit Against Public Participation "SLAPP" laws. According to the court, the John Does had done little more than post negative opinions about Global Telemedia. Even assuming the opinions were facts, Global had failed to show harm such as a decline in stock price following the postings. Rather, the court found that the complaint constituted an attempt to stifle public discussion under SLAPP and, pursuant to that law, awarded attorneys' fees to the defendants who, in reality, were investors located in the Midwest.¹

¹ In Curzon-Brown v. Lathouwers, (N.D. Cal. 2000). two San Francisco City College professors brought a defamation suit in the Northern District of California against the webmaster of Teacher Review, a website offering anonymous reviews of teachers. The reviews ranged from praise to several that were extremely profane and homophobic and included statements calling one of the plaintiffs a

Likewise in Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, (W.D. Wash. 2001), the court granted the John Does' motion to quash subpoenas that had been issued against 23 Does. The plaintiff company, TMRT, sought their identity as part of one of its defenses in an ongoing shareholder lawsuit – TMRT's defense was that the shareholders were harmed due to the postings and not due to actions of the company. One poster, for example, said "TMRT is a Ponzi scam that Charles Ponzi would be proud of. . . . The company's CEO, . . . has defrauded employees in the past. The company's other large shareholder, . . ., defrauded customers in the past." The Court found four factors to evaluate a civil subpoena seeking the identity of an anonymous Internet user who is not a party to the underlying litigation:

- (1) whether the subpoena seeking the information was issued in good faith and not for any improper purpose;
- (2) whether the information sought relates to a core claim or defense of the plaintiff;
- (3) whether the identifying information is directly and materially relevant to that claim or defense; and
- (4) whether information sufficient to establish or to disprove that claim or defense is unavailable from any other source.

Most recently, on August 10, 2001, a California state court quashed a subpoena issued by Pre-Paid Legal Services requesting the identity of 8 John Does posting critical messages on Yahoo!'s chat boards. The company argued that it needed the Does' identities to determine compliance with a court injunction forbidding certain ex-employees from disclosing trade secrets. The Electronic Freedom Foundation defended the John Does, asserting that no trade secrets had been disclosed and that the true reason for the subpoena was to permit the company to ascertain whether the Does were employees and, if so, to punish them for constitutionally-protected speech. Ruling from the bench, the Honorable Neil Cabrinha of the Santa Clara County Superior Court quashed the subpoena, noting the messages did not appear to violate the injunction, and therefore the First Amendment protection of anonymous speech outweighed PPLS's interest in learning the identity of the speakers.

"fuc*ing faggot" who would "die of AIDs". The professors dropped their complaint and agreed to pay \$10,000 in legal fees to the defendant due to concerns that the court would award a higher amount to the defendant. An article discussing this case is located at www.wired.com/news/politics/0,1283,39258,00.html.

2. Cases Favoring Unmasking John Doe

The same day that it issued its Dendrite decision, the same New Jersey court reached the opposite conclusion in Immunomedics v. Jean Doe, 2001 N.J. Super. LEXIS 299 (Sup. Ct. N.J. App. Div. July 11, 2001). Applying Dendrite, the court found that sufficient evidence exists to identify a "Jean Doe" who had, in anonymous postings on Yahoo!, stated that she was a "worried employee" and that Immunomedics was "out of stock for diagnostic products in Europe" and that there would be "no more sales if [the] situation [did] not change." In a second message, Doe reported that Immunomedics Chairman was going to fire the Immunomedics "European manager." In its complaint, Immunomedics stated that information posted by Doe was true, that Doe must therefore be an employee, and that such posting violated the employee's confidentiality agreement.

In a case closely followed by the press, Hvides v. Does 1-8, 770 So. 2d 1237 (App. Div. Fl. 2000), a Florida Appellate Court affirmed without opinion a lower court order that Yahoo! and AOL must comply with a subpoena and unveil the names of John Doe's so that they may formally be named. The John Does had alleged that the CEO of Hvide Marine, Inc., Eric Hvide, was under SEC investigation and engaging in illegal accounting practices. The Does attempted to quash the subpoenas claiming First Amendment protection for Internet postings, even those that are defamatory. The lower court declined to first decide whether the complaint was sufficiently detailed to warrant a lawsuit and instead ordered compliance with the subpoenas.

In Melvin v. Doe, 49 Pa. D. & C.4th 449, 2000 Pa. D. & C. LEXIS 242 (2000), the court granted discovery into the identity of John Does who published statements on a website accusing Superior Court Judge Joan Orié Melvin of unlawfully lobbying the governor on behalf of a local attorney to fill a vacancy on the Allegheny Court of Common Pleas. Melvin filed a defamation action and sought to obtain the identity of the John Does. In response, the publisher of the website. The John Doe defendants sought a protective order preventing Melvin from conducting any discovery to determine their identity. The court found that Melvin had made a prima facie showing that the statements were false, were defamatory, and had caused her harm redressable by money damages. It therefore permitted discovery.

One of the best-known John Doe cases involved Raytheon Inc. which, in February of 1999, filed suit in Massachusetts Superior Court against 21 employees it alleged posted or discussed confidential corporate information on a Yahoo! message board, in violation of their employment contracts and Raytheon's published employment policy, and that this conduct constituted misappropriation of Raytheon's trade secrets. To identify the "John Does," Raytheon sought and received a court order allowing its counsel to take out-of-state discovery from Yahoo, AOL, Earthlink and various other ISPs, seeking documents and information identifying the 21. Yahoo, after being served with a subpoena identified

the posters. In May, 1999, Raytheon dismissed the action, after several of the posters resigned.²

A California county Judge in Xircom, Inc. v. Doe, (Cal. Sup. Ct., June 14, 1999), required Yahoo! to unmask an anonymous John Doe who had claimed to be an employee of Xircom and had posted messages stating that the company produced faulty products, was losing people and was poorly managed. An article about the case may be found online at www.nytimes.com/library/tech/99/06/cyber/articles/15identity.html.

3. No Anonymity for Corporate Plaintiff

The Virginia Supreme Court has held that a corporate plaintiff may not, absent unusual circumstances, anonymously seek to obtain the identity of John Does who posted negative information online about the company. America Online v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001). XIS 38, 29 Media L. Rep. (BNA) 1442 (2001). The anonymous plaintiff filed its complaint in an Indiana state court alleging that various John Does which it believed to be company employees had made disparaging comments about the company in chat rooms. It further stated that disclosure of its identity would cause it to suffer irreparable harm. The court rejected those arguments, noting that there were only limited circumstances in which a plaintiff could proceed anonymously:

Whether the justification asserted by the requesting party is merely to avoid the annoyance and criticism that may attend any litigation or is to preserve privacy in a matter of sensitive and highly personal nature; whether identification poses a risk of retaliatory physical or mental harm to the requesting party or even more critically, to innocent non-parties; the ages of the persons whose privacy interests are sought to be protected; whether the action is against a governmental or private party; and, relatedly, the risk of unfairness to the opposing party from allowing an action against it to proceed anonymously.

AOL's motion to quash was granted because the company had not submitted evidence showing the harms resulting from disclosure of its identity.

² An earlier case with a similar outcome involved Itex Corp. which filed an action in September 1998 against 100 John Does on Yahoo! for posting false and defamatory statements about Itex's management, including referring to Itex's management as "blind, stupid, and incompetent." In response to a court order, Yahoo provided Itex with the authors' email addresses it had on file from which the company identified 5 of the Does.

Conclusion

Online chat rooms are filled with all types of anonymous statements about companies and their management team, from legitimate praise and criticism to rumor, innuendo and worse. Indeed, many CEO's and board members have been accused of crimes, affairs, etc. by anonymous postings on chat boards. More significant, some companies have had sensitive business information placed anonymously on boards.

The question of whether or not to bring a lawsuit can be difficult. As a practical matter, there are often so many rumors and statements on a chat board that it is difficult for any reader to know which, if any, are true. A lawsuit would do little more than lend credence to the message, a message whose content might otherwise be overlooked. Additionally, if the lawsuit is frivolous or designed to stifle public speech, your company may find itself in the position of having to pay the attorneys' fees of the John Doe. With respect to defamation claims, the best defense may be a thick skin by your company and its management team.

With respect to the disclosure of confidential and sensitive business information that could come only from an employee, the calculus may be quite different. In that case, it may be a matter of business imperative to discover which employee is disclosing the confidential information. In such case, filing of a John Doe complaint may be not only appropriate but also required in order to protect the business.

EXHIBIT LIST

Exhibit A – Bibliography of Cybersmear cases (reprinted with permission of Glasser Legal Works)

Exhibit B – Dendrite International

Exhibit C – Prototype Complaint in a John Doe Case

EXHIBIT A

http://www.cybersecuritieslaw.com/lawsuits/cases_corporate_cybersmears.htm



cyber
SecuritiesLaw
PUBLISHED BY GLASSER LEGALWORKS
[Blake A. Bell, Editor in Chief](#)

Monday, August 13

- Home
- News
- News Archive

- Bibliography

- Legislative Alert
- Hot Issues

- Internet Securities Law Links
- Securities Industry Links
- Discussion Groups

CyberSecuritiesLaw™ Case Digest _____

Corporate Cybersmear Lawsuits

▶ Amazon Natural Treasures, Inc., a Nevada Corporation, Plaintiff, vs. Janice Shell, Dean Dumont, D. Tod Pauly, Jeffrey Mitchell, Cynthia Demonte, Demonte & Associates, a New York corporation, Silicon Investor, a Delaware Corporation, Raging Bull, a Delaware Corporation, John Doe No. 1 A/K/A CarlW, Does 1 through CXIII, and Black Corporations I through XX, *Case No.: CV-5-00-0158-PMP-RLH (D. Nev., complaint for defamation, libel and tortious interference filed Jan. 2000).*

▶ American Eco Corp. v. John Doe

Noted in [American Eco Wins Libel Suit Against Internet Critic](#), Nat'l Post, Dec. 15, 1998, at C2; see also American Eco Corp. Press Release: American Eco and its Executives Awarded \$8.3 Million from Internet Libel Suit, Dec. 14, 1998.

▶ American Health Scan v. Technical Chem. and Prods., Inc.

Noted in press release: American Health Scan Files Libel Suit Against TCPI and Individuals Over Anonymous Yahoo! Postings, Business Wire, June 18, 1999

▶ Amway Corp. v. Procter & Gamble
(*Mich. Federal Court*).

Amway Corp. has filed a lawsuit in Michigan federal court against Procter & Gamble Co. alleging that P&G paid the author of a Web site to post "misleading" information about Amway. The Web site, located at <http://www.teleport.com/~schwartz/>, is entitled "Amway: The Untold Story," and includes court documents filed in lawsuits against Amway. See http://enquirer.com/editions/1998/10/15/bus_amwaypg15.html.

▶ AnswerThink Consulting Group Inc. v. John Doe, a/k/a/ Aquacool_2000
(*D. Ct. Fla.*).

Referenced in Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart); Michael D. Goldhaber, [Associate Is a Leading 'Cybersmear' Lawyer](#), *NYLJ.com Backpage* (Jul. 14, 2000).

▶ Appel and Bartlett v. [Unknown]
0015028 (11th Judicial Circuit Court, Dade County, Florida)

See As If They Need a Subpoena, Yahoo! Finance OSE [Message 14861](#) (June 19, 2000).

▶ Ben Ezra, Weinstein & Co. v. America Online, Inc.
(*D.N.M. 1999*).

Court granted summary judgment in favor of America Online in action where plaintiff alleged that AOL was responsible for injuries suffered by plaintiff when message board postings on AOL message board purportedly caused a decline in the plaintiff's stock price.

▶ BioShield Technologies, Inc. v. John Does 1-3

Noted in press release: [BioShield Institutes Legal Action To Stop Defamatory and Fraudulent Statements on Internet](#) Message Board, Business Wire, Sept. 2, 1999 .

▶ Bowker, et al. v. America Online, Inc.
No. 95L 013509 (*Cir. Ct. of Cook County, Ill., filed Sept. 12, 1995*).

▶ Bridge Publications v. John Doe

▶ David Bukstel, Edward Bukstel and Halfpenny, Incorporated v. AHT Corporation
(*N.Y. Sup. Ct. for County of Westchester*).

Cybersmear claims are counterclaims brought by AHT Corporation; Hon. James R. Cowhey, Judge; court vacated preliminary injunction granted on May 13, 1999 on grounds that plaintiffs' hands were "unclean" due to cybersmeas.

▶ Callaway Golf v. Steven Cade

See Apology by stevencade [Part 1 - Message No. 5820]; Part Two by

stevencade [Part 2 - Message No. 5821]. To read examples of the skepticism with which the apology initially was met, see Yeah Right by techshortie [Message No. 5822] and I Do Not Believe You by thebigcrankshaft [Message No. 5835]. See also Mike Freeman, Callaway Finds Internet Critic Was La Jolla Club Executive [Part 1], *The San Diego Union-Tribune*, Feb. 26, 2000 (scroll down to "Callaway Finds Internet Critic Was La Jolla Club Executive" for very beginning of article) (Part 2).

▶ Caremark Rx Inc. and Edwin "Mac" Crawford v. Mark E. Holiday, Neil S. Subin, Trendex Capital Management II Corp., et al., No. CV-00-0-767-9 (*N.D. Alabama, complaint filed Mar. 24, 2000*).

See New Filings: 'Reverse Pump and Dump' Suit Filed Against Individuals, Hedge Fund, Premier Issue (2000), e-Trading Legal Alert, at 4 (Andrews Publications); Companies Fight 'Cybersmear' But Will They Lose the Battle?, Premier Issue (2000), e-Trading Legal Alert, at 4 (Andrews Publications).

▶ Clipclop.com Enterprises and John Henry v. Stockhouse Media, Raging Bull and John Does 1 through 5 a/k/a WaveyDavey, Wavey, garpike, Montero and Cook81 (*Supreme Court of British Columbia, complaint filed Nov. 26, 1999*).

See Brent Mudry, [clipclop Tackles Raging Bull, Stockhouse, Five Posters](#) (Nov. 29, 1999) (Raging Bull CLOPF message board posting).

▶ Carnegie International v. [Executives of Ark Capital] (*D. Md., complaint filed on May 28, 1999*).

See [CNET News.com story](#).

▶ Cohr Inc. v. Does 1 Through 50 (*complaint filed in Los Angeles in August, 1998*).

See [Wired News story](#).

▶ Creditrust Corp. and Joseph K. Rensin, Plaintiffs, v. Enhance Financial Services Group, Inc., Asset Guaranty Insurance Co. and Charles Henneman, Defendants *Civ. Action No. WMN00966, Complaint and Jury Demand (D. Md., Northern Div., complaint filed Apr. 4, 2000)*.

▶ Credit Suisse First Boston v. Chuan Chang and John Does 1-10 (*S.D.N.Y., complaint filed Jul. 12, 2000*).

See [Investment Firm Files Suit Over Message Boards](#), Bloomberg News special to CNET News.com, Jul. 12, 2000; [Credit Suisse Sues Over Yahoo! Message Board](#), Reuters special to Excite News (Jul. 12, 2000); Elinor Abreu, [Yahoo Postings Prompt More Lawsuits](#), TheStandard (Jul. 14, 2000); Bill Murdoch, [Free Speech on Internet Under Question](#), The Irish Times on the Web (Jul. 17, 2000).

▶ Cummins Engine Company, Inc. v. John Does 1 through 100 *Case No. CV789553 (Superior Court of the State of California for the County of Santa Clara)*.

See [Subpoena, Yahoo! Finance CUM Message Board Message #2565](#) (June 22, 2000).

▶ Cyberguard Corp. v. John Does

Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg*

Times Online (May 28, 2000) (referenced in chart).

- ▶ Dendrite International, Inc., a New Jersey Corporation, Plaintiff, v. John Does Nos. 1 through 4 and Does 5 through 14, inclusive, Defendants
Docket No. MRSC-129-00 (Superior Court of N.J., Morris County Chancery Division -- General Equity Part) (complaint filed and order to show cause issued on June 20, 2000).

Dendrite International, Inc., a New Jersey Corporation, Plaintiff, v. John Does Nos. 1 through 4 and Does 5 through 14, inclusive, Defendants, Docket No. MRSC-129-00, [Order To Show Cause](#) (Superior Court of N.J., Morris County Chancery Division -- General Equity Part) (complaint filed and order to show cause issued on June 20, 2000); Dendrite International, Inc., a New Jersey Corporation, Plaintiff, v. John Does Nos. 1 through 4 and Does 5 through 14, inclusive, Defendants, Docket No. MRSC-129-00, [Memorandum of Public Citizen as Amicus Curiae in Opposition to the Requested Discovery](#) (Jul. 11, 2000); [Order To Show Cause](#) (Superior Court of N.J., Morris County Chancery Division -- General Equity Part) Derrick Henry, [Company Suing To Get Names of Online Critics](#), Associated Press special of Bergen County Record Online (Jul. 20, 2000); Aaron Elstein, [Public Citizen, ACLU File Briefs To Restrict Cybersmear Suits](#), Wall St. J. Interactive Ed. (Jul. 26, 2000).

- ▶ Epitope Inc. v. [Shortselling Stockbroker]

Lois Rosenbaum of Stoel Rives in Portland, Oregon reportedly represented Beaverton-based Epitope in a 1993 case against a stockbroker who posted critical remarks about the company on a public bulletin board administered by Prodigy. See [USA Today story](#).

- ▶ Flooring America Inc. v. John Does 1-34,
No. 0011 (D. Del.).

See New Filings: 'Reverse Pump and Dump' Suit Filed Against Individuals, Hedge Fund, Premier Issue (2000), e-Trading Legal Alert, at 4 (Andrews Publications); Companies Fight 'Cybersmear' But Will They Lose the Battle?, Premier Issue (2000), e-Trading Legal Alert, at 4 (Andrews Publications).

- ▶ Fonix Corp. v. John Does 1-10
(3rd District Court, Utah, complaint filed October 1999).

See Steven Oberbeck, [Online Remarks Are Out of Line](#), Salt Lake Tribune, Oct. 27, 1999;

- ▶ Fonix Corp. v. John Doe 1
(complaint filed 1996).

Gregg Wirth, [Tearing Down the Internet's Anonymous Posters](#), *CNET News.com* (Sept. 22, 1998).

- ▶ In re Fruit of the Loom Ltd. Pre-Litigation Discovery
(Cook County [Illinois] Circuit Court)

On Dec. 2, 1999, Dow Jones Newswires reported that "[t]he apparel maker has filed a pre-litigation discovery order with the Cook County Circuit Court in Illinois that requests that Yahoo! Inc. (YHOO) identify the legal names of two message-board participants who use the monikers 'expertone 2000' and

'prognosticator man"). See Nicole Ridgway, [Fruit of the Loom Seeking To Unmask Online Critics, Dow Jones Newswires](#) (Dec. 2, 1999) (pasted copy on Silicon Investor Message Board).

▶ Harbor Florida Bancshares v. John Doe
(*complaint filed July 1999 in Santa Clara County [California] Superior Court*).

Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart).

▶ Harken Energy Corp. v. John Does a/k/a "walking_soft" and "FearViciousRaptor_RippingSlashing"
(*Superior Court of the State of California, complaint filed November 12, 1999*).

See Howard Mintz, ['Cybersmear' Lawsuits Raise Privacy Concern](#), Silicon Valley News, SV.com at Mercury Center online, Nov. 28, 1999.

▶ Harbor Florida Bancshares v. John Doe
(*complaint filed July 1999 in Santa Clara County [California] Superior Court*).

See [Las Vegas Sun story](#).

▶ Harken Energy Corp. v. John Does a/k/a "walking_soft" and "FearViciousRaptor_RippingSlashing"
(*Superior Court of the State of California, complaint filed November 12, 1999*).

See Howard Mintz, ['Cybersmear' Lawsuits Raise Privacy Concern](#), Silicon Valley News, SV.com at Mercury Center online, Nov. 28, 1999.

▶ Healthcare Recoveries, Inc. v. John Doe a/k/a legal{HR1us and legal{HR15us
(*filed Jan. 13, 2000*).

See Harold J. Adams, [Louisville Firm Sues Over Data on Yahoo! - Company Critic Posts Material, Hides His Identity](#), *The Courier-Journal*, Jan. 13, 2000.

▶ HealthSouth Corp. v. Krum
Case No. 98-2812 (Pa. Ct. C.P. 1998).

Complaint alleges that defendant made anonymous posting falsely claiming that company and its CEO were engaged in fraud and that CEO's wife was having adulterous affair

▶ HealthSouth Corp. v. Landry
No. 455485M (Dist. Ct. La. 1999).

▶ Hemispherx Biopharma Inc. v. Manuel Asensio
(*Pennsylvania, complaint filed Sept. 1998*).

See [The Industry Standard story](#).

▶ Hitsgalore.com, Inc. v. Janice Shell, Paul Kersey, Mayor, Mr. Pink, Mshater and John Does 5-100
No. 99-1387-CIV-T-26C (M.D. Fla. 1999).

According to May 27, 1999 news report, company retained Carl F. Schoepl, Esq. of Schoepl & Burke, P.A. in Boca Raton, Florida and "plans to file a lawsuit in federal court against anonymous posters on the Internet. See [Business Wire press release](#). See also Hitsgalore.com Asserts Recent Class

Action Lawsuits Based on False and Misleading Bloomberg Report, Business Wire, June 16, 1999 (available via DowVision from Dow Jones).

▶ Hollywood.com v. John Does

Referenced in Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart).

▶ Horizon Hotels dba Carib Inn v. America Online
(Cook County, Illinois, complaint filed November 1995).

▶ Eric Hvide, Plaintiff v. John Does 1 through 8, persons presently unknown to Plaintiffs but whose true identities will be included in the amendments hereto when those identities are discovered, Defendants
Case No. 99-22831 CA01 (Circuit Court of the 11th Judicial Circuit in and for Miami, Dade County, Florida, complaint filed September 1999).

Referenced in Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in text of article and in chart). Brief of Amicus Curiae American Civil Liberties Union and American Civil Liberties Union of Florida dated February 18, 2000. See also Chris Gaither, Judge Orders AOL, Yahoo! To Identify Online Writer, *Miami Herald*, May 26, 2000; ACLU Florida Case of the Month - Anonymous Speech on the Internet: Hvide v. Does 1-8 (visited May 26, 2000); American Civil Liberties Union of Florida, Overview of the Anonymous Speech Case (visited May 26, 2000); American Civil Liberties Union of Florida, Legal Issues in the anonymous Speech Case (visited May 26, 2000); American Civil Liberties Union of Florida, Plaintiffs, Defendants and Attorneys Involved (May 26, 2000); American Civil Liberties Union of Florida, Frequently Asked Questions in the Anonymous Speech Case (visited May 26, 2000).

▶ Image Guided Technologies v. John Doe a/k/a Net Surfin Rat

Noted in Karen Auge, Firm Tries To Find "Net Surfin' Rat," *Denver Post*, March 22, 1999, at B1.

▶ Imaging Diagnostic Systems, Inc. v. Steven Cortopassi (a/k/a "docpatel")
(Cir. Court of the 17th Judicial Circuit, Broward County, Florida, final judgment entered on July 12, 2000) (Hon. Patricia Cocalis).

Imaging Diagnostic Systems, Inc., [Imaging Diagnostic Obtained Injunction in Cybersmear Lawsuit](#), Press Release distributed via PR Newswire (Jul. 14, 2000) (available via premium subscription library at Northernlight.com).

▶ Imperial Sugar Company v. John Does 1 - 8 (a/k/a "ducko-1999", "mouthofthesouth1961", "bestinthwest-95337", "midwestrader", "henryvii2040", "shawnelson", "irightuwrong", and "buy-lower-sell-higher")
(152nd District Court in Harris County, Texas [Houston Area], order entered Jul. 21, 2000).

Tasha Gatlin & Ben Werner, [Imperial Sugar Wants Secret Bashers Revealed](#), *Savannah Morning News on the Web* (Jul. 20, 2000); Ben Werner, [Court Orders Yahoo To Name Names](#), *Savannah Morning News on the Web* (Jul. 22, 2000).

▶ Informix v. Does 1-10, CV 413449
(San Mateo County Superior Court, Redwood City).

See [Subpoena for Those That Missed It](#), IFMX Yahoo! Finance Message Board Message #73054.

- ▶ InvestAmerica Inc. (Optica Communications Group Inc.) v. John Does 1 - 14 (*D. Mass., complaint filed May 23, 2000*).

See [InvestAmerica, Inc. Optica Communications Group Inc., Announces Defamation Action, Business Wire](#) (May 24, 2000) (pasted copy); see also Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in text of article).

- ▶ Itex Corp. and Graham Norris v. John Does 1 Through 100 No. 98-09-06393 (*Circuit Court of Oregon for the County of Multnomah in Portland, Oregon, original complaint filed week of Aug. 31, 1998*).

Greg Wirth, [Tearing Down the Internet's Anonymous Posters](#), CNET News.com (Sept. 22, 1998). See also [USA Today article](#); [ZDNet.com article](#); and [N.Y. Times on the Web article](#).

- ▶ Kellstrom Industries v. Yahoo! Inc. (*Miami, Fla., Bill of Discovery against Yahoo! filed March 23, 2000*).

See New Filings: 'Reverse Pump and Dump' Suit Filed Against Individuals, Hedge Fund, Premier Issue (2000), e-Trading Legal Alert, at 4 (Andrews Publications); Companies Fight 'Cybersmear' But Will They Lose the Battle?, Premier Issue (2000), e-Trading Legal Alert, at 4 (Andrews Publications). Also referenced in Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart).

- ▶ Legacy Software v. Dean Dumont, et al. (*D.N.H., complaint filed 1998*).

See [Wired News article](#).

- ▶ Lilly Industries Inc. and Lawrence Dalton v. John Does 1-5 (*complaint filed in Marion County Court, Indiana, week of July 19, 1999*).

[Lilly Files Message Board Defamation Suit](#), CNET News.com (Jul. 28, 1999). See also [Techserver article](#)

- ▶ Liviakis Financial Communications v. John Does 1-100 (*complaint filed April 12, 1999 in Marin Superior Court, California*).

See Jon Swartz, Corporations Fight Internet 'Cybersmear', SF Gate (San Francisco Chronicle on the Web), April 13, 1999 <<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/04/13/BU93359.DTL>>.

- ▶ Log On America Settlement Agreement.

See [SiliconInvestor.com Message Board LOAX](#)

- ▶ Medphone Corp. v. DeNegriss
Civ. Action No. 069400012 or 92-3785 (D.N.J. 1992)

(Prodigy subscriber made posting to bulletin board alleging company "appears to be a fraud").

▶ Medinah Energy, Inc., a Nevada corporation, and Larry Regis v. Staggerlee, a trade name for DOE 1 and/or Black Corporation 1; DOES 2-5, Black Corporations 2-5, Case No. CV98-06518 Dept. No. 4 (2nd Judicial Dist. Ct. of Nevada in and for County of Washoe, [complaint](#) filed October 19, 1998)

▶ M.H. Meyerson v. John Does
(Complaint filed March 1999 in New Jersey state court in Hackensack)

See [CNET News.com article](#) and second [CNET News.com article](#)

▶ Michael Moore v. Steptoe & Johnson
(D.D.C., complaint filed November 1999)

See Craig Bicknell, Strange Corporate Hacking Saga, Wired News, Nov. 12, 1999 ([Part 1](#)) ([Part 2](#))
See also
Computer Hacking Suit Escalates Against Top U.S. Law Firm, PRNewswire.com, Nov. 11, 1999.

▶ Nanopierce Technologies Inc. v. Louis DiFrancesco
(D. Col., complaint filed Oct. 1998).

See [Denver Post article](#).

▶ Ocwen Financial Corp.

Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), St. Petersburg Times Online (May 28, 2000) (referenced in chart).

▶ Owens Corning v. John Doe
(S.D.N.Y., complaint filed Oct. 28, 1999)

See Benjamin Weiser, [Lawsuit Over Web Posting](#), N.Y. Times on the Web (Oct. 28, 1999) (copy also pasted to Silicon Investor Investment Chat Board Lawsuits Message Board, [Message #254](#) (May 15, 2000).

▶ Dimitri Papadakos v. Gyrodyne Co. of America
(Sup. Ct. of State of N.Y. for County of N.Y., amended complaint filed on January 12, 2000)

See Alan J. Wax, Kin Named in Gyrodyne Suit, N.Y. Newsday, Jan. 13, 2000, Bus. Sec. Q. See also Carrie Lee, CEO Says Officials Planted Web Posts that Got Him Fired, Wall St. J. Interactive Ed., Jan. 27, 2000
<<http://interactive.wsj.com/articles/SB948911151691620714.htm>>.

▶ Pacificorp v. John Does.

See [The Standard](#) article. See also Steve Woodward, Three Corporations Go to Court to Fight Internet Falsehoods, Seattle Times, Nov. 1, 1998, at B5.

▶ Philip Services Corp. V. Does 1-100
(Super. Ct. Calif. for County of Santa Clara, filed June 4, 1998).

▶ Phoenix International Ltd. v. John Does 1-7
(Complaint filed in circuit court at the Seminole County [Florida] Courthouse on March 19, 1999)

See

http://www.zdii.com/industry_list.asp?mode=news&doc_id=ZE304668&pic=Y (noting that "Software developer Phoenix International Ltd. (Nasdaq: PHXX) filed a suit last month against seven unidentified people who wrote critical comments about the company on an Internet message board . . ."). See also Software Maker Sues Online Critics, Mercury Center Breaking News, Apr. 7, 1999 (available via search at <http://www.sjmercury.com>).

- ▶ Phoenix International Ltd., Inc. v. William Toole
(*M.D. Fla., Orlando Division, complaint filed on July 14, 1999, agreement to settle filed on Oct. 26, 1999*).

See Company Press Release: Phoenix International Ltd., Inc. Announces Settlement of Litigation With Former Employee, [Yahoo! Finance, Oct. 26, 1999](#); Emily Kaiser, Lilly Sues Anonymous Internet Critics, NandoTimes, July 28, 1999 (stating "Banking software maker Phoenix International Ltd. Inc. said this month that it filed a civil complaint in Florida against a former employee the company thinks is responsible for negative message board postings").

- ▶ Phycor v. John Does

Referenced in Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart); see also ['John Does' Fight To Keep Anonymity](#), *St. Petersburg Times special to JSONline* (Milwaukee Journal Sentinel online) (Jun. 5, 2000); Bob Cook, Down and Dirty: Phycor and Other Companies Sue Anonymous Message Posters for Internet Mudslinging, *Mod. Physician*, June 1, 1999, at 30.

- ▶ Presstek Inc. v. Lustig
(D.N.H., complaint filed Sept. 17, 1997).

- ▶ ProMedCo Management Co. v. John Does 1 - 50
Civ. Action No. 806956 (Cal. Super. Court, Santa Clara County (March 1999)).

Noted in Mark Thompson, [On the Net, In the Dark: Companies Want To Know Who's Criticizing Them Online -- Some Critics Say That's None of Their Business](#), *Law News Network*, Nov. 8, 1999).

- ▶ Quest Net Corp. v. John Does
Dade County [Florida] Circuit Court, complaint filed Feb. 17, 2000).

Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart).

- ▶ Raytheon Corp. v. John Does 1 through 21
Civ. Action No. 99-816 (Commonwealth of Massachusetts Superior Court, Middlesex County, complaint filed February 1, 1999)

[Raytheon Sues 21 People Over Sharing of Company Secrets Online](#), *FreedomForum.org* (last modified Mar. 5, 1999); David L. Sobel, [The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity](#), *VJOLT.net* (visited Jul. 25, 2000); [Raytheon Drops Suit Over Internet Chat](#), *Associated Press special to N.Y. Times on the Web* (May 22, 2000).

- ▶ Remtrak Corporation v. Kunderling, et al.
CV00-820-HA (N.D. Cal.)

See [To My Surprise](#), Yahoo! Finance RENT Message 2929 (Jul. 6, 2000)

- ▶ Sabratek Corp. v. Keyser
99 Civ. 8589 (HB), order (S.D.N.Y., order entered April 19, 2000).

See Federal News - Antifraud: Newsletter Publisher Wins Dismissal of Securities Fraud, Defamation Claims, 32(18) Sec. Reg. & Law Rep. (BNA) 601 (May 8, 2000).

- ▶ SATX v. John Does

Referenced in Robert Trigaux, [The Fight To Speak Their Mind, Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart).

- ▶ Shaman Pharmaceuticals, Inc. v. John Does
(filing of complaint announced on July 14, 2000).

Shaman Pharmaceuticals, Inc., [Shaman Files Complaint Against 'Cyber-Bashers'](#), Company Press Release issued via Business Wire Health Wire (Jul. 14, 2000) (copy pasted on SiliconInvestor Investment Chat Board Lawsuits, [Message #446](#) (Jul. 14, 2000)).

- ▶ Shoney's Inc. v. John Does 1 - 3
(complaint filed in Davidson County [Tennessee] Chancery Court on April 9, 1999).

See [ZDNet article](#); [CNET News.com](#) article.

- ▶ Southern Pacific Funding Corp. v. John Does (noted in Star Telecommunications, Inc. v. DOES 1 Through 75
(Super. Court of Cal. for County of Santa Barbara).

See Rhonda Parks Manville, [Company, CEO Targeted on Internet - Star Telecom Sues Detractors](#), News-Press (Jul. 12, 1999).

- ▶ Sovereign Partners Limited Partnership, Dominion Capital Fund Ltd. and Stephen M. Hicks v. Restaurant Teams International, Inc., ConSyGen, Inc., Stanley Swanson, Curtis Swanson and Thomas Dreaper
(S.D.N.Y., proposed amended complaint filed on Oct. 5, 1999).

[Business Wire - Company Press Release: Investors Amend Defamation Complaint Filed Against ConSyGen and Restaurant Teams - Mark Weiss, Tom Dreaper, Harry McMillan, Lee Walsh and Other Internet Posters Named as Additional Parties in Amended Complaint](#), Business Wire (Oct. 4, 1999);
Business Wire - Company Press Release: Investors Amend Defamation Complaint Filed Against ConSyGen and Restaurants - Mark Weiss, Tom Dreaper, Harry McMillan, Lee Walsh and Other Internet Posters Named as Additional Parties in Amended Complaint, Bus. Wire, Oct. 5, 1999 (10:23 a.m. Eastern Time) (copy pasted on [SiliconInvestor.com Message Board](#)); [Business Wire - Company Press Release: Restaurant Teams International, Inc. and Debenture Holders Reach Settlement](#), Business Wire (Dec. 28, 1999) (announcing that Restaurant Teams International reached agreement with Sovereign Partners, Dominion Capital and Steven Hicks, among others).

- ▶ Stampede Worldwide, Inc. v. Charles R. Will, Jr.
(Circuit Court for Pinellas County, Florida, complaint filed May 15, 2000).

[Stampede Worldwide, Inc., Files Defamation Lawsuit Against Charles R. Will.](#)

[Jr.](#), Business Wire special to Yahoo! Finance (May 15, 2000) (pasted copy also available via [SiliconInvestor.com Message Board](#)); Robert Trigaux, [The Fight To Speak Their Mind. Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in text of article and in chart).

- ▶ Starnet Communications International, Softec Systems Caribbean Inc. and John Carley v. Las Vegas Casino, Inc., Claude Levy, and Gambling Magazine (*Vancouver Registry of Supreme Court of British Columbia [Canada], Writ of Summons and Statement of Claim filed on Aug. 3, 1999*).

Starnet Files Defamation Law Suit Against Las Vegas Casino Inc. Claiming Damages for False and Malicious Statements on the Internet, Business Wire (Aug. 5, 1999) (pasted copy available via [SiliconInvestor.com Message Board](#)).

- ▶ Stone & Webster v. [20 Individuals It Claims Made False Statements or Revealed Inside Information About the Company on the Internet] (*complaint filed in Suffolk County [Massachusetts] Court on Aug. 20, 1999*).

See Stone & Webster Files Suit Against Online Chatters, Newsbytes.com (Aug. 1999) (copy pasted at [SiliconInvestor.com Message Board](#) (Aug. 25, 1999)).

- ▶ Sunbeam Corp. v. John Does

Referenced in Robert Trigaux, [The Fight To Speak Their Mind. Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart).

- ▶ Robert Talbot and Medical Resorts International v. StockHouse Media Corporation, StockHouse.com, John Doe 1 a/k/a Peter41 and John Doe 2 a/k/a Waitnsee (*Court of Queen's Bench of Alberta in Edmonton [Canada], statement of claim filed prior to March 9, 2000*).

See [StockHouse and Anonymous Posters Face \\$6 Million Suit](#), Stockwatch Business Reporter (Mar. 29, 2000)

- ▶ Talk Visual Corp. v. John Does (*Third Judicial Court of Salt Lake County, Utah, complaint filed February 14, 2000; Notice of Dismissal filed on May 24, 2000*).

According to a report posted on the boards of JohnDoes.org, on May 24 a notice of dismissal with prejudice was filed with the Third Judicial Court of Salt Lake County, Utah in the cybersmear suit filed on February 14, 2000 by Talk Visual Corporation against pseudonymous posters who used the aliases "the worm" and "investordeal," among others, to post comments critical of the company. See Posting by "LesLFrench Forum Host" Posted 05-25-2000 20:05. See also Robert Trigaux, [The Fight To Speak Their Mind. Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart).

- ▶ Technical Chem & Prods., Inc. v. John Does 1-10 Case No. 99004548 (*Fla. Cir. Ct. 17th 1999*) (*complaint alleges defendants posted anonymous messages to Yahoo! message board accusing company and certain of its officers of fraud*).

Referenced in Robert Trigaux, [The Fight To Speak Their Mind. Anonymously](#), *St. Petersburg Times Online* (May 28, 2000) (referenced in chart).

▶ Thomas & Betts Corporation, a Tennessee Corporation, Plaintiff, v. Does 1 through 50, Defendants
 Case No.: GIC 748128 (Superior Court of the State of California for the County of San Diego, complaint filed May 12, 2000) (Hon. William C. Pate, Dept. 60).

▶ Thomas & Betts Corporation, a Tennessee Corporation, Plaintiff, v. Does 1 through 50, Defendants
 Case No.: GIC 748128, [Memorandum of Points and Authorities in Support of Special Motion To Strike \(Code Civ. Proc. Section 425.16\)](#) (Superior Court of the State of California for the County of San Diego, complaint filed May 12, 2000) (Hon. William C. Pate, Dept. 60).

▶ Thomson Kernaghan & Co. Ltd. v. Yahoo! Inc., Silicon Investor Inc., John Does, et al. (Ontario Court [Canada] General Division).

See <http://www.nationalpost.com/story.asp?f=990112/2173914>. See Katherine Macklem, Slammed in Chat Rooms, Brokerage Files Lawsuit, Financial Post (pasted copy of story at SiliconInvestor.com Investment Chat Board Lawsuits [Message 11](#) (May 25, 1999)).

▶ Titan Investments v. John Doe
 4-00-CV-10303 (S.D. Iowa).

See [It Seems That Titan Corporate Is Scared](#), Yahoo! Finance TWI Message 525 (June 22, 2000)

▶ Total Renal Care Holdings Inc. and M.G. Chaltiel v. John Does.

Noted in Total Renal Sues Internet Users, Alleges Misleading Postings, Bloomberg.com, Aug. 24, 1999.

▶ Universal Foods Corp. v. John Does.

See [The Standard](#) article.

▶ Universal Foods Corp. v. Yahoo! Inc. and Jane Doe
 (complaint filed in Circuit Court in Wisconsin on July 27, 1998, but was removed to D. Wis. subsequently).

See <http://www.jsonline.com/business/news/980728universalfoodsalleges.stm>.

▶ Varian Medical Systems, Inc., Varian Semiconductor Equipment Associates, Inc., Susan B. Felch, and George Zdasiuk v. Michelangelo Delfino, Mary E. Day, and Does 2-20, Inclusive
 Case No. C-99 20256 RMW ENE (N.D. Cal., complaint filed under seal Feb. 25, 1999).

See [Plaintiff's Memorandum of Points and Authorities in Support of Motion for Leave To File Third Amended and Supplemental Complaint \(Code of Civ. Proc. Sections 464 & 473\)](#) (Jul. 10, 2000); [Plaintiffs' \[Proposed\] Third Amended and Supplemental Complaint for Damages and Injunctive Relief](#) (Jul. 10, 2000); [Brief for Appellant, Mary Day on Appeal From a Modified Preliminary Injunction of the United States District Court for the Northern District of California](#) (June 28, 2000); [chronology of the case](#), with links to excerpts of pertinent papers.

▶ Wade Cook Financial Corp. v. John Does 1-10

Noted in Washington State Senate First in the Nation To Seek to Remedy

Anonymous Internet Slander, PR Newswire, April 16, 1999, at 1).

▶ Xircom Inc. v. John Doe

Case No. CIV 188724 (Complaint filed in Ventura County [California] Superior Court, May 1999).

Rebecca Fairley Raney, [Judge Rejects Online Critic's Efforts To Remain Anonymous](#), N.Y. Times on the Web (Jun. 15, 1999); Carl S. Kaplan, [Company Settles Suit Against Online Critic](#), N.Y. Times on the Web (Jul. 16, 1999); Michael D. Goldhaber, [Associate Is a Leading 'Cybersmear' Lawyer](#), NYLJ.com Backpage (Jul. 14, 2000).

▶ ZiaSun Technologies, Inc. v. Steve Worthington, Floyd Scheider, Mike Morelock and John Does

Noted in Aaron Elstein, Heard on the Net: ZiaSun Sues Its Online Critics As Posts Get Nasty and Personal, Wall St. J. Interactive Ed., Aug. 13, 1999 (available via search at <http://interactive.wsj.com/> - paid subscription required); ZiaSun Technologies, Inc. Company Press Release: ZiaSun Files Second Defamation Lawsuit (July 2, 1999) .

▶ ZiaSun Technologies, Inc., a Nevada corporation, and Anthony L. Tobin, Plaintiffs, v. Floyd D. Schneider a.k.a. "Floydie," et al., No. C99-1025P, Order Granting Preliminary Injunction (W.D. Wash., order filed Jan. 21, 2000).

See Aaron Elstein & Jason Anders, [Net Firm Wins First Round In Battle With Online Critic](#), Wall St. J. Interactive Ed., Jan. 25, 2000
<<http://interactive.wsj.com/articles/SB948827406701233070.htm>>.

▶ Zixit Corp. v. Visa USA Inc.

(State Court in Dallas, Texas, complaint filed on Dec. 31, 1999).

See Alan Goldstein, [Zixit Sues Visa for Alleged Web Remarks](#), Dallas Morning News, Jan. 3, 2000

▶ Michael J. Zwebner v. Dean Dumont, Gary Dobry (a/k/a "Pugs" and "Spider Valdez"), David Shepard (a/k/a "Rico Staris"), et al., Civ. Action No. 98-CV-682-M (D.N.H., complaint filed Dec. 10, 1998).

Talk Visual Corporation, [Talk Visual Chairman Michael J. Zwebner Obtains a Second Lawsuit Award of \\$1 Million Against Internet Poster](#), Company Press Release issued via Business Wire special to Yahoo! Finance (Jul. 25, 2000) (copy available via SiliconInvestor.com Investment Chat Board Lawsuits [Reply #490](#) (Jul. 25, 2000)); Talk-Visual Corporation, [Talk Visual Chairman Wins \\$1 Million Judgment Against Libelous Internet Poster](#), Company Press Release issued via Business Wire (Jul. 13, 2000); Talk-Visual Corporation, [Talk Visual Chairman Wins \\$1 Million Judgment Against Libelous Internet Poster](#), Company Press Release issued via Business Wire special to Yahoo! Finance (Jul. 13, 2000); Aaron Elstein, [In This Cybersmear Settlement, Loose Lips May Cost \\$1 Million](#), Wall St. J. Interactive Ed. (Jul. 21, 2000) (paid subscription required). See also [Techstocks.com Story](#); John R. Emshwiller, [Defamation Suit Sent Ex-Boxer Reeling From Stock-Chat Ring](#), Wall St. J. Interactive Ed. (Jul. 24, 2000) (paid subscription required); Apology Posted to RagingBull Message Board signed "Gary Dobry", RagingBull.Altavista.com TVCP Message Board [Post #63533](#) (Jul. 18, 2000); Apology Posted to RagingBull Message Board signed "Gary Dobry", RagingBull.Altavista.com DCTC

Message Board [Post #4968](#) (Jul. 18, 2000); [7/18/00 - Gary Dobry's Stipulated Apology to TVCP](#), SiliconInvestor.com Investment Chat Board Lawsuits Message Board Reply #467 (Jul. 19, 2000).

▶ Michael J. Zwebner v. Roberto Villasenor
(*Superior Court of Mass., complaint filed May 22, 2000*).

See Chairman Files and Serves Defamation Lawsuit on Internet Stock Bashers, Business Wire (May 24, 2000).

Note: Three separate cyberlibel lawsuits reportedly have been filed in Florida courts by Sunbeam Corp., Technical Chemicals & Products, and Ocwen Financial. See <http://www.bergen.com/biz/online04199810041.htm>.

[Credits and Disclaimers](#)

Copyright © 2000 by Glasser LegalWorks. All rights reserved.

No part of this Web site may be reproduced without the prior written permission of Glasser LegalWorks.

EXHIBIT B

*2001 N.J. Super. LEXIS 300, **

DENDRITE INTERNATIONAL, INC., a New Jersey Corporation, Plaintiff-Appellant, v. JOHN DOE NO. 3, Defendant-Respondent, and JOHN DOES NOS. 1, 2 and 4, and JOHN DOES 5 through 14, inclusive, Defendants.

A-2774-00T3

SUPERIOR COURT OF NEW JERSEY, APPELLATE DIVISION

2001 N.J. Super. LEXIS 300

May 22, 2001, Argued
July 11, 2001, Decided

SUBSEQUENT HISTORY: [* 1] Approved for Publication July 11, 2001.

PRIOR HISTORY: On appeal from Superior Court of New Jersey, Chancery Division, Morris County, Docket No. MRS-C-129-00.

DISPOSITION: Accordingly, we affirm.

CASE SUMMARY

PROCEDURAL POSTURE: Plaintiff corporation filed a motion for leave to appeal the interlocutory order of the Superior Court of New Jersey, Chancery Division, Morris County, which denied its request to conduct limited discovery for the purpose of ascertaining the identity of a fictitiously-named defendant from an Internet service provider in an action alleging, inter alia, defamation, on an Internet bulletin board. The appellate court granted leave to appeal.

OVERVIEW: The corporation filed a complaint contending that the action of a number of fictitiously-named defendants, posting messages on an Internet bulletin board, constituted actionable defamation. The trial court denied the corporation's application for expedited discovery disclosing the identity of a particular defendant. On appeal, the appellate court determined that the record did not support the conclusion that defendant's postings negatively affected the value of the corporation's stock, or did the corporation offer evidence or information that the postings had actually inhibited its hiring practices. Accordingly, the appellate court found the trial court appropriately concluded that the corporation failed to establish a sufficient nexus between defendant's statements and the corporation's allegations of harm. Therefore, the appellate court was satisfied that the analysis and conclusions by the trial court were supported by the record, and observed that the corporation failed to establish that the trial court abused its discretion in entering the order.

OUTCOME: The appellate court affirmed the interlocutory order.

CORE TERMS: discovery, internet, message, posting, defamation, com, anonymous, motion to dismiss, posted, seescandy, bulletin board, user, First Amendment, disclosure, anonymously, disclose, prong, cause of action, actionable, stock, unknown, stock prices, free speech, fictitiously-named, reputation, subscriber, ascertain, subpoena, entity, harmed

CORE CONCEPTS - ♦ [Hide Concepts](#)

 [Civil Procedure : Discovery Methods : Motions to Compel](#)

⬇ When faced with an application by a plaintiff for expedited discovery seeking an order compelling an Internet service provider to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals, corporations, or businesses, the trial court must consider and decide those applications by striking a balance between the well-established U.S. Const. amend. I right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendants.


 [Civil Procedure : Discovery Methods : Motions to Compel](#)

⬇ When faced with an application by a plaintiff for expedited discovery seeking an order compelling an Internet service provider (ISP) to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals, corporations, or businesses, the trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notification efforts should include posting a message of notification of the identity discovery request to the anonymous user on the ISP's pertinent message board. The application of these procedures and standards must be undertaken and analyzed on a case-by-case basis. The guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue.


 [Civil Procedure : Discovery Methods : Motions to Compel](#)

⬇ When faced with an application by a plaintiff for expedited discovery seeking an order compelling an Internet service provider to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals, corporations, or businesses, the court shall require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech. The complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants. The application of these procedures and standards must be undertaken and analyzed on a case-by-case basis. The guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue.


 [Civil Procedure : Discovery Methods : Motions to Compel](#)

 When faced with an application by a plaintiff for expedited discovery seeking an order compelling an Internet service provider to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals, corporations, or businesses, in addition to establishing that its action can withstand a motion to dismiss for failure to state a claim upon which relief can be granted pursuant to N.J. Ct. R. 4:6-2(f), the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant. The application of these procedures and standards must be undertaken and analyzed on a case-by-case basis. The guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue.

 [Civil Procedure : Discovery Methods : Motions to Compel](#)

 When faced with an application by a plaintiff for expedited discovery seeking an order compelling an Internet service provider to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals, corporations, or businesses, assuming the court concludes that the plaintiff has presented a prima facie cause of action, the court must balance the defendant's U.S. Const. amend. I right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed. The application of these procedures and standards must be undertaken and analyzed on a case-by-case basis. The guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue.

 [Constitutional Law : Fundamental Freedoms : Freedom of Speech : Scope of Freedom](#)

 It is well-established that rights afforded by the U.S. Const. amend. I remain protected even when engaged in anonymously.

 [Constitutional Law : Fundamental Freedoms : Freedom of Speech : Scope of Freedom](#)

 U.S. Const. amend. I protections extend to speech on the Internet.

 [Constitutional Law : Fundamental Freedoms : Freedom of Speech](#)

 [Constitutional Law : State Constitutional Operation & Amendment](#)

 New Jersey's State Constitution affords even greater protection to persons' rights to free speech than does the United States Constitution.


 [Constitutional Law : Fundamental Freedoms : Freedom of Speech : Freedom of the Press](#)

 [Constitutional Law : Fundamental Freedoms : Freedom of Speech : Scope of Freedom](#)

 See N.J. Const. art. 1, par. 6.


 [Constitutional Law : State Constitutional Operation & Amendment](#)

 [Constitutional Law : Fundamental Freedoms : Freedom of Speech : Scope of Freedom](#)


 The New Jersey State right of free speech is protected not only from abridgment by government, but also from unreasonably restrictive and oppressive conduct by private entities.

 [Torts : Defamation & Invasion of Privacy : Defamation Actions](#)


 [Constitutional Law : Fundamental Freedoms : Freedom of Speech : Scope of Freedom](#)

 The key principle in defamation/free expression cases is the profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open. The law of defamation exists to achieve the proper balance between protecting reputation and protecting free speech. Thus, the purpose of the law of defamation is to strike the right balance between protecting reputation and preserving free speech.


 [Civil Procedure : Pleading & Practice : Service of Process](#)


 In such cases where a tortfeasor acting pseudonymously, anonymously, or giving fictitious or incomplete identifying information, commits certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely on-line, the traditional reluctance for permitting filings against John Doe defendants or fictitious names and the traditional enforcement of strict compliance with service requirements should be tempered by the need to provide injured parties with a forum in which they may seek redress for grievances. However, this need must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously.

 [Civil Procedure : Disclosure & Discovery : Mandatory Disclosure](#)

 In determining whether discovery to uncover the identity of a defendant is warranted: first, plaintiff should identify the missing party with sufficient specificity such that the court can determine that defendant is a real person or entity who could be sued in federal court. Second, plaintiff must identify all previous steps taken to locate the elusive defendant to demonstrate that plaintiffs have made a good-faith effort to comply with the requirements of service of process. Third, plaintiff should establish to the court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss. Fourth, plaintiff should file a request for discovery with the court, with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood the discovery process will lead to identifying information about defendant that would make service of process possible.

 [Civil Procedure : Pleading & Practice : Pleadings](#)

 [Civil Procedure : Pleading & Practice : Defenses, Objections & Demurrers : Failure to State a Cause of Action](#)

 The test for determining the adequacy of a pleading is whether a cause of action is "suggested" by the facts.

 [Civil Procedure : Pleading & Practice : Defenses, Objections & Demurrers :](#)

Failure to State a Cause of Action

Civil Procedure : Appeals : Standards of Review : General Rules

↓ In reviewing a complaint dismissed under N.J. Ct. R. 4:6-2(e) an appellate court's inquiry is limited to examining the legal sufficiency of the facts alleged on the face of the complaint. However, the appellate court searches the complaint in depth and with liberality to ascertain whether the fundament of a cause of action may be gleaned even from an obscure statement of claim, opportunity being given to amend if necessary. At this preliminary stage of the litigation the court is not concerned with the ability of plaintiffs to prove the allegation contained in the complaint. For purposes of analysis plaintiffs are entitled to every reasonable inference of fact. The examination of a complaint's allegations of fact required by the aforesaid principles should be one that is at once painstaking and undertaken with a generous and hospitable approach.

Torts : Defamation & Invasion of Privacy : Defamation Actions

↓ In the case of a complaint charging defamation, plaintiff must plead facts sufficient to identify the defamatory words, their utterer and the fact of their publication.

Civil Procedure : Discovery Methods : Motions to Compel

↓ Pre-service discovery is akin to the process used during criminal investigations to obtain warrants. The requirement that the government show probable cause is, in part, a protection against the misuse of ex parte procedures to invade the privacy of one who has done no wrong. A similar requirement is necessary to prevent abuse of this extraordinary application of the discovery process and to ensure that plaintiff has standing to pursue an action against defendant. Probable cause as it relates to obtaining warrants is a non-technical, flexible concept that does not require rigid, technical demands for specificity and precision. By equating this prong to the probable cause requirement for warrants, plaintiff must make some showing that an act giving rise to civil liability actually occurred and that the discovery is aimed at revealing specific identifying features of the person or entity who committed the act.


Civil Procedure : Discovery Methods : Motions to Compel

↓ The four-part Seescandy.Com test was envisioned to act as a flexible, non-technical, fact-sensitive mechanism for courts to use as a means of ensuring that plaintiffs do not use discovery procedures to ascertain the identities of unknown defendants in order to harass, intimidate, or silence critics in the public forum opportunities presented by the Internet.


Civil Procedure : Discovery Methods : Motions to Compel

↓ A court should only order a non-party, Internet service provider to provide information concerning the identity of a subscriber (1) when the court is satisfied by the pleadings or evidence supplied to that court (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and (3) the subpoenaed identity information is centrally needed to advance that claim.

 [Civil Procedure : Discovery Methods : Motions to Compel](#)

 When evaluating a plaintiff's request to compel an Internet service provider to disclose the identity of a John Doe subscriber, courts may depart from traditionally-applied legal standards in analyzing the appropriateness of such disclosure in light of the U.S. Const. amend. I implications.


 [Torts : Defamation & Invasion of Privacy : Defamation Actions](#)

 A defamatory statement is one that is false and (1) injures another person's reputation; (2) subjects the person to hatred, contempt or ridicule; or (3) causes others to lose good will or confidence in that person. A defamatory statement harms the reputation of another in a way that lowers the estimation of the community about that person or deters third persons from associating or dealing with him.

 [Torts : Defamation & Invasion of Privacy : Defamation Actions](#)

 Words that clearly denigrate a person's reputation are defamatory on their face and actionable per se.

 [Torts : Defamation & Invasion of Privacy : Defamation Actions](#)

 When determining if a statement is defamatory on its face a court must scrutinize the language according to the fair and natural meaning which will be given it by reasonable persons of ordinary intelligence. A plaintiff does not make a prima facie claim of defamation if the contested statement is essentially true.

COUNSEL: Michael S. Vogel argued the cause for appellant (Allegaert Berger & Vogel and Robert L. Weigel (Gibson, Dunn & Crutcher) of the New York bar, admitted pro hac vice, attorneys; Mr. Vogel, Mr. Weigel, Lee G. Dunst and David A. Zonana, on the brief).

Eugene G. Reynolds argued the cause for respondent (Wacks, Mullen & Kartzman, attorneys; Mr. Reynolds, of counsel and on the brief).

Paul Alan Levy argued the cause for Amici Curiae, Public Citizen Litigation Group (Mr. Levy, on the joint brief) and American Civil Liberties Union of New Jersey Foundation (J.C. Salyer, on the joint brief).

JUDGES: Before Judges Stern, A. A. Rodriguez and Fall. The opinion of the court was delivered by FALL, J.A.D.

OPINIONBY: FALL

OPINION: The opinion of the court was delivered by

FALL, J.A.D.

In this opinion, we examine the appropriate procedures to be followed and the standards to be applied by courts in evaluating applications for discovery of the identity of anonymous users of Internet Service Provider (ISP) message

boards.

Information [*2] contained in postings by anonymous users of ISP message boards can form the basis of litigation instituted by an individual, corporation or business entity under an array of causes of action, including breach of employment or confidentiality agreements; breach of a fiduciary duty; misappropriation of trade secrets; interference with a prospective business advantage; defamation; and other causes of action.

Plaintiff, **Dendrite International, Inc. (Dendrite)**, on leave granted, appeals from an interlocutory order of the trial court denying its request to conduct limited expedited discovery for the purpose of ascertaining the identity of defendant, John Doe No. 3, from Yahoo!, an ISP. Here, the posting of certain comments about **Dendrite** on a Yahoo! bulletin board by defendant, John Doe No. 3, forms the basis of the dispute in this appeal in the context of a cause of action based on **Dendrite's** claims of defamation. n1 We affirm the denial of **Dendrite's** motion based on the conclusion of the motion judge that **Dendrite** failed to establish harm resulting from John Doe No. 3's statements as an element of its defamation claim.

-----Footnotes-----

n1 The complaint filed by **Dendrite** against a number of fictitiously-named defendants, including John Doe No. 3, alleged various claims for breach of contract, defamation and other actionable statements on the Yahoo! bulletin board. Although the trial court issued decisions on **Dendrite's** request for information concerning the identity of all fictitiously-named defendants, this appeal focuses solely on the court's denial of **Dendrite's** application for expedited discovery disclosing the identity of John Doe No. 3.

-----End Footnotes----- [*3]

We offer the following guidelines to trial courts when faced with an application by a plaintiff for expedited discovery seeking an order compelling an ISP to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals, corporations or businesses. The trial court must consider and decide those applications by striking a balance between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendants.

We hold that when such an application is made, the trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notification efforts should include posting a message of notification of the identity discovery request to the anonymous user on the [*4] ISP's pertinent message board.

The court shall also require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech.

The complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants. In addition to establishing that its action can withstand a motion to dismiss for failure to state a claim upon which relief can be granted pursuant to R. 4:6-2(f), the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant.

Finally, assuming the court concludes that the plaintiff has presented a prima facie cause of action, the court must balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed.

The application of these procedures [*5] and standards must be undertaken and analyzed on a case-by-case basis. The guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue.

With these principles in mind, we now turn to an analysis of **Dendrite's** action against John Doe No. 3 and the trial court's decision.

Dendrite is a New Jersey corporation based in Morristown that provides "highly specialized integrated product and service offerings for the Pharmaceutical and Consumer Package Goods (CPG) industries." **Dendrite** is publicly traded and has offices located in 21 countries.

"The Internet is an international network of interconnected computers[,]" providing "a unique and wholly new medium of world-wide human communication." [Reno v. American Civil Liberties Union, 521 U.S. 844, 849-50, 117 S. Ct. 2329, 2334, 138 L. Ed. 2d 874, 884 \(1997\).](#) In further describing the Internet and the services available, the Supreme Court noted, in part:

Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation. . . . Several major national "online services" . . . offer access to their [*6] own extensive proprietary networks as well as a link to the much larger resources of the Internet. . . .

Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. . . .

. . . .

The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. . . .

. . . .

The Web is thus comparable, from the reader's viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and [*7] individuals. Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web."

[[Id. 521 U.S. at 850-53, 117 S. Ct. at 2334- 36, 138 L. Ed. 2d at 884-86.](#) (citations and footnotes omitted).]

Yahoo! is an ISP that, among other things, provides a service where users may post comments on bulletin and message boards related to the financial matters of particular companies. Yahoo! maintains a message board for every publicly-traded company and permits anyone to post messages on it. As such, Yahoo! operates a bulletin board specifically devoted to **Dendrite**, hosting exchanges of messages and comments about issues related to the company's stock performance. Generally, users of the bulletin boards post messages anonymously under pseudonyms. Yahoo! requires, however, that users provide identifying information, including real names, mailing addresses, and e-mail addresses prior to using the [*8] service. Nonetheless, Yahoo! guarantees to a certain extent that information about the identity of their individual subscribers will be kept confidential. Yahoo!'s privacy policy states that:

As a general rule, Yahoo! will not disclose any of your personally identifiable information except when we have your permission or under special circumstances, such as when we believe in good faith that the law requires it or under the circumstances described below.

. . . .

Yahoo! may also disclose account information in special cases when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against someone who may be violating Yahoo!'s Terms of Service or may be causing injury to . . . anyone . . . that could be harmed by such activities.

The postings by John Doe No. 3 on the Yahoo! **Dendrite** message board must be viewed in the following context. **Dendrite** filed its Quarterly Report for the second quarter of 1999 with the Securities and Exchange Commission (SEC) in August of 1999. In this report, **Dendrite** stated:

Historically, we have generally recognized license fees as revenue using the percentage of completion method [*9] over a period of time that begins with execution of the license agreement and ends with the completion of initial

customization and installation, if any. However, we believe that with some of our newer sales force software products, such as, ForcePharma and SalesPlus, our customers will not require customization and therefore we may be able to recognize license fees from these products upon delivery.

Following the release of this report, several stock analysts commented on the disclosures therein. The Center for Financial Research and Analysis, Inc. (CFRA) issued a report in September 1999 specifically addressing what it characterized as **Dendrite's** "Change in Revenue Recognition." The CFRA report concluded that due to the apparent change indicated in its Quarterly Report, **Dendrite's** revenue recognition would provide an earnings boost and was actually one of the reasons for **Dendrite's** then-improved financial condition. Further, the CFRA report opined that the associated earnings boost may have "masked weaknesses in the company's core segment."

An Internet website, "TheStreet.com," published a similar article concerning **Dendrite** in September 1999, also responding to **Dendrite's** Quarterly [* 10] Report. There, TheStreet.com noted several "red flags" about **Dendrite**, including its "more aggressive recognition of revenue." The author of the article stated that this change in **Dendrite's** revenue recognition policy "could mean more revenue up front."

Thereafter, at least two users of the Yahoo! **Dendrite** bulletin board mentioned the CFRA report and the article from TheStreet.com in respective postings. On September 21, 1999 one poster, citing the CFRA report, commented on **Dendrite's** purported accounting and operational problems. On September 22, 1999 another poster, citing TheStreet.com article, noted changes in **Dendrite's** policy of recognizing revenue. Sometime after the CFRA report was released **Dendrite** responded, denying it changed its revenue recognition policy as asserted in the CFRA report.

During the period from March 14, 2000 through June 2, 2000 John Doe No. 3, posted nine comments on the Yahoo! **Dendrite** bulletin board under the pseudonym "xxplrr." Three of these comments related to purported changes in **Dendrite's** revenue recognition accounting. Specifically, these comments included the following:

John's [(**Dendrite** president John Bailye)] got his contracts salted [* 11] away to buy another year of earnings - and note how they're changing revenue recognition accounting to help it.

. . . .

Bailye has his established contracts structured to provide a nice escalation in revenue. And then he's been changing his revenue-recognition accounting to further boost his earnings (see about 100 posts back).

. . . .

[**Dendrite**] signed multi-year deals with built in escalation in their revenue year-over-year (pharma cares most about total price of the contract, so they don't care; nor do they care if the price is in software or services). They also have been able to restructure their contracts with Pfizer and Lilly the same

way.

The certification of **Dendrite** Vice President, R. Bruce Savage, submitted in support of **Dendrite's** discovery application, asserts that the substance of these statements are categorically false, specifically averring that **Dendrite** did not change its revenue recognition policy, nor are **Dendrite's** contracts structured to defer income.

Dendrite also takes issue with the following March 28, 2000 posting by John Doe No. 3:

[**Dendrite**] simply does not appear to be competitively moving forward. John [Bailey, **Dendrite's** president] [* 12] knows it and is shopping hard. But Siebel and SAP already have turned him down. Hope Oracle does want in bad (and that's why they'll get). But it doesn't help job prospects in Morristown any does it?

Dendrite contends this statement falsely asserts **Dendrite** was secretly and unsuccessfully "shopping" the company. **Dendrite** states John Doe No. 3's claims that **Dendrite** is not competitive, that its president is aware of this and is trying to sell the company, and that the company is not desirable to potential purchasers, are all false.

In light of these statements, and those posted by other Yahoo! bulletin board users, **Dendrite** filed a verified complaint on May 24, 2000 against numerous fictitiously-named John Doe defendants, including John Doe No. 3. The complaint alleged that certain postings on the Yahoo! **Dendrite** bulletin board constituted breaches of contract, defamatory statements and misappropriated trade secrets. Relevant to this appeal, the complaint alleged that the aforementioned messages posted by John Doe No. 3 defamed **Dendrite** and misappropriated trade secrets. n2

-----Footnotes-----

n2 In this appeal, **Dendrite** bases its application seeking disclosure of John Doe No. 3's identity on its contention that John Doe No. 3's posted messages constitute actionable defamation.

-----End Footnotes----- [* 13]

Since most participants on the Yahoo! **Dendrite** bulletin board identified themselves through the use of pseudonyms unrelated to their actual identities, **Dendrite** sought an order to show cause why **Dendrite** should not be granted leave to conduct limited discovery for the purpose of ascertaining the true identity of the John Doe defendants Nos. 1 through 4. Accordingly, on June 20, 2000 the trial court issued an order directing these John Doe defendants to show cause why the relief requested by **Dendrite** should not be granted. The order further directed that this same notice be posted on the Yahoo! **Dendrite** bulletin board.

In the interim, the Public Citizen Litigation Group of Washington, D.C. filed a motion for leave to file a brief as amicus curiae. The trial court granted the motion and permitted the organization's participation.

On July 28, 2000 the motion judge heard argument on the order to show cause. At the close of argument, the judge reserved decision on **Dendrite's** motion to compel discovery purportedly necessary to identify these John Doe defendants.

On November 23, 2000, the motion judge issued a detailed written opinion, granting **Dendrite's** motion to conduct limited [* 14] discovery to ascertain the identities of John Doe defendants Nos. 1 and 2, but denied the motion as to John Doe defendants Nos. 3 and 4. In reaching his decision, the judge stated, in pertinent part:

The Court has been called upon to balance an individual's right to anonymously voice their opinions against a plaintiff's right to confront his accusers. . . . **Dendrite** has not made a prima facie case of defamation against John Doe No. 3, as **Dendrite** has failed to demonstrate that it was harmed by any of the posted messages. **Dendrite** has also failed to provide this Court with ample proof from which to conclude that John Does Nos. 3 and 4 have used their constitutional protections in order to conduct themselves in a manner which is unlawful or that would warrant this Court to revoke their constitutional protections. Therefore, **Dendrite's** request for limited expedited discovery, including the issuance of a commission to take discovery out-of-state is denied.

The conclusions of the judge were memorialized in an order executed on December 13, 2000.

By order entered on January 31, 2001, we granted **Dendrite's** motion for leave to appeal from that portion of the December 13, 2000 order [* 15] denying limited discovery as to John Doe No. 3.

On appeal, **Dendrite** presents the following arguments for our consideration:

POINT I

DISCOVERY OF THE IDENTITIES OF FICTITIOUS NAMED DEFENDANTS IS PERMISSIBLE UNDER BLACK-LETTER NEW JERSEY LAW.

POINT II

PLAINTIFF'S DEFAMATION CLAIM AGAINST JOHN DOE NO. 3 CAN WITHSTAND A DISMISSAL MOTION AND, ACCORDINGLY, DISCOVERY OF HIS IDENTITY IS WARRANTED.

- A. **Dendrite** Adequately Plead Harm to Survive a Motion to Dismiss.
- B. As a Matter of Pleading, **Dendrite** Is Not Required to Allege Harm.
- C. The Lower Court Erred to the Extent It Used a De Facto Summary Judgment Standard to Reject **Dendrite's** Defamation Claim.

POINT III

JOHN DOES ARE NOT ENTITLED TO SPECIAL DISCOVERY RULES TO PREVENT

PLAINTIFF FROM DISCOVERING THEIR IDENTITIES.

A. Defendants Are Not Entitled to Imposition of an Unduly Burdensome Proof Standard at the Initial Stage of This Lawsuit.

B. Requests for Disclosure of Defendants' True Identities Are Granted Routinely in Similar Cases Involving Subpoenas to Internet Service Providers.

C. Defendants Receive Little or No Privacy in Exchange for Their Use of Yahoo's Financial [* 16] Bulletin Board and Other Services.

D. Defendant's Tortious Conduct Is Not Protected by the First Amendment and Does Not Warrant Imposition of Any Special Discovery Rules.

✦ It is well-established that rights afforded by the First Amendment remain protected even when engaged in anonymously. [Buckley v. American Constitutional Law Found.](#), 525 U.S. 182, 197-99, 119 S. Ct. 636, 645-46, 142 L. Ed. 2d 599, 609-10 (1999); [McIntyre v. Ohio Elections Comm.](#), 514 U.S. 334, 115 S. Ct. 1511, 131 L. Ed. 2d 426 (1995); [Talley v. California](#), 362 U.S. 60, 80 S. Ct. 536, 4 L. Ed. 2d 559 (1960).

Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. [Talley v. California](#), 362 U.S. at 64, 80 S. Ct. at 538. Great works of literature have frequently been produced by authors writing under assumed names. Despite readers' curiosity and the public's interest in identifying the creator of a work of art, an author generally is free to decide whether or not to disclose his or her true identity. The decision in favor of anonymity may be motivated by fear of economic or official [* 17] retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.

[[McIntyre](#), *supra*, 514 U.S. at 341-42, [115 S. Ct. at 1516](#), [131 L. Ed. 2d at 436](#).]

In [Buckley](#), *supra*, 525 U.S. at 197-98, 119 S. Ct. at 645-46, 142 L. Ed. 2d at 606-08, the Court addressed a Colorado statute that required distributors of political petitions campaign materials to wear identifying badges and file affidavits disclosing their identity. There, the Court found the requirement that petitioners wear identifying badges was prohibitively burdensome on a person's right to anonymously exercise First Amendment rights. [Id.](#), 525 U.S. at 200, [119 S. Ct. at 646](#), [142 L. Ed. 2d at 614-15](#). [* 18] Specifically, the Court concluded that "the badge requirement discourages participation in the petition circulation process by forcing name identification without sufficient cause." *Ibid.*

In [Reno v. American Civil Liberties Union](#), *supra*, the Supreme Court made it clear that ✦ First Amendment Protections extend to speech on the [Internet](#). [521 U.S. at 885](#), [117 S. Ct. at 2351](#), [138 L. Ed. 2d at 906](#).

✦ New Jersey's State Constitution affords even greater protection to persons' rights to free speech than does our federal Constitution, specifically providing:

✦
 Every Person may freely speak, write and publish his sentiments on all subjects, being responsible for the abuse of that right. No law shall be passed to restrain or abridge the liberty of speech or of the press. In all prosecutions or indictments for libel, the truth may be given in evidence to the jury; and if it shall appear to the jury that the matter charged as libelous is true, and was published with good motives and for justifiable ends, the party shall be acquitted; and the jury shall have the right to determine the law and the fact.

[N.J. Const., Art. 1, par. 6.]

Our Supreme [* 19] Court has held that the rights attendant to this provision are "the most substantial in our constitutional scheme." [Green Party of New Jersey v. Hartz Mountain Indus., Inc., 164 N.J. 127, 144, 752 A.2d 315 \(2000\)](#) (quoting, New Jersey Coalition Against War in the [Middle East v. J.M.B. Realty, 138 N.J. 326, 364, 650 A.2d 757 \(1994\)](#), cert. denied, [516 U.S. 812, 116 S. Ct. 62, 133 L. Ed. 2d 25 \(1995\)](#)). In fact, "the reach of our constitutional provision [is] affirmative. Precedent, text, structure, and history all compel the conclusion that the New Jersey Constitution's right of free speech is broader than the right against governmental abridgement of speech found in the First Amendment." Coalition, supra, 138 N.J. at 352. Our Supreme Court has further clarified that ✦our "State right of free speech is protected not only from abridgment by government, but also from unreasonably restrictive and oppressive conduct by private entities." [Id. at 353.](#)

Assuming John Doe No. 3's statements are lawful, they would be afforded Constitutional protection, both under the First Amendment of the Federal Constitution and our [* 20] New Jersey Constitution. Accordingly, the discovery of John Doe No. 3's identity largely turns on whether his statements were defamatory or not.

✦ "The key principle in defamation/free expression cases is the 'profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open[.]'" [Sedore v. Recorder Pub. Co., 315 N.J. Super. 137, 146, 716 A.2d 1196 \(App. Div. 1998\)](#) (quoting [New York Times Co. v. Sullivan, 376 U.S. 254, 270, 84 S. Ct. 710, 721, 11 L. Ed. 2d 686, 701 \(1964\)](#)). "The law of defamation exists to achieve the proper balance between protecting reputation and protecting free speech." [Ward v. Zelikovskiy, 136 N.J. 516, 528, 643 A.2d 972 \(1994\)](#); Sedore, supra, 315 N.J. Super. at 146. "Thus, the purpose of the law of defamation is to strike the right balance between protecting reputation and preserving free speech." [Lynch v. New Jersey Educ. Ass'n, 161 N.J. 152, 166, 735 A.2d 1129 \(1999\)](#).

Dendrite argues on appeal that the motion judge imposed an inappropriate burden of proof when he evaluated whether **Dendrite's** claim could withstand a motion to dismiss. [* 21] **Dendrite** asserts this burden of proof is contrary to the recognized standards applicable to motions to dismiss, which require a judge to look liberally upon a complaint at the pleading stage. Moreover, **Dendrite** contends harm is not an element that must be pled in a defamation action, and if it is a required element of the pleading, then it has in fact

sufficiently pled that element.

In light of free speech and defamation considerations, as well as the fact that the Internet played a role in this dispute, the motion judge relied on the case of [Columbia Ins. Co., v. Seescandy.Com, 185 F.R.D. 573 \(N.D. Cal. 1999\)](#) to resolve whether he should permit **Dendrite** to conduct discovery to ascertain John Doe No. 3's identity. In Seescandy.Com, the Federal District Court for the Northern District of California addressed whether it should authorize limited discovery so that plaintiff could ascertain defendant's identity so as to effectuate service. [Id. at 575](#). There, the unknown defendant had registered an Internet domain name, "seescandy.com." [Id. at 575-76](#). Plaintiff, the assignee of various trademarks related to the operation of "See's [*22] Candy Shops, Inc.", sued the unknown defendants alleging that in registering that domain name the unknown defendant infringed on federally registered trademarks. [Id. at 576](#). However, the actual identity of the defendant who registered the domain name was unknown to plaintiff.

Although the Seescandy.Com case did not implicate defendant's free speech rights, as alleged here, the District Court recognized the unique circumstances created by the advent of the Internet and noted the following in regards to disclosing the identity of unknown Internet users:

With the rise of the Internet has come the ability to commit certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely on-line. The tortfeasor can act pseudonymously or anonymously and may give fictitious or incomplete identifying information. Parties who have been injured by these acts are likely to find themselves chasing the tortfeasor from Internet Service Provider (ISP) to ISP, with little or no hope of actually discovering the identity of the tortfeasor.

✦ In such cases the traditional reluctance for permitting filings against John Doe defendants or fictitious names [*23] and the traditional enforcement of strict compliance with service requirements should be tempered by the need to provide injured parties with a forum in which they may seek redress for grievances. However, this need must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously. People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity.

[[Id. at 578](#) (footnote omitted).]

In light of the particularly unique arena of discussion and communication created by the Internet forum, the District Court imposed certain [*24] limiting principles on "whether discovery to uncover the identity of a defendant is warranted" under such circumstances. [Id. at 578](#). The court outlined a four-prong approach to this issue seeking to "ensure that this unusual procedure will

only be employed in cases where the plaintiff has in good faith exhausted traditional avenues for identifying a civil defendant pre-service, and will prevent use of this method to harass or intimidate." Ibid.

First, the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court." Ibid. Second, plaintiff must "identify all previous steps taken to locate the elusive defendant" to demonstrate that plaintiffs have made a good-faith effort to comply with the requirements of service of process. Id. at 579. Third, and most relevant to this appeal, "plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss." Ibid. Fourth, the moving "plaintiff should file a request for discovery with the Court, along with a statement [*25] of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible." Id. at 580.

Relying on Seescandy.Com, the motion judge reasoned that **Dendrite** did not satisfy the third prong -- the ability to withstand a motion to dismiss -- because it failed to make out a prima facie case of defamation against John Doe No. 3. Accordingly, the judge concluded **Dendrite** was not entitled to conduct limited discovery to ascertain the identity of John Doe No. 3. Specifically, the judge found **Dendrite** failed to show that the statements posted by John Doe No. 3 caused **Dendrite** any harm. n3 **Dendrite** contends the motion judge imposed an excessively demanding burden of proof, generally not required when defending a motion to dismiss.

-----Footnotes-----

n3 The judge found the first prong satisfied because "the assumption that this court has jurisdiction and that venue is proper is not unfounded, and, without evidence to the contrary, jurisdiction will be presumed." Regarding the second prong he found "**Dendrite** has not provided the Court with any previously taken steps aimed at locating the defendants[;]" however, the judge reasoned **Dendrite** could not have been expected to know they were supposed to attempt to identify the defendants on their own since he had just invoked the Seescandy.Com test. Lastly, the judge made no findings concerning the fourth prong of the test.

-----End Footnotes----- [* 26]

Dendrite cites to Printing Mart-Morristown v. Sharp Electronics Corp., 116 N.J. 739, 563 A.2d 31 (1989) to support this contention. There, our Supreme Court reviewed, in part, whether we properly upheld dismissal of a plaintiff's defamation claim for a failure to state a cause of action. Id. at 744. The Court initially established that the review of plaintiffs' pleadings on a motion to dismiss are entitled to deference, stating:

We approach our review of the judgment below mindful of the test for determining the adequacy of a pleading: whether a cause of action is "suggested" by the facts. In reviewing a complaint dismissed under Rule 4:6-

2(e) our inquiry is limited to examining the legal sufficiency of the facts alleged on the face of the complaint. However, a reviewing court "searches the complaint in depth and with liberality to ascertain whether the fundament of a cause of action may be gleaned even from an obscure statement of claim, opportunity being given to amend if necessary." At this preliminary stage of the litigation the Court is not concerned with the ability of plaintiffs to prove the allegation contained in the complaint. For purposes [*27] of analysis plaintiffs are entitled to every reasonable inference of fact. The examination of a complaint's allegations of fact required by the aforestated principles should be one that is at once painstaking and undertaken with a generous and hospitable approach.

[[Id. at 746](#) (citations omitted).]

The Court reversed, finding three of six contested statements made by defendants were "open to a defamatory meaning and actionable on their face." [Id. at 766](#). Those three statements asserted plaintiffs were (1) "'ripping off" clients; (2) plaintiffs "'were not qualified to do the work for defendant . . . (if stated as fact rather than merely as opinion, an issue to be determined at trial)"; and (3) that plaintiffs "did unreasonably-priced, inadequate work." Ibid. The Court found the import of these statements to be clear, and concluded "that those statements could not be held as a matter of law to be not defamatory." [Id. at 766-67](#).

Dendrite's verified complaint alleges, in relevant part, the following:

46. Defendants' publication of these statements has caused irreparable harm to **Dendrite** for which **Dendrite** has [*28] no adequate remedy at law, and will continue to cause such irreparable harm unless restrained by this Court. In addition, as a proximate result of defendants' publication of these statements, **Dendrite** has sustained harm to its business reputation resulting in damages in an amount to be proven at trial, and **Dendrite** will continue to suffer additional damages in the future according to proof.

47. **Dendrite** is informed and believes, and thereon alleges, that defendants' publication of these statements was willful, malicious and oppressive, in that they intended to harm the business reputation of **Dendrite**. These acts, therefore, justify awarding of punitive damages.

In addition, the complaint highlights the postings made by John Doe No. 3, which asserted **Dendrite** had changed its revenue recognition policy and that **Dendrite** was "shopping" the company.

Dendrite argues that in applying the motion-to-dismiss standard, the motion judge ignored the Court's direction to review pleadings on motions to dismiss with liberality and generosity and, instead, applied a de facto summary judgment standard. **Dendrite** asserts the judge mistakenly concluded that **Dendrite** must prove "actual reputational [*29] injury" in its complaint.

Our review of the motion judge's analysis of the harm/injury element of **Dendrite's** defamation claim reveals he required more evidentiary support for the pleading than is traditionally required when applying motion-to-dismiss standards. The judge relied on [McLaughlin v. Rosanio, Bailets & Talamo, Inc.](#),

[331 N.J. Super. 303, 751 A.2d 1066 \(App. Div. 2000\)](#), as the basis for outlining the requirement for a defamation cause of action. However, it is clear the judge implemented an analysis that relied on more than a motion-to-dismiss standard, stating:

It is not obvious that the statements at issue are false or that **Dendrite** has been harmed. **Dendrite** has failed to show that the messages in question in any way harmed **Dendrite**. Although **Dendrite** alleges that it has been harmed and that it will continue to be harmed by the defendants' statements, saying it is so does not make the alleged harm a verifiable reality. In his reply certification, Michael Vogel, **Dendrite's** counsel, attempts to link the messages posted in this case to a drop in **Dendrite's** stock price. . . . Furthermore, Mr. Vogel has not purported to be an expert in the field [*30] of stock valuation and analysis, thus, he cannot draw the conclusion that the fluctuations in **Dendrite's** stock prices are anything more than coincidence.

Despite the fact that Plaintiff is entitled to every reasonable inference of fact in this analysis of whether a case against John Doe No. 3 could survive dismissal, the Court will not take the leap to linking messages posted on an Internet message board regarding individual opinions, albeit incorrect opinions, to a decrease in stock prices without something more concrete.

[(Emphasis added).]

This analysis reveals that the motion judge engaged in a more probing review of **Dendrite's** complaint and pleadings than outlined in Printing Mart, requiring specific proof establishing **Dendrite's** harm as an element of its defamation claim. The judge found **Dendrite** had not established that fluctuations in its stock prices were a result of John Doe No. 3's postings, and could not find any nexus between the postings and the drop in **Dendrite's** stock prices.

✦"In the case of a complaint charging defamation, plaintiff must plead facts sufficient to identify the defamatory words, their utterer and the fact of their publication." [*31] [Zoneraich v. Overlook Hosp., 212 N.J. Super. 83, 101, 514 A.2d 53](#) (App. Div.), cert. denied, [107 N.J. 32 \(1986\)](#). Here, **Dendrite** has (1) identified the "revenue recognition" and "shopping" statements as purportedly defamatory words, (2) identified "xxplrr" (John Doe No. 3) as the utterer, and (3) established that they were in fact published on Yahoo!'s bulletin board. Accordingly, **Dendrite** meets the bare minimum requirements for a defamation cause of action, and would survive a motion to dismiss under the traditional application of R. 4:6-2(e).

However, application of our motion-to-dismiss standard in isolation fails to provide a basis for an analysis and balancing of **Dendrite's** request for disclosure in light of John Doe No. 3's competing right of anonymity in the exercise of his right of free speech.

We first note that the motion judge was not presented with an actual motion to dismiss and, as such, was not necessarily bound to a dogmatic application of the associated rules. Nonetheless, the third prong of the Seescandy.Com test requires a showing that plaintiff's claim would survive a motion to dismiss. However, a closer analysis discloses [*32] that the District Court distinguished the actual application of the third prong of the test from the

traditional application of a motion-to-dismiss standard, stating:

Pre-service discovery is akin to the process used during criminal investigations to obtain warrants. The requirement that the government show probable cause is, in part, a protection against the misuse of ex parte procedures to invade the privacy of one who has done no wrong. A similar requirement is necessary here to prevent abuse of this extraordinary application of the discovery process and to ensure that plaintiff has standing to pursue an action against defendant.

[Seescandy.Com, supra, 185 F.R.D. at 579-80.]

Probable cause as it relates to obtaining warrants is a non-technical, flexible concept that does not require rigid, "technical demands for specificity and precision[.]" [State v. Boyd, 44 N.J. 390, 392-93, 209 A.2d 134 \(1965\); Ornelas v. United States, 517 U.S. 690, 695-96, 116 S. Ct. 1657, 1661, 134 L. Ed. 2d 911, 918 \(1996\)](#). The District Court added that by equating this prong to the probable cause requirement for warrants, "plaintiff must make **[*33]** some showing that an act giving rise to civil liability actually occurred and that the discovery is aimed at revealing specific identifying features of the person or entity who committed the act." [185 F.R.D. at 580](#) (emphasis added).

In fact, the literal reading of the third prong of the Seescandy.Com test, as worded by the District Court, supports such a flexible, non-technical application of the motion to dismiss standard. Specifically, the third prong provides "plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss." Seescandy.Com, supra, 185 F.R.D. at 579 (emphasis added). The court characterized the four-prong test as "safeguards," necessary to "prevent [plaintiffs from] harassing or intimidating" anonymous persons on the Internet. Ibid.

Our review of Seescandy.Com discloses that a strict application of our rules surrounding motions to dismiss is not the appropriate litmus test to apply in evaluating the disclosure issue. We conclude that the District Court envisioned this four-part test to act as a flexible, non-technical, fact-sensitive mechanism for courts to use as a **[*34]** means of ensuring that plaintiffs do not use discovery procedures to ascertain the identities of unknown defendants in order to harass, intimidate or silence critics in the public forum opportunities presented by the Internet.

Analogous circumstances were recently presented to the Virginia Circuit Court in [In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26, 2000 WL 1210372, *1](#) (Va. Cir. Ct. 2000). There, a publicly traded company sought and obtained an order from an Indiana court authorizing plaintiff to conduct discovery in order to ascertain the identities of certain John Does who posted allegedly defamatory comments on a stock-trading Internet chat room maintained by America Online (AOL). AOL refused to voluntarily comply with the order to disclose its subscribers' identities, contending disclosure of the subscribers' identities pursuant to the subpoena would impair the subscribers' First Amendment rights to speak anonymously. Id. at *2. Ultimately, the circuit court ordered AOL to disclose the identities, establishing a test functionally similar to that put forth in Seescandy.Com, as follows:

[A] court should only order a non-party, Internet **[*35]** service provider to

provide information concerning the identity of a subscriber (1) when the court is satisfied by the pleadings or evidence supplied to that court (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and (3) the subpoenaed identity information is centrally needed to advance that claim.

[Id. at *8.]

The test created by the Virginia Circuit Court departed from that state's traditional legal standard applied when ruling on a motion to quash a subpoena. Id. at *2, *7. Although the Circuit Court ordered disclosure of the identities of the John Doe defendants, it found a more probing evaluation into the "bona fides of [plaintiff's] claim was necessary in order to properly evaluate the reasonableness of the subpoena request in light of all the surrounding circumstances." Id. at *8.

The Virginia case supports the notion that when evaluating a plaintiff's request to compel an ISP to disclose the identity of a John Doe subscriber, courts may depart from traditionally-applied legal standards in analyzing the appropriateness of [*36] such disclosure in light of the First Amendment implications.

Here, although **Dendrite's** defamation claims would survive a traditional motion to dismiss for failure to state a cause of action, we conclude the motion judge appropriately reviewed **Dendrite's** claim with a level of scrutiny consistent with the procedures and standards we adopt here today and, therefore, the judge properly found **Dendrite** should not be permitted to conduct limited discovery aimed at disclosing John Doe No. 3's identity. Moreover, the motion judge's approach is consistent with the approach by both the District Court in *Seescandy.Com*, and by the Virginia Circuit Court in the *America Online* decision.

A defamatory statement is one that is false and 1) injures another person's reputation; 2) subjects the person to hatred, contempt or ridicule; or 3) causes others to lose good will or confidence in that person. [Romaine v. Kallinger, 109 N.J. 282, 289, 537 A.2d 284 \(1988\)](#). A defamatory statement harms the reputation of another in a way that lowers the estimation of the community about that person or deters third persons from associating or dealing with him. [McLaughlin v. Rosanio, supra, 331 N.J. Super. at 312; \[*37\]](#) Restatement (Second) of Torts § 559 (1977). "Words that clearly denigrate a person's reputation are defamatory on their face and actionable per se." *Printing Mart-Morristown, supra*, 116 N.J. at 765. "When determining if a statement is defamatory on its face "a court must scrutinize the language 'according to the fair and natural meaning which will be given it by reasonable persons of ordinary intelligence.'" *Ibid.* (quoting *Romaine, supra*, 109 N.J. 282 at 290, [537 A.2d 284](#)). A plaintiff does not make a prima facie claim of defamation if the contested statement is essentially true. [Hill v. Evening News Co., 314 N.J. Super. 545, 552, 715 A.2d 999 \(App. Div. 1998\)](#).

The motion judge determined that **Dendrite** failed to demonstrate the statements posted by John Doe No. 3 caused it any harm. The certification of **Dendrite** Vice-President, Bruce Savage alleges John Doe No. 3's postings "may

. . . have a significant deleterious effect on **Dendrite's** ability to hire and keep employees." (Emphasis added). **Dendrite** also contends that John Doe No. 3's postings caused detrimental fluctuations in its stock prices.

Dendrite's NASDAQ trading [* 38] records were submitted to the court for the period of March 1, 2000 through June 15, 2000. Those records indicate **Dendrite** experienced gains on 32 days, losses on 40 days, and no change on two days during that period, which overlaps the period when John Doe No. 3 was posting his statements on the Yahoo! bulletin board. **Dendrite's** total loss during this period was 29/32 of a point.

Moreover, John Doe No. 3 made nine postings, two on the same day. On three of the days that immediately followed a posting by John Doe No. 3, **Dendrite's** stock value decreased. However, on five of the days that immediately followed a posting by John Doe No. 3, **Dendrite's** stock value increased. The net change in **Dendrite's** stock value over those seven days was actually an increase of 3 and 5/8 points.

Although the motion judge stated **Dendrite** was "entitled to every reasonable inference of fact in this analysis[,]" he refused to "take the leap to linking messages posted on an internet message board regarding individual opinions, albeit incorrect opinions, to a decrease in stock prices without something more concrete." The record does not support the conclusion that John Doe's postings negatively affected [* 39] the value of **Dendrite's** stock, nor does **Dendrite** offer evidence or information that these postings have actually inhibited its hiring practices, as it alleged they would. Accordingly, the motion judge appropriately concluded that **Dendrite** failed to establish a sufficient nexus between John Doe No. 3's statements and **Dendrite's** allegations of harm.

We are satisfied that the analysis and conclusions by Judge MacKenzie set forth in his comprehensive letter opinion dated November 23, 2000 are supported by the record. **Dendrite** has failed to establish that the judge abused his discretion in entering the December 13, 2000 order.

Accordingly, we affirm.

Source: [All Sources](#) > [Combined Federal & State Case Law - U.S.](#) > [Most Recent Year Federal and State Cases](#) 

Terms: **dendrite international inc** ([Edit Search](#))

View: Full

Date/Time: Sunday, August 12, 2001 - 3:32 PM EDT

EXHIBIT C

This is an example of the kinds of complaints filed in John Doe cases. This example complaint was prepared by Roger Furey at the D.C. office of Katten Muchin Zavis. He can be reached at the following address:

Roger Furey, Esq.
Katten Muchin Zavis.
1025 Thomas Jefferson Street, N.W.
East Lobby, Suite 700
Washington, D.C. 20007-5201
(202) 625-3630

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

FAKE COMPANY, INC.,
XXXX
XXXX
XXXX
a Delaware Corporation,
Plaintiff,
v.
JOHN DOE
Defendant.
Civil Action No. _____

COMPLAINT

Plaintiff Fake Company, Inc., for its Complaint against Defendant John Doe, alleges as follows:

JURISDICTION AND VENUE

- 1. This action is for common law defamation, tortious interference with contractual relationships, and tortious interference with prospective economic advantage.
2. This Court has jurisdiction over the subject matter and the parties pursuant to the Judicial Code, 28 U.S.C. §§ 1332. Upon information and belief, this dispute involves citizens of different States. The amount in controversy exceeds the sum or value of \$75,000, exclusive of interest and costs.
3. This court has in personam jurisdiction over Defendant because he posted the defamatory and damaging communication on the Internet, after contracting with a multimedia publisher with headquarters in this District, and utilizing the services of that

publisher. Moreover, Defendant's tortious acts were maliciously targeted at Plaintiff, who is incorporated in and has its principal place of business in this District.

4. Venue is proper in this District under 28 U.S.C. § 1391(a).

THE PARTIES

5. Plaintiff Fake Company, Inc. is a Delaware corporation, having its principal place of business at 111 Compete Drive, Reston, Virginia 22182. Fake Company markets a wide variety of communications services, including local telephone services, long distance telephone services and Internet services, through digital communications networks that Fake Company has built, and continues to build, throughout the United States.

6. Upon information and belief, Defendant John Doe transacts business within this District by posting communications on the Internet utilizing the services of a multimedia publisher with headquarters in this District, using the alias "Mad Hatter12". The true name and capacity of John Doe, whether individual, corporate, associate or otherwise, is unknown to Plaintiff at this time. Plaintiff will amend this complaint to show John Doe's true name and capacity when the same have been ascertained.

BACKGROUND

7. On September 16, 2000, Defendant, using the alias "Mad Hatter12", posted the following message on an Internet world-wide web Message Board maintained by The Biz Talk Now, a multimedia publisher headquartered in Alexandria, Virginia:

Fake Company during a conference call announced yesterday that it will be eliminating the jobs of their data specialists and sales managers across the country. Fake Company states that a portfolio of data products outside of simple internet access does not fit in with their market plans. Instead

Fake Company just wants to focus on the sale of long distance products.

The reason given for the cuts is that data orders are too difficult to provision and maintain. Obviously this is good news for their competitors including Big Company, Giant Company, etc. It gives them the edge in offering broadband services to customers.

See <http://boards.com/message.asp?id=XXXXXXXX=postedate>.

8. The information contained in this message is false, and is damaging to Plaintiff's reputation, prestige and standing in the telecommunications and Internet services industry, and in the marketplace for telecommunications and Internet services. Defendant's message purports to provide information obtained directly from Plaintiff to the effect that Plaintiff is abandoning a significant portion of the broadband service market, and taking a back seat in this highly competitive area to businesses such as Big Company and Giant Company. As a publicly traded corporation, Plaintiff has suffered and will continue to suffer harm to the value of its stock because investors will place a reduced value on the stock of Plaintiff on the basis of this false information. Plaintiff has also been damaged, and will continue to be damaged, in its contractual relationships and prospective contractual relationships with customers, vendors and sources of financing, who will be less likely to contract with Plaintiff based on this false information.

9. Upon information and belief, Defendant published this false information for the express purpose of damaging Fake Company's reputation in the industry and marketplace, and/or to enhance the reputation of the competitors referenced in Defendant's message, Big Company and Giant Company.

10. On September 17, 2000, Plaintiff contacted the publisher whose web site is being used to communicate the false messages, The Biz Talk Now, but The Biz Talk Now has refused to provide information that may identify Defendant John Doe, citing privacy provisions in its contract with Defendant. Consequently, Plaintiff has been forced to file this Complaint naming Defendant as a John Doe.

COUNT I

DEFAMATION UNDER THE COMMON LAW OF VIRGINIA

11. Plaintiff hereby incorporates by reference and realleges paragraphs 1- 10 as if fully set forth herein.

12. Defendant has intentionally and maliciously made, and continues to make, false and/or misleading representations on The Biz Talk Now's Message Board about Plaintiff's business operations, plans and services, in reckless disregard for the truth.

13. Defendant's false and/or misleading descriptions and representations are material and have deceived or misled actual and prospective customers, investors and contracting parties. Defendant's statements have caused a diminishment in esteem, respect, goodwill and confidence in which Plaintiff is held, and have caused injury to Plaintiff's business reputation and good name.

14. Upon information and belief, Defendant's false and/or misleading descriptions and representations have caused and will continue to cause substantial damage to the value of Plaintiff's stock, and have caused prospective customers to avoid doing business with Plaintiff. As a result, Defendant's wrongful conduct has caused monetary loss to Plaintiff in an amount well in excess of the jurisdictional requirements of this Court, in an amount to be proved at trial.

COUNT II**INTENTIONAL INTERFERENCE WITH BUSINESS RELATIONSHIPS
UNDER THE COMMON LAW OF VIRGINIA**

15. Plaintiff hereby incorporates by reference and realleges paragraphs 1-14 as if fully set forth herein.

16. At the time Defendant published the defamatory statements, Defendant had actual knowledge that third parties had contracted with Plaintiff for the purpose of utilizing Plaintiff's telecommunications and Internet services. In addition, upon information and belief, Defendant had actual knowledge that third party vendors, sources of financing and other contracting parties had contracted with Plaintiff for the purpose of conducting business with Plaintiff.

17. Defendant intentionally and maliciously published the defamatory comments for the purpose of confusing Plaintiff's customers and dissuading them from continuing to do business with Plaintiff. Upon information and belief, Defendant's wrongful actions have had the intended consequences.

18. Defendant intentionally and maliciously published the defamatory comments for the purpose of confusing Plaintiff's customers and other contracting parties and causing them to terminate or alter their business relationships with Plaintiff. Upon information and belief, Defendant's wrongful actions have had the intended consequences.

19. Upon information and belief, as a direct result of Defendant's defamatory statements, Plaintiff has lost actual sales to its customers and has otherwise suffered economic and irreparable damage well in excess of the jurisdictional requirements of this Court.

COUNT III**INTENTIONAL INTERFERENCE WITH PROSPECTIVE ECONOMIC
ADVANTAGES
UNDER THE COMMON LAW OF VIRGINIA**

20. Plaintiff hereby incorporates by reference and realleges paragraphs 1-19 as if fully set forth herein.

21. At the time Defendant published the defamatory statements, Defendant knew that Plaintiff was negotiating with prospective customers in an effort to enter into contracts for the purpose of providing Plaintiff's services to those prospective customers. Defendant further knew that Plaintiff was negotiating with potential vendors, suppliers and sources of financing regarding a variety of possible contractual relationships.

22. Defendant intentionally and maliciously published the defamatory comments in an attempt to interfere with Plaintiff's efforts to enter into these contractual relationships. Upon information and belief, Defendant's wrongful actions have had the intended consequences.

23. As a direct result of Defendant's actions in interfering with Plaintiff's prospective contractual relationships, Plaintiff has suffered and is continuing to suffer economic and irreparable damage well in excess of the jurisdictional requirements of this Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court:

1. Preliminarily and permanently enjoin and restrain Defendant, his employees, agents, and all others in active concert or participation with Defendant, from further dissemination of false or misleading information about Plaintiff's business operations or services, whether on The Biz Talk Now or otherwise.

2. Require Defendant to:
 - a. pay to Plaintiff such damages as have been suffered by Plaintiff, in an amount to be proven at trial, but in excess of \$75,000;
 - b. pay punitive damages to Plaintiff;
 - c. pay to Plaintiff the costs of this action, together with Plaintiff's reasonable attorneys' fees and expenses,
 - d. immediately submit a message to the same The Biz Talk Now Board stating that Defendant's original comments were false, that there was no basis for the comments, and that Plaintiff was never privy to a conference call in which the subject matter of the message was discussed,
 - e. file with this Court and serve on Plaintiff a report in writing and under oath setting forth in detail the manner and form in which Defendant has complied with the terms of any injunction entered by this Court.
3. Grant Plaintiff such other and further relief as this Court deems just and proper.

Respectfully submitted,

Roger P. Furey, Va. Bar #23575

Katten Muchin Zavis.
1025 Thomas Jefferson Street, N.W.
East Lobby, Suite 700
Washington, D.C. 20007-5201
(202) 625-3630

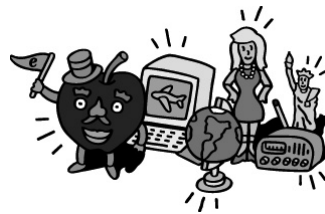
Counsel for Plaintiff
Fake Company, Inc.



To Bot or Not: Using the Law to Prevent Web Site Access

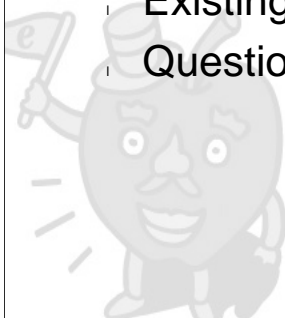
ACCA Annual Meeting
San Diego California

Jay Monahan
October 16, 2001



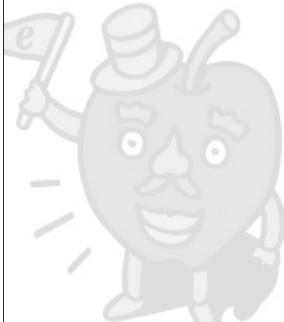
Overview on Robots and the Law

- | What are robots (spiders, crawlers, 'bots) and why do we care?
- | Weapons to stop bots
- | Existing case law
- | Questions for discussion



'Bot Defined

- A 'Bot (aka robot or "spider") is a software device which accesses a web site and performs various functions at super-human speeds



'Bots Are Fast and Unpredictable

Data Profile is very different

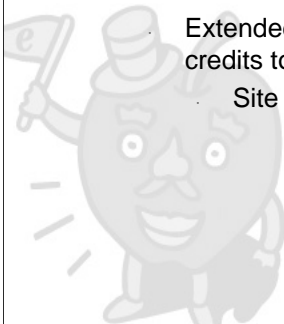
- A single 'Bot can process 20-1000 times the data a user can in the same time
- Unpredictable and higher peak loads
- We would have to expand our capacity to handle these artificial peaks; i.e., more expenses



'Bots Can Lead to Degraded Site Performance and Outage

Degraded Performance

- Partial or Complete Loss of Functionality
 - Any 'Bot-access effectively "steals" capacity from a human user
- Slow-downs affect **velocity of trade** and directly translate into lost revenue
- Extended outages leads to increased losses through credits to our community
 - Site Outage in 6/11/99: \$ write-off

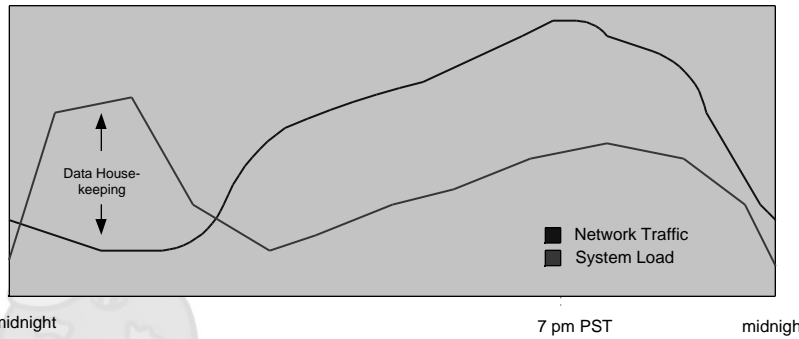


Kinds of 'Bots and Their Targets

- Email addresses -- personal information
- Price information
- Auction listings
- Ad insertion/Images
- Job listings
- Movie/TV Listings
- Golf scores
- Domain registration information



Network Traffic vs. System Load



Data Housekeeping includes end-of-auction processing, data warehousing, reports, archival, backups



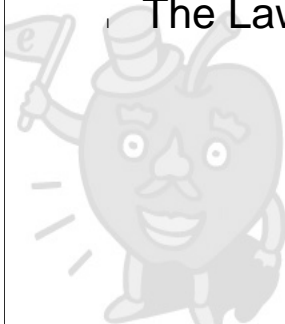
Are 'Bots a Problem for eBay?

- 10% of traffic to entire site appears to be some type of bot
- Costs eBay millions \$ each year to support unwanted, possibly harmful access
- Has interfered with site performance and caused outages in past
- Users get harmed by results (e.g., spamming)



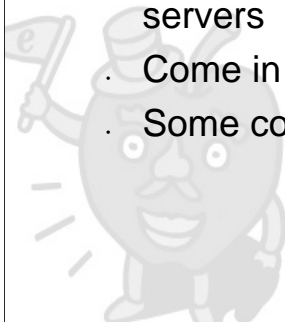
Potential Weapons for Fighting Against 'Bots

- Technology
- No Trespassing Signs--Terms of Use
- Contracts
- The Law



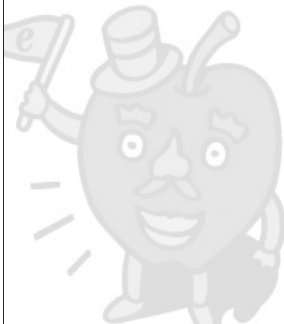
Technology: Can't You Just Block or Stop 'Bots?

- Can be very difficult to block IP addresses/'Bots
- Companies get around by IP spoofing, Switching IP addresses, rotating proxy servers
- Come in through the same way users do
- Some companies bragging about it



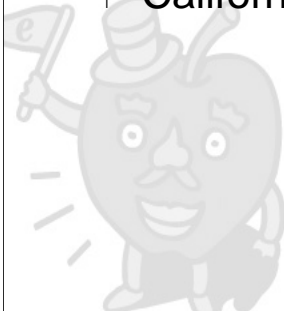
No Trespassing Signs

- Anti-Robot Protocols—strictly voluntary, but helpful
- Terms of Use



Legal Theories Sounding in Trespass

- Trespass--state laws (Bidder's Edge)
- Computer Fraud and Abuse Act, 18 U.S.C. Section 1030
- California Penal Code 502(c)



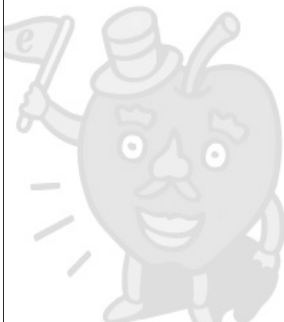
18 U.S.C. Section 1030

- Statute directed to, but not limited to hacking situations
- Applied in Register.com vs. Verio
- Argued in Bidder's Edge


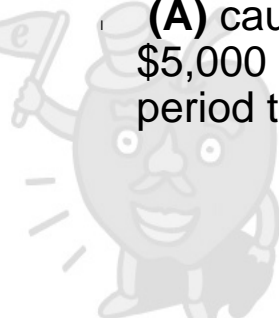


Unauthorized Access



- **(C)** intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;



<h2>Damage</h2>
<ul style="list-style-type: none">· (8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that--<ul style="list-style-type: none">· (A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals;

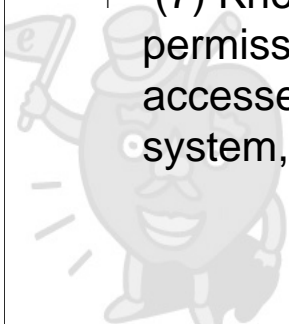


<h2>California Penal Code Section 502(c)</h2>
<ul style="list-style-type: none">· Criminal penalties· Private right of action provided since January 2001· Attorneys' fees provision



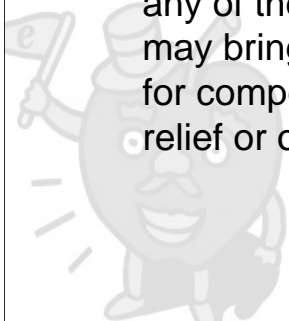
Statutory Language 502(c)

- any person who commits any of the following acts is guilty of a public offense:
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.



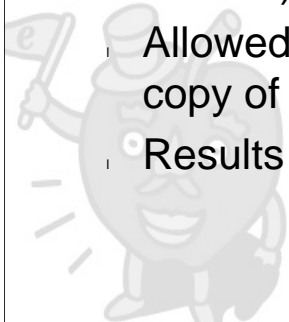
Civil Action Under 502(c)

- the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief.



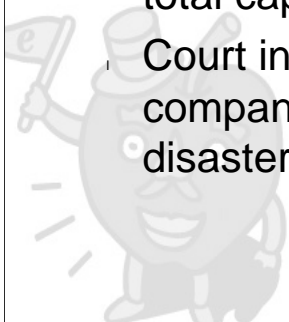
eBay vs. Bidder's Edge

- Periodically used 'Bot to access eBay site and copy over 100,000 category listing pages (every category page on the site)
- Allowed BE users to search their copy of our data
- Results incomplete, inaccurate



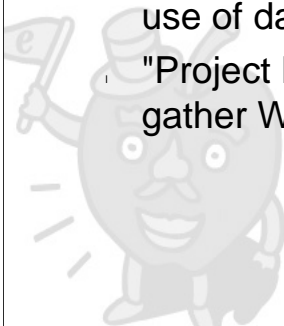
eBay vs. Bidder's Edge

- Preliminary injunction issued based upon common law trespass
- Court found that BE occupied 1.8% of total capacity of eBay Listing Servers
- Court influenced by risk of additional companies—eBay need not wait for disaster to come to court for relief



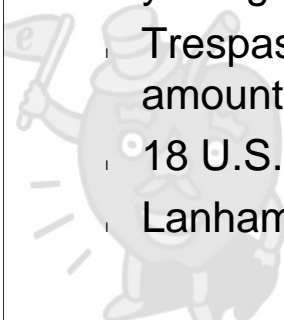
Register.com v. Verio

- Verio not a registrar but competes directly with Register.co in offering certain Internet services, e.g., web hosting, development
- Register.com User Agreement prohibits use of data for spam; Terms of Use
- "Project Henhouse" -- robots used to gather Whois information



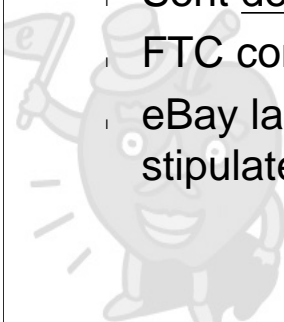
Register.com v. Verio (cont.)

- Terms of use held enforceable event though Verio never affirmatively assented ["by submitting this query, you agree to abide by these terms."]
- Trespass to chattels--yes, exact amount of "damage" not required
- 18 U.S.C section 1030--yes
- Lanham Act--yes



eBay vs. ReverseAuction.com

- Robotically accessed eBay site and harvested eBay User IDs, email addresses and feedback ratings.
- Sent deceptive spam to eBay users
- FTC consent decree
- eBay lawsuit and \$1.2 million stipulated judgment



Beyond Trespass

- Misappropriation (database protection)
- False Advertising/business Reputation
- Unfair Business Practices
- Trademark Infringement/Dilution
- Copyright Infringement
- Hot News Doctrine



Discussion Questions re: Robots and the Law

- What rights should a web site have to prevent access?
- Does the current case law mean that any access, such as linking, can be prohibited?



Thank You



**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

NO. C-99-21200 RMW

**ORDER GRANTING PRELIMINARY
INJUNCTION**

[Docket Nos. 6, 12]

**EBAY, INC.,
*Plaintiff,***

vs.

**BIDDER'S EDGE, INC.,
*Defendant.***

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 papers¹ and heard the argument of counsel. For the reasons set forth below, the court preliminarily enjoins defendant Bidder's Edge, Inc. ("BE") from accessing eBay's computer systems by use of any automated querying program without eBay's written authorization.

I. BACKGROUND

eBay is an Internet-based, person-to-person trading site. (Jordan Decl. =B6 3.) eBay offers sellers the ability to list items for sale and prospective buyers the ability to search those listings and bid on items. (Id.) The seller can set the terms and conditions of the auction. (Id.) The item is sold to the highest bidder. (Id.) The transaction is consummated directly between the buyer and seller without eBay's involvement. (Id.) 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. (Id.) eBay has also created category listings which identify items in over 2500 categories, such as antiques, computers, and dolls. (Id.)

Users may browse these category listing pages to identify items of interest. (Id.) Users of the eBay site must register and agree to the eBay User Agreement. (Id. =B6 4.) Users agree to the seven page User Agreement by clicking on an "I Accept" button located at the end of the User Agreement. (Id. Ex. D.) 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." (Id.) 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. (Jordan Decl. =B6 4.) Over 400,000 new items are added to the site every day. (Id.) Every minute, 600 bids are placed on almost 3 million items. (Id.) 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. (Id.) 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.² (Maynor Decl. =B6 3; Johnson-Laird Decl. =B6 15.)

A software robot is capable of executing thousands of instructions per minute, far in excess of what a human can accomplish. (Maynor Decl. =B6 3) 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. (Id.) 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." (Id.) A severe malfunction can cause a loss of data and an interruption in services. (Id.)

The eBay site employs "robot exclusion headers." (Id. =B6 5.) 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. (Id.) 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. (Johnson-Laird Decl. =B6 20.)

To enable computers to communicate with each other over the Internet, each is assigned a unique Internet Protocol ("IP") address. (Maynor Decl. =B6 6.) 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. (Id.) These IP addresses allow the identification of the source of incoming requests. (Id.) eBay identifies robotic activity on its site by monitoring the number of incoming requests from each particular IP address. (Id. =B6 7.) Once eBay identifies an IP address believed to be involved in robotic activity, an investigation into the identity, origin and owner of the IP address may be made in order to determine if the activity is legitimate or authorized. (Id. =B6 8.) If an investigation reveals unauthorized robotic activity, eBay may attempt to ignore ("block") any further requests from that IP address. (Id.) Attempts to block requests from particular IP addresses are not always successful. (Id. =B6 9; Johnson-Laird Decl. =B6 27.)

Organizations often install "proxy server" software on their computers. (Johnson-Laird Decl. =B6 12.) Proxy server software acts as a focal point for outgoing Internet requests. (Id.) Proxy servers conserve system resources by directing all outgoing and incoming data traffic through a centralized portal. (Id.) Typically, organizations limit the use of their proxy servers to local users. (Id.) However, some organizations, either as a public service or because of a failure to properly protect their proxy server through the use of a "firewall," allow their proxy servers to be accessed by remote users. (Id. =B6 13.) Outgoing requests from remote users can be routed through such unprotected proxy servers and appear to originate from the proxy server. (Id.) Incoming responses are then received by the proxy server and routed to the remote user. (Id.) 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. (Id. =B6 14.) 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. (Id. =B6 22.)

BE is a company with 22 employees that was founded in 1997. (Carney Decl. =B6 2.) The BE web site debuted in November 1998. (Id. =B6 3.) BE does not host auctions. (Id. =B6 2.) 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. (Id.) As of March 2000, the BE web site contained information on more than five million items being auctioned on more than one hundred auction sites. (Id. =B6 3.) BE also

provides its users with additional auction-related services and information. (Id. =B6 2.) 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. (Id. =B6 4.) 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. (Id. =B6 5.) 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. (Id. =B6 6.) 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. (Id.)

On June 16, 1997, over a year before the BE web site debuted, Peter Leeds³ wrote an email in response to an email from Kimbo Mundy, co-founder of BE. (Ritchey Decl. Ex 6.) Mundy's email said, "I think the magazines may be overrating sites' ability to block. The early agent experiments, like Arthur Anderson's BargainFinder were careful to check the robots.txt file on every site and desist if asked." (Id.) (underline in original). Mundy wrote back: "I believe well-behaved robots are still expected to check the robots.txt file. . . . Our other concern was also legal. It is one thing for customers to use a tool to check a site and quite another for a single commercial enterprise to do so on a repeated basis and then to distribute that information for profit." (Id.) In early 1998, eBay gave BE permission to include information regarding eBay-hosted auctions for Beanie Babies and Furbies in the BE database. (Id. =B6 7.)

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. (Id. =B6 8.) On April 24, 1999, eBay verbally approved BE crawling the eBay web site for a period of 90 days. (Id.) The parties contemplated that during this period they would reach a formal licensing agreement. (Id.) They were unable to do so.

It appears that the primary dispute was over the method BE uses to search the eBay database. eBay wanted BE to conduct a search of the eBay system only when the BE system was queried by a BE user. (Ploen Decl. Ex. 9.) This reduces the load on the eBay system and increases the accuracy of the BE data. (Id.) BE wanted to recursively crawl the eBay system to compile its own auction database. (Carney Decl. =B6 18.) This increases the speed of BE searches and allows BE to track the auctions generally and automatically update its users when activity occurs in particular auctions, categories of auctions, or when new items are added. (Id.)

In late August or early September 1999, eBay requested by telephone that BE cease posting eBay auction listings on its site. (Id. =B6 9; Rock Decl. =B6 5.) BE agreed to do so. (Rock Decl. =B6 5.) In October 1999, BE learned that other auction aggregations sites were including information regarding eBay auctions. (Carney Decl. =B6 12.) On November 2, 1999, BE issued a press release indicating that it had resumed including eBay auction listings on its site. (Rock Decl. Ex. H.) 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. (Id. Ex. I.) 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. (Maynor Decl.=B6 12.) BE elected to continue crawling eBay's site by using proxy servers to evade eBay's IP blocks. (Mundy Depo. at 271:18-19 ("We eventually adopted the rotating proxy servers."))

Approximately 69% of the auction items contained in the BE database are from auctions hosted on eBay. (Carney Decl. =B6 17.) BE estimates that it would lose one-third of its users if it ceased to cover the eBay auctions. (Id.)

The parties agree that BE accessed the eBay site approximate 100,000 times a day. (Felton Decl. =B6 33.) eBay alleges that BE activity constituted up to 1.53% of the number of requests received by eBay, and up to 1.10% of the total data transferred by eBay during certain periods in October and November of 1999. (Johnson-Laird Decl. =B6 64.) BE alleges that BE activity constituted no more than 1.11% of the requests received by eBay, and no more than 0.70% of the data transferred by eBay. (Felton Decl. =B6 60.) eBay alleges that BE activity had fallen 27%, to 0.74% of requests and 0.61% of data, by February 20, 2000. (Johnson-Laird Decl. =B6=B6 70-71.) eBay alleges damages due to BE's activity totaling between \$45,323 and \$61,804 for a ten month period including seven months in 1999 and the first three months in 2000. (Meyer Decl. =B6 28.) However, these calculations appear flawed in that they assume the maximal BE usage of eBay resources continued over all ten months. (Id.) Moreover, the calculations attribute a pro rata share of eBay expenditures to BE activity, rather than attempting to calculate the incremental cost to eBay due to BE activity. (Id.) eBay has not alleged any specific incremental damages due to BE activity. (See Rock Depo., 192:8-10.)⁴

It appears that major Internet search engines, such as Yahoo!, Google, Excite and AltaVista, respect the Robot Exclusion Standard. (Johnson-Laird Decl. =B6=B6 81-85.)⁵

eBay now moves for preliminary injunctive relief preventing BE from accessing the eBay computer system based on nine causes of action: trespass, false advertising, federal and state trademark dilution, computer fraud and abuse, unfair competition, misappropriation, interference with prospective economic advantage and unjust enrichment. However, eBay does not move, either independently or alternatively, for injunctive relief that is limited to restricting how BE can use data taken from the eBay site.⁶

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). The alternatives in the above standard represent "extremes of a single continuum," rather than two separate tests. *Benda v. Grand Lodge of Int'l Ass'n of Machinists & Aerospace Workers*, 584 F.2d 308, 315 (9th Cir. 1978). "The critical element in determining the test to be applied is the relative hardship to the parties. If the balance of harm tips decidedly toward the plaintiff, then the plaintiff need not show as robust a likelihood of success on the merits as when the balance tips less decidedly." *Alaska v. Native Village of Venetie*, 856 F.2d 1384, 1389 (9th Cir. 1988). A "serious question" is one on which the movant has a "fair chance of success on the merits." *Sierra On-Line, Inc. v. Phoenix Software, Inc.*, 739 F.2d 1415, 1421 (9th Cir. 1984). Generally, the "balance of harm" evaluation should precede the "likelihood of success analysis" because until the balance of harm has been evaluated the court cannot know how strong and substantial the plaintiff's showing of the likelihood of success must be. See *Village of Venetie*, 856 F.2d at 1389.

III. ANALYSIS

A. Balance of Harm

eBay asserts that it will suffer four types of irreparable harm if preliminary injunctive relief is not granted: (1) lost capacity of its computer systems resulting from to BE's use of automated agents; (2) damage to eBay's reputation and goodwill caused by BE's misleading postings; (3) dilution of the eBay mark; and (4) BE's unjust

enrichment.⁷ (Mot. at 23:18-25.) The harm eBay alleges it will suffer can be divided into two categories. The first type of harm is harm that eBay alleges it will suffer as a result of BE's automated query programs burdening eBay's computer system ("system harm"). The second type of harm is harm that eBay alleges it will suffer as a result of BE's misrepresentations regarding the information that BE obtains through the use of these automated query programs ("reputational harm").

As noted above, eBay does not seek an injunction that is tailored to independently address the manner in which BE uses the information it obtains from eBay.⁸ Even without accessing eBay's computer systems by robot, BE could inflict reputational harm by misrepresenting the contents of eBay's auction database or by misusing eBay's trademark. Moreover, allowing frequent and complete recursive searching of eBay's database (which would presumably exacerbate the system harm), requiring appropriate disclaimers regarding the accuracy of BE's listings, or limiting BE's use of the eBay mark would all reduce or eliminate the possibility of reputational harm, without requiring the drastic remedy of enjoining BE from accessing eBay's database.⁹ Since eBay does not move independently or alternatively for injunctive relief tailored toward the alleged reputational harm, the court does not include the alleged reputational harm in the balance of harm analysis, nor does the court address the merits of the causes of action based on the alleged reputational harm in the likelihood of success analysis.

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.¹⁰ 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:

Where the conduct complained of does not amount to a substantial interference with possession or the right thereto, but consists of intermeddling with or use of or damages to the personal property, the owner has a cause of action for trespass or case, and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use.

Zaslow v. Kroenert, 29 Cal. 2d 541, 551 (1946). Moreover, even if BE is inflicting incremental maintenance costs on eBay, potentially calculable monetary damages are not generally a proper foundation for a preliminary injunction. See e.g., Sampson v. Murray, 415 U.S. 61, 90 (1974). Nor does eBay appear to have made the required showing that this is the type of extraordinary case in which monetary damages may support equitable relief. See *In re Estate of Ferdinand Marcos, Human Rights Litigation*, 25 F.3d 1467, 1480 (9th Cir. 1994) ("a district court has authority to issue a preliminary injunction where the plaintiffs can establish that money damages will be an inadequate remedy due to impending insolvency of the defendant or that defendant has engaged in a pattern of secreting or dissipating assets to avoid judgment.").

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"¹¹ 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. See e.g., *State v. Carriker*, 214 N.E.2d 809, 811-12 (Ohio App. 1964) (interpreting Ohio criminal trespass law to cover a business invitee who, with no intention of making a purchase, uses the business premises of another for his own gain after his invitation has been revoked); *General Petroleum Corp. v. Beilby*, 213 Cal. 601, 605 (1931). 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. (See Spafford Decl. =B6 32;12 Parker Decl. =B6 19;13 Johnson-Laird Decl. =B6 85.14) 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. See, e.g., *People of State of California ex rel. Van De Kamp v. Tahoe Reg'l Planning Agency*, 766 F.2d 1316, 1319 (9th Cir. 1985). 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.¹⁵

In the patent infringement context, the Federal Circuit has held that a preliminary injunction may be based, at least in part, on the harm that would occur if a preliminary injunction were denied and infringers were thereby encouraged to infringe a patent during the course of the litigation. See *Atlas Powder Co. v. Ireco Chems*, 773 F.2d 1230, 1233 (Fed. Cir. 1985). In the absence of preliminary injunctive relief, "infringers could become compulsory licensees for as long as the litigation lasts." *Id.* The Federal Circuit's reasoning is persuasive. "The very nature of the patent right is the right to exclude others. . . . We hold that where validity and continuing infringement have been clearly established, as in this case, immediate irreparable harm is presumed. To hold otherwise would be contrary to the public policy underlying the patent laws." *Smith Intern., Inc. v. Hughes Tool Co.*, 718 F.2d 1573, 1581 (Fed. Cir. 1983) (footnotes omitted). Similarly fundamental to the concept of ownership of personal property is the right to exclude others. See *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979) (characterizing "the right to exclude others" as "one of the most essential sticks in the bundle of rights that are commonly characterized as property"). If preliminary injunctive relief against an ongoing trespass to chattels were unavailable, a trespasser could take a compulsory license to use another's personal property for as long as the trespasser could perpetuate the litigation.

BE correctly observes that there is a dearth of authority supporting a preliminary injunction based on an ongoing 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. See *Allred v. Harris*, 14 Cal. App. 4th 1386, 1390 (1993) (citing 5 B.E. Witkin, *Summary of California Law, Torts* =A7 605 (9th ed. 1988)). 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.¹⁶ 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.

BE argues that even if eBay is entitled to a presumption of irreparable harm, the presumption may be rebutted. The presumption may be rebutted by evidence that a party has engaged in a pattern of granting licenses to engage in the complained of activity such that it may be reasonable to expect that invasion of the right can be recompensed with a royalty rather than with an injunction, or by evidence that a party has unduly delayed in bringing suit, thereby negating the idea of irreparability. See *Polymer Technologies, Inc. v. Bridwell*, 103 F.3d 970, 974 (Fed. Cir. 1996) (discussing presumption of irreparable harm in patent infringement context). BE alleges that eBay has both engaged in a pattern of licensing aggregators to crawl its site as well as delayed in seeking relief. For the reasons set forth below, the court finds that neither eBay's limited licensing activities nor its delay in seeking injunctive relief while it attempted to resolve the matter without judicial intervention are sufficient to rebut the possibility of irreparable harm.

If eBay's irreparable harm claim were premised solely on the potential harm caused by BE's current crawling activities, evidence that eBay had licensed others to crawl the eBay site would suggest that BE's activity would not result in irreparable harm to eBay. However, the gravamen of the alleged irreparable harm is that if eBay is allowed to continue to crawl the eBay site, it may encourage frequent and unregulated crawling to the point that eBay's system will be irreparably harmed. There is no evidence that eBay has indiscriminately licensed all comers. Rather, it appears that eBay has carefully chosen to permit crawling by a limited number of aggregation sites that agree to abide by the terms of eBay's licensing agreement. "The existence of such a [limited] license, unlike a general license offered to all comers, does not demonstrate a decision to relinquish all control over the distribution of the product in exchange for a readily computable fee." *Ty, Inc. v. GMA Accessories, Inc.*, 132 F.3d 1167, 1173 (7th Cir. 1997) (discussing presumption of irreparable harm in copyright infringement context). eBay's licensing activities appear directed toward limiting the amount and nature of crawling activity on the eBay site. Such licensing does not support the inference that carte blanche crawling of the eBay site would pose no threat of irreparable harm.

eBay first learned of BE in late 1997 or early 1998 when BE sought to retain the same public relations firm used by eBay. (See Ploen Decl. Ex. 1.) This motion was filed on January 18, 2000. An unexplained delay of two years would certainly raise serious doubts as the irreparability of any alleged harm. See *Playboy Enters., Inc. v. Netscape Communications Corp.*, 55 F. Supp. 2d 1070, 1090 (C.D. Cal. 1999) (noting that delay of as little as 60 days to three months has been held sufficient to rebut the presumption of irreparable harm). Here, the circumstances establish that any delay resulted from eBay's good faith efforts to resolve this dispute without judicial intervention and do not rebut a finding of the possibility of irreparable harm.

In April 1999, eBay agreed to allow BE to crawl the eBay site for 90 days while the parties negotiated a license. In late August or early September 1999, after the parties had failed to negotiate a license, eBay requested that BE stop crawling the eBay site, and BE complied. It was not until November 2, 1999, that BE issued a press release indicating that it had resumed including eBay auction listings on its site. In response, on November 9, 1999, eBay sent BE a letter again informing BE that its activities were unauthorized and again offering to license BE's activities.¹⁷ After eBay and BE were again unable to agree on licensing terms, eBay attempted to block BE from accessing the eBay site. By the end of November 1999, despite blocking more than 150 IP addresses, it became apparent that eBay was unable to prevent BE's crawling of the eBay system via rotating

proxy servers. Having failed in its attempt at self-help, eBay filed this suit on December 10, 1999, and filed this motion five weeks later. The fact that eBay's primary concern is the threat from the likely increase in crawling activity that would result if BE is allowed to continue its unauthorized conduct, combined with eBay's repeated attempts to resolve this dispute without judicial intervention, and BE's continuing attempts to thwart eBay's protection of its property, convinces the court that eBay's delay in seeking preliminary relief was justified.

BE argues that even if eBay will be irreparably harmed if a preliminary injunction is not granted, BE will suffer greater irreparable harm if an injunction is granted. According to BE, lack of access to eBay's database will result in a two-thirds decrease in the items listed on BE, and a one-eighth reduction in the value of BE, from \$80 million to \$70 million. (Sweeny Decl. =B6=B6 42, 43.) Although the potential harm to BE does not appear insignificant, BE does not appear to have suffered any irreparable harm during the period it voluntarily ceased crawling the eBay site. Barring BE from automatically querying eBay's site does not prevent BE from maintaining an aggregation site including information from eBay's site. Any potential economic harm is appropriately addressed through the posting of an adequate bond.

Moreover, it appears that any harm alleged to result from being forced to cease an ongoing trespass may not be legally cognizable. In the copyright infringement context, once a plaintiff has established a strong likelihood of success on the merits, any harm to the defendant that results from the defendant being preliminarily enjoined from continuing to infringe is legally irrelevant. See *Triad Sys. Corp. v. Southeastern Exp. Co.*, 64 F.3d 1330, 1338 (9th Cir. 1995) (defendant "cannot complain of the harm that will befall it when properly forced to desist from its infringing activities."). The Ninth Circuit has held it to be reversible error for a district court to even consider "the fact that an injunction would be devastating to [defendant's] business" once the plaintiff has made a strong showing of likely success on the merits of a copyright infringement claim. *Cadence Design Sys., Inc. v. Avant! Corp.*, 125 F.3d 824, 830 (9th Cir. 1997). The reasoning in these cases appears to be that a defendant who builds a business model based upon a clear violation of the property rights of the plaintiff cannot defeat a preliminary injunction by claiming the business will be harmed if the defendant is forced to respect those property rights. See *Concrete Mach. Co., Inc. v. Classic Lawn Ornaments, Inc.*, 843 F.2d 600, 613 (1st Cir. 1988) ("If a strong likelihood of success is demonstrated, then the court should issue the injunction even if the defendant will incur the relatively greater burden; a probable infringer simply should not be allowed to continue to profit from its continuing illegality at the copyright owner's expense."). The Federal Circuit has crafted a similar rule with respect to patent infringement. See *Windsurfing Int'l Inc. v. AMF, Inc.*, 782 F.2d 995, 1003 n.12 (Fed. Cir. 1986) ("One who elects to build a business on a product found to infringe cannot be heard to complain if an injunction against continuing infringement destroys the business so elected."). Accordingly, the court concludes that eBay has demonstrated at least a possibility of suffering irreparable system harm and that BE has not established a balance of hardships weighing in its favor.

B. Likelihood of Success

As noted above, eBay moves for a preliminary injunction on all nine of its causes of action. These nine causes of action correspond to eight legal theories: (1) trespass to chattels, (2) false advertising under the Lanham Act, 15 U.S.C. =A7 1125(a), (3) federal and state trademark dilution, (4) violation of the Computer Fraud and Abuse Act, 18 U.S.C. =A7 1030, (5) unfair competition, (6) misappropriation, (7) interference with prospective economic advantage and (8) unjust enrichment. The court finds that eBay has established a sufficient likelihood of prevailing on the trespass claim to support the requested injunctive relief. Since the court finds eBay is entitled to the relief requested based on its trespass claim, the court does not address the merits of the remaining claims or BE's arguments that many of these other state law causes of action are preempted by federal copyright

law. The court first addresses the merits of the trespass claim, then BE's arguments regarding copyright preemption of the trespass claim, and finally the public interest.

1. Trespass

Trespass to chattels "lies where an intentional interference with the possession of personal property has proximately cause injury." *Thrifty-Tel v. Beznik*, 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; see also *Itano v. Colonial Yacht Anchorage*, 267 Cal. App. 2d 84, 90 (1968) ("When conduct complained of consists of intermeddling with personal property 'the owner has a cause of action for trespass or case, and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use.'") (quoting *Zaslow v. Kroenert*, 29 Cal. 2d 541, 550 (1946)). 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. "In general, California does recognize a trespass claim where the defendant exceeds the scope of the consent." *Baugh v. CBS, Inc.*, 828 F.Supp. 745, 756 (N.D. Cal. 1993).

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. See *City of Amsterdam v. Daniel Goldreyer, Ltd.*, 882 F. Supp. 1273, 1281 (E.D.N.Y. 1995) ("One who uses a chattel with the consent of another is subject to liability in trespass for any harm to the chattel which is caused by or occurs in the course of any use exceeding the consent, even though such use is not a conversion."). 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. See *Civic Western Corp. v. Zila Industries, Inc.*, 66 Cal. App. 3d 1, 17 (1977) ("It seems clear, however, that a trespass may occur if the

party, entering pursuant to a limited consent, . . . proceeds to exceed those limits . . .") (discussing trespass to real property).

eBay argues that BE interfered with eBay's possessory interest in its computer system. Although eBay appears unlikely to be able to show a substantial interference at this time, such a showing is not required. Conduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel. See *Thrifty-Tel*, 46 Cal. App. 4th at 1567 (distinguishing the tort from conversion). Although the court admits some uncertainty as to the precise level of possessory interference required to constitute an intermeddling, there does not appear to be any dispute that eBay can show that BE's conduct amounts to use of eBay's computer systems. Accordingly, eBay has made a strong showing that it is likely to prevail on the merits of its assertion that BE's use of eBay's computer system was an unauthorized and intentional interference with eBay's possessory interest.

b. Damage to eBay's Computer System

A trespasser is liable when the trespass diminishes the condition, quality or value of personal property. See *Compuserve, Inc. v. Cyber Promotions*, 962 F. Supp. 1015 (S.D. Ohio 1997). 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 =A7 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. (Ritchey Decl. Ex. 3 at 391:11-12.) 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,¹⁸ 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. See *CompuServe*, 962 F.Supp. at 1022 ("any value [plaintiff] realizes from its computer equipment is wholly derived from the extent to which that equipment can serve its subscriber base.").

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.

2. Copyright Preemption

BE argues that the trespass claim, along with eBay's other state law causes of action, "is similar to eBay's originally filed but now dismissed copyright infringement claim, and each is based on eBay's assertion that Bidder's Edge copies eBay's auction listings, a right within federal copyright law." Opp'n at 8:10-12. BE is factually incorrect to the extent it argues that the trespass claim arises out of what BE does with the information it gathers by accessing eBay's computer system, rather than the mere fact that BE accesses and uses that system without authorization.

A state law cause of action is preempted by the Copyright Act if, (1) the rights asserted under state law are "equivalent" to those protected by the Copyright Act, and (2) the work involved falls within the "subject matter" of the Copyright Act as set forth in 17 U.S.C. §§ 102 and 103. *Kodadek v. MTV Networks, Inc.*, 152 F.3d 1209, 1212 (9th Cir. 1998). "In order not to be equivalent, the right under state law must have an extra element that changes the nature of the action so that it is qualitatively different from a copyright infringement claim." *Xerox Corp. v. Apple Computer, Inc.*, 734 F. Supp. 1542, 1550 (N.D. Cal. 1990). Here, eBay asserts a right not to have BE use its computer systems without authorization. The right to exclude others from using physical personal property is not equivalent to any rights protected by copyright and therefore constitutes an extra element that makes trespass qualitatively different from a copyright infringement claim. But see, *Ticketmaster Corp. v. Tickets.com, Inc.*, No. CV-99-7654 (C.D. Cal. minute order filed Mar. 27, 2000) (dismissing trespass claim based on unauthorized Internet information aggregation as preempted by copyright law).

3. Public Interest

The traditional equitable criteria for determining whether an injunction should issue include whether the public interest favors granting the injunction. *American Motorcyclist Ass'n v. Watt*, 714 F.2d 962, 965 (9th Cir. 1983). The parties submit a variety of declarations asserting that the Internet will cease to function if, according to eBay, personal and intellectual property rights are not respected, or, according to BE, if information published on the Internet cannot be universally accessed and used. Although the court suspects that the Internet will not only survive, but continue to grow and develop regardless of the outcome of this litigation, the court also recognizes that it is poorly suited to determine what balance between encouraging the exchange of information,

and preserving economic incentives to create, will maximize the public good. Particularly on the limited record available at the preliminary injunction stage, the court is unable to determine whether the general public interest factors in favor of or against a preliminary injunction.

BE makes the more specific allegation that granting a preliminary injunction in favor of eBay will harm the public interest because eBay is alleged to have engaged in anticompetitive behavior in violation of federal antitrust law. The Ninth Circuit has noted that in evaluating whether to issue a preliminary injunction, the district court is under no obligation to consider the merits of any antitrust counterclaims once the plaintiff has demonstrated a likelihood of success on the merits. See *Triad Sys. Corp. v. Southeastern Exp. Co.*, 64 F.3d 1330, 1336 n.13 (9th Cir. 1995) (discussing claim of copyright infringement). Although anticompetitive behavior may be appropriately considered in the context of a preliminary injunction based on trademark infringement, where misuse is an affirmative defense, see *Helene Curtis Indus. v. Church & Dwight Co.*, 560 F.2d 1325 (7th Cir. 1977), it does not appear to be appropriately considered here, because there is no equivalent affirmative defense to trespass to chattels. Accordingly, the court concludes the public interest does not weigh against granting a preliminary injunction.

IV. ORDER

Bidder's Edge, its officers, agents, servants, employees, attorneys and those in active concert or participation with them who receive actual notice of this order by personal service or otherwise, are hereby enjoined pending the trial of this matter, from using any automated query program, robot, web crawler or other similar device, without written authorization, to access eBay's computer systems or networks, for the purpose of copying any part of eBay's auction database. As a condition of the preliminary injunction, eBay is ordered to post a bond in the amount of \$2,000,000 to secure payment of any damages sustained by defendant if it is later found to have been wrongfully enjoined. This order shall take effect 10 days from the date on which it is filed.

Nothing in this order precludes BE from utilizing information obtained from eBay's site other than by automated query program, robot, web crawler or similar device. The court denies eBay's request for a preliminary injunction barring access to its site based upon BE's alleged trademark infringement, trademark dilution and other claims. This denial is without prejudice to an application for an injunction limiting or conditioning the use of any information obtained on the theory that BE's use violates some protected right of eBay.

FOOTNOTES

1 On April 21, 2000, defendant Bidder's Edge, Inc. filed an ex parte motion for leave to file a supplemental declaration in order to respond to factual assertions in the reply. Although the court suspects that with reasonable diligence BE could have prepared the declaration at least by the hearing date, the declaration consists merely of the results of four searches performed on major Internet search engines. eBay's opposition did not cite any prejudice that would result from its filing. Accordingly, BE's motion is granted.

2 Programs that recursively query other computers over the Internet in order to obtain a significant amount of information are referred to in the pleadings by various names, including software robots, robots, spiders and web crawlers.

3 It is unclear who Peter Leeds is, except that his email address at the time was <peter@biddersedge.com>.

4 Q: Are you aware of any complaints from eBay users about slowdowns that were caused by aggregators?

A: No.

5 BE appears to argue that this cannot be the case because searches performed on each of these search engines will return results that include eBay web pages. (Supp. Ploen Decl. =B6=B6 1-9.) However, this does not establish that these sites do not respect robot exclusion headers. There are numerous ways in which search engines can obtain information in compliance with exclusion headers, including; obtaining consent, abiding by the robot.txt file guidelines, or manually searching the sites. BE did not present any evidence of any site ever complaining about the activities of any of these search engines.

6 The bulk of eBay's moving papers and declarations address the alleged misuse of the eBay mark and the information BE obtains from the eBay computers. The court does not address the facts specific to these claims, nor the merits of these claims. Even if eBay were able to establish a likelihood of success on the merits as to these causes of action, such a showing would only support injunctive relief addressing BE's use of the eBay mark and BE's use of the eBay auction listings (the appropriate relief for which would appear to be a disclaimer regarding the lack of affiliation between eBay and BE and explicitly alerting customers to the limited scope of BE's information). Such a showing would not be sufficient to enjoin BE from accessing eBay's computer systems, which is the only relief eBay appears to request.

7 eBay does not appear to offer any support for the proposition that unjust enrichment is an independent cause of action, let alone an independently adequate basis for preliminary injunctive relief.

8 Although, as a practical matter, enjoining BE from accessing eBay's computers or searching eBay's auction database may result in BE's inability to make effective use of information from eBay's auction site.

9 Thus, eBay's motion appears to be, in part, a tactical effort to increase the strength of its license negotiating position and not just a genuine effort to prevent irreparable harm.

10 This case was filed on December 10, 1999. BE decommissioned a number of its servers in mid-December 1999. (See Mundy Depo. at 75:12-14.) Reformatting the hard drives resulted in the destruction of the server logs that may have indicated the actual duration of access to eBay's system. (See id. at 74:17-24.) eBay argues this should support an adverse inference against BE because eBay is unable to correlate BE's access to eBay's system with service disruptions. BE responds that these actions were a result of hardware failures unrelated to the litigation. The court agrees that these actions may support an inference that the information BE destroyed was prejudicial. However, final resolution of the fact-dependent questions regarding the circumstances under which this information was destroyed requires a more complete record. Accordingly, eBay is not entitled to a conclusive presumption of harm at this juncture in the proceedings, and eBay's motion to strike all evidence submitted by BE relating to a lack of harm is denied.

11 The phrase "brick and mortar" is often used to designate a traditional business when contrasting it with a predominantly, or entirely, on-line business. The phrase appears to refer to the historical reliance on conducting

commerce within the context of a physical space made from materials such as brick and mortar, as opposed to the modern trend toward conducting commerce in a cyberspace made from computers programs.

12 "If 30 or 40 companies spring into existence using similar business models, what will be the total load and impact on eBay's servers?"

13 "One crawler may currently use 1% of eBay's resources. What if hundred of users used similar crawlers?"

14 "Given that Bidder's Edge can be seen to have imposed a load of 1.53 % on eBay's listing servers, simple arithmetic and economics reveal how only a few more such companies deploying rude robots [that do not respect the Robot Exclusion Standard] would be required before eBay would be brought to its knees by what would be then a debilitating load."

15 As discussed below, eBay has a established a strong likelihood of success on the merits of the trespass claim, and is therefore entitled to preliminary injunctive relief because it has established the possibility of irreparable harm. Accordingly, the court does not reach the issue of whether the threat of increased activity would be sufficient to support preliminary injunctive relief where the plaintiff has not made as strong of a showing of likelihood of success on the merits.

16 As other courts have noted, applying traditional legal principles to the Internet can be troublesome. See *ImOn, Inc. v. ImaginOn, Inc.*, =97 F. Supp. 2d =97, =97, 2000 WL 310373, at *1 (S.D.N.Y. Mar. 27, 2000) ("Both parties are suppliers of 'services or products' on the Internet which, as I recognize and grapple with hereafter, is one of the most fluid, rapidly developing, and virtually daily changing areas of commerce that the law has had to focus upon and endeavor to apply established principles to.")

17 Because BE was expressly notified that its conduct was unauthorized, it does not matter whether BE ever agreed to a version of the eBay User Agreement that prohibited robotic activity.

18 Plaintiff believes that it may have experienced system failures and a decrease in system performance during the times that defendant was searching its system, however, it is unable to produce any correlation between its outages and defendant's activities. Plaintiff contends that it would likely be able to produce such a correlation but for defendant's alleged destruction of logs that recorded the details of its robotic search activities.

18 USCA § 1030
18 U.S.C.A. § 1030

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 47--FRAUD AND FALSE STATEMENTS

Current through P.L. 107-11, approved 5-28-01

§ 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act ([15 U.S.C. 1681](#) et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and [\[FN1\]](#)

18 USCA § 1030
18 U.S.C.A. § 1030

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000; [\[FN2\]](#)

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and [\[FN3\]](#)

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means 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;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

- (B) which is used in interstate or foreign commerce or communication;
- (3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
- (4) the term "financial institution" means--
- (A) an institution with deposits insured by the Federal Deposit Insurance Corporation;
- (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
- (C) a credit union with accounts insured by the National Credit Union Administration;
- (D) a member of the Federal home loan bank system and any home loan bank;
- (E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
- (F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
- (G) the Securities Investor Protection Corporation;
- (H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
- (I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.
[\[FN4\]](#)
- (5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
- (6) the 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;
- (7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5; and
[\[FN5\]](#)
- (8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that--
- (A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more
- Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety; and

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

CREDIT(S)

2000 Main Volume

(Added Pub.L. 98-473, Title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190, and amended Pub.L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub.L. 100-690, Title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub.L. 101-73, Title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub.L. 101-647, Title XII, § 1205(e), Title XXV, § 2597(j), Title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub.L. 103-322, Title XXIX, § 290001(b) to (f), Sept. 13, 1994, 108 Stat. 2097-2099; Pub.L. 104-294, Title II, § 201, Title VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508.)

[\[FN1\]](#) So in original. The word "and" should probably not appear.

[\[FN2\]](#) So in original. Probably should be followed by "and".

[\[FN3\]](#) So in original. The "; and" should probably be a period.

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

[FN4] So in original. The period probably should be a semicolon.

[FN5] So in original. The word "and" should probably not appear.

<General Materials (GM) - References, Annotations, or Tables>

HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports

1984 Acts. House Report No. 98-1030 and House Conference Report No. 98-1159, see 1984 U.S. Code Cong. and Adm. News, p. 3182.

1986 Acts. House Report No. 99-797, see 1986 U.S. Code Cong. and Adm. News, p. 6138.

1989 Acts. House Report No. 101-54(Parts I-VII) and House Conference Report No. 101-222, see 1989 Code Cong. and Adm. News, p. 86.

1990 Acts. House Report Nos. 101-681(Parts I and II) and 101-736, Senate Report No. 101-460, and Statement by President, see 1990 U.S. Code Cong. and Adm. News, p. 6472.

1994 Acts. House Report Nos. 103-324 and 103-489, and House Conference Report No. 103-711, see 1994 U.S. Code Cong. and Adm. News, p. 1801.

1996 Acts. House Report No. 104-788, see 1996 U.S. Code Cong. and Adm. News, p. 4021.

References in Text

Reference to "paragraph y of section 11 of the Atomic Energy Act of 1954", referred to in subsec. (a)(1) is classified to section 2014(y) of Title 42, Public Health and Welfare.

The Fair Credit Reporting Act, referred to in subsec. (a)(2)(A), is Title VI of Pub.L. 90-321 as added by Pub.L. 91-508, Title VI, Oct. 26, 1970, 84 Stat. 1127, which is classified to subchapter III (section 1681 et seq.) of chapter 41 of Title 15, Commerce and Trade.

The Farm Credit Act of 1971, referred to in subsec. (e)(4)(E), is Pub.L. 92-181, Dec. 10, 1971, 85 Stat. 585, as amended, which is classified generally to chapter 23 (section 2001 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 2001 of Title 12 and Tables.

Section 15 of the Securities Exchange Act of 1934, referred to in subsec. (e)(4)(F), is classified to section 78o of Title 15, Commerce and Trade.

Section 1(b) of the International Banking Act of 1978, referred to in subsec. (e)(4)(H), is

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

classified to section 3101 of Title 12, Banks and Banking.

Section 25 of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter I (section 601 et seq.) of chapter 6 of Title 12.

Section 25(a) of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter II (section 611 et seq.) of chapter 6 of Title 12.

The date of the enactment of this subsection, referred to in subsec. (h), means the date of the enactment of [Pub.L. 103-322](#), 108 Stat. 1796, which enacted subsec. (h) and was approved Sept. 13, 1994.

Amendments

1996 Amendments. Subsec. (a)(1). [Pub.L. 104-294, § 201\(1\)\(A\)](#), amended par. (1) generally. Prior to amendment, par. (1) read as follows: "(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;"

Subsec. (a)(2)(A) to (C). [Pub.L. 104-294, § 201\(1\)\(B\)](#), added subpars. (B) and (C), and designated existing provisions relating to obtaining information contained in financial institution records, or of a card issuer, or contained in a file of a consumer reporting agency on a consumer, as subpar. (A).

Subsec. (a)(3). [Pub.L. 104-294, § 201\(1\)\(C\)](#), substituted "any nonpublic computer of a department or agency" for "any computer of a department or agency" and "such conduct affects that use by or for the Government of the United States" for "such conduct adversely affects the use of the Government's operation of such computer".

Subsec. (a)(4). [Pub.L. 104-294, § 201\(1\)\(D\)](#), substituted "accesses a protected computer" for "accesses a Federal interest computer" and inserted, before the semicolon, "and the value of such use is not more than \$5,000 in any 1-year period".

Subsec. (a)(5). [Pub.L. 104-294, § 201\(1\)\(E\)](#), amended par. (5) generally, substituting provisions relating to one who knowingly causes the transmission of a program, information, code, or command, and intentionally causes damage without authorization to a protected computer, or intentionally accesses a protected computer without authorization and recklessly or otherwise causes damage, for provisions relating to one who through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to such computer or systems with the intent to cause damage to or deny usage of such computer or systems, or knowingly and with reckless disregard of a

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

substantial an unjustifiable risk that such transmission will cause damage to or deny usage of such computer or systems, and does cause such damage or denial of usage and such transmission occurs without authorization and causes loss of more than \$1,000 to, or impairs medical care of, one or more individuals.

Subsec. (a)(5)(B)(ii)(II)(bb). [Pub.L. 104-294, § 604\(b\)\(36\)\(A\)](#), inserted "or" at the end thereof.

Subsec. (a)(7). [Pub.L. 104-294, § 201\(1\)\(G\)](#), added par. (7).

Subsec. (c)(1). [Pub.L. 104-294, § 201\(2\)\(A\)](#), substituted "this section" for "such subsection" wherever appearing.

Subsec. (c)(1)(B). [Pub.L. 104-294, § 604\(b\)\(36\)\(B\)](#), struck out "and" which followed the semicolon at the end thereof.

Subsec. (c)(2)(A). [Pub.L. 104-294, § 201\(2\)\(B\)\(i\)](#), inserted ", (a)(5)(C)," following "(a)(3)" and substituted "this section" for "such subsection".

Subsec. (c)(2)(B). [Pub.L. 104-294, § 201\(2\)\(B\)\(iii\)](#), added subpar. (B). Former subpar. (B) redesignated (C).

Subsec. (c)(2)(C). [Pub.L. 104-294, § 201\(2\)\(B\)\(ii\), \(iv\)](#), redesignated former subpar. (B) as (C), substituted "this section" for "such subsection", and inserted "and" at the end thereof.

Subsec. (c)(3)(A). [Pub.L. 104-294, § 201\(2\)\(C\)\(i\)](#), substituted "(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)" for "(a)(4) or (a)(5)(A)" and "this section" for "such subsection".

Subsec. (c)(3)(B). [Pub.L. 104-294, § 201\(2\)\(C\)\(ii\)](#), substituted "(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)" for "(a)(4) or (a)(5)(A)" and "this section" for "such subsection".

Subsec. (c)(4). [Pub.L. 104-294, § 201\(2\)\(D\)](#), struck out par. (4) which read as follows: "(4) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B)."

Subsec. (d). [Pub.L. 104-294, § 201\(3\)](#), inserted "subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of" preceding "this section".

Subsec. (e)(2). [Pub.L. 104-294, § 201\(4\)\(A\)\(i\)](#), substituted "protected computer" for "Federal interest computer".

Subsec. (e)(2)(A). [Pub.L. 104-294, § 201\(4\)\(B\)\(ii\)](#), substituted "that use by or for the financial institution or the Government" for "the use of the financial institution's operation or the Government's operation of such computer".

Subsec. (e)(2)(B). [Pub.L. 104-294, § 201\(4\)\(A\)\(iii\)](#), amended subpar. (b) generally. Prior to

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

amendment subpar. (B) read as follows: "(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;"

Subsec. (e)(8), (9). [Pub.L. 104-294, § 201\(4\)\(B\) to \(D\)](#), added pars. (8) and (9).

Subsec. (g). [Pub.L. 104-294, § 604\(b\)\(36\)\(C\)](#), substituted "this section" for "the section".

[Pub.L. 104-294, § 201\(5\)](#), deleted ", other than a violation of subsection (a)(5)(B)," which followed "by reason of a violation of the section" and substituted "involving damage as defined in subsection (e)(8)(A)" for "of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)".

Subsec. (h). [Pub.L. 104-294, § 604\(b\)\(36\)\(D\)](#), substituted "subsection (a)(5)" for " [section 1030\(a\)\(5\) of title 18, United States Code](#)".

1994 Amendments. Subsec. (a)(3). [Pub.L. 103-322, § 290001\(f\)](#), substituted "adversely affects" for "affects".

Subsec. (a)(5). [Pub.L. 103-322, § 290001\(b\)](#), completely revised par. (5). Prior to revision par. (5) related only to a person who "intentionally accesses a Federal interest computer without authorization, and by means of one or more of such conduct alters, damages, or destroys any information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby causes loss to one or more others of a value aggregating \$1,000 or more during any one year period, or modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals".

Subsec. (c)(3)(A). [Pub.L. 103-322, § 290001\(c\)\(2\)](#), substituted "(a)(5)(A) of this section" for "(a)(5) of this section".

Subsec. (c)(4). [Pub.L. 103-322, § 290001\(c\)\(1\), \(3\), \(4\)](#), added par. (4).

Subsec. (g). [Pub.L. 103-322, § 290001\(d\)](#), added subsec. (g).

Subsec. (h). [Pub.L. 103-322, § 290001\(e\)](#), added subsec. (h).

1990 Amendments. Subsec. (a)(1). [Pub.L. 101-647, § 3533](#), substituted "paragraph y of section 11" for "paragraph r of section 11".

Subsec. (e)(3). [Pub.L. 101-647](#) inserted "commonwealth," before "possession or territory of the United States".

Subsec. (e)(4)(H), (I). [Pub.L. 101-647, § 2597\(j\)](#), added subpars. (H) and (I).

1989 Amendments. Subsec. (e)(4)(A). [Pub.L. 101-73, § 962\(a\)\(5\)\(A\)](#), substituted "an
Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

institution" for "a bank".

Subsec. (e)(4)(C) to (H). [Pub.L. 101-73, § 962\(a\)\(5\)\(B\), \(C\)](#), redesignated former subpars. (D) to (H) as (C) to (G), respectively, and struck out former subpar. (C), which had included within the definition of the term "financial institution" institutions with accounts insured by the Federal Savings and Loan Insurance Corporation.

1988 Amendments. Subsec. (a)(2). [Pub.L. 100-690](#) inserted a comma after "financial institution" and substituted "title 15," for "title 15.,".

1986 Amendments. Subsec. (a)(1). [Pub.L. 99-474, § 2\(c\)](#), substituted "or exceeds authorized access" for "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend".

Subsec. (a)(2). [Pub.L. 99-474, § 2\(a\)\(1\)-\(4\)](#), substituted "intentionally" for "knowingly"; struck out "as such terms are defined in the Right to Financial Privacy Act of 1978 ([12 U.S.C. 3401](#) et seq.)," following "financial institution,"; struck out "or" appearing at end of par. (2); and added following "financial institution" the phrase "or of a card issuer as defined in section 1602(n) of title 15,".

[Pub.L. 99-474, § 2\(c\)](#), substituted "or exceeds authorized access" for "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend".

Subsec. (a)(3). [Pub.L. 99-474, § 2\(b\)\(1\)](#), added par. (3) and struck out former par. (3) provision which read [Whoever--] "knowingly access a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation; ", now covered in par. (5).

Subsec. (a)(3) end text. [Pub.L. 99-474, § 2\(b\)\(2\)](#), struck out following par. (3) sentence reading "It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer.", now covered in subsec. (a)(4).

Subsec. (a)(4)-(6). [Pub.L. 99-474, § 2\(d\)](#), added pars. (4) to (6).

Subsec. (b). [Pub.L. 99-474, § 2\(e\)\(1\), \(2\)](#), struck out par. (1) designation and par. (2) provision respecting specific conspiracy offense and prescribing as a fine an amount not greater than the amount provided as the maximum fine for such offense under subsec. (c) or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsec. (c), or both.

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

Subsec. (c). [Pub.L. 99-474, § 2\(f\)\(9\)](#), substituted in opening phrase subsec. "(b)" for "(b)(1)".

Subsec. (c)(1)(A). [Pub.L. 99-474, § 2\(f\)\(1\)](#), substituted "under this title" for "of not more than the greater of \$10,000 or twice the value obtained by the offense".

Subsec. (c)(1)(B). [Pub.L. 99-474, § 2\(f\)\(2\)](#), substituted "under this title" for "of not more than the greater of \$100,000 or twice the value obtained by the offense".

Subsec. (c)(2)(A). [Pub.L. 99-474, § 2\(f\)\(3\), \(4\)](#), inserted reference to subsec. (a)(6) and substituted "under this title" for "of not more than the greater of \$5,000 or twice the value obtained or loss created by the offense".

Subsec. (c)(2)(B). [Pub.L. 99-474, § 2\(f\)\(3\), \(5\)-\(7\)](#), inserted reference to subsec. (a)(6) and substituted "under this title" for "of not more than the greater of \$10,000 or twice the value obtained or loss created by the offense", "not more than" for "not than", and "; and" for the period at end of subpar. (B), respectively.

Subsec. (c)(3). [Pub.L. 99-474, § 2\(f\)\(8\)](#), added par. (3).

Subsec. (e). [Pub.L. 99-474, § 2\(g\)\(1\)](#), substituted at end of introductory phrase a one-em dash for the comma.

Subsec. (e)(1). [Pub.L. 99-474, § 2\(g\)\(2\), \(3\)](#), aligned so much of the subsec. so that it be cut in two ems and begin as an indented and designated par. (1), and substituted a semicolon for the period at end thereof.

Subsec. (e)(2)-(7). [Pub.L. 99-474, § 2\(g\)\(4\)](#), added pars. (2) to (7).

Subsec. (f). [Pub.L. 99-474, § 2\(h\)](#), added subsec. (f).

Effective and Applicability Provisions

1996 Acts. Amendment by [section 604 of Pub.L. 104-294](#) effective Sept. 13, 1994, see [section 604\(d\) of Pub.L. 104-294](#), set out as a note under section 13 of this title.

Severability of Provisions

If any provision of [Pub.L. 101-73](#) or the application thereof to any person or circumstance is held invalid, the remainder of [Pub.L. 101-73](#) and the application of the provision to other persons not similarly situated or to other circumstances not to be affected thereby, see [section 1221 of Pub.L. 101-73](#), set out as a note under section 1811 of Title 12, Banks and Banking.

Report to Congress

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

[Section 2103 of Pub.L. 98-473](#) provided that: "The Attorney General shall report to the Congress annually, during the first three years following the date of the enactment of this joint resolution [Oct. 12, 1984], concerning prosecutions under the sections of title 18 of the United States Code added by this chapter [this section]."

18 USCA § 1030
18 U.S.C.A. § 1030

CROSS REFERENCES

Optional venue for espionage and related offenses on the high seas, see [18 USCA § 3239](#).

AMERICAN LAW REPORTS

[What constitutes a public record or document within statute making falsification, forgery, mutilation, removal, or other misuse thereof an offense. 75 ALR4th 1067.](#)

LIBRARY REFERENCES

American Digest System

Copyrights and Intellectual Property  109.

Encyclopedias

Copyrights and Intellectual Property, see C.J.S. § § 104, 108.

Law Review and Journal Commentaries

Computer crime. Scott Charney & Kent Alexander, [45 Emory L.J. 931 \(1996\)](#).

Computer Fraud and Abuse Act of 1986: A measured response to a growing problem. Note, [43 Vand.L.Rev. 453 \(1990\)](#).

Computer Fraud and Abuse Act of 1986: The saga continues. John A. Potter, 10 Corp., Finance & Bus.L. Section J. 243 (1987).

Computer-related crimes. Adam G. Ciongoli, Jennifer A. DeMarrais, and James Wehner, [31 Am.Crim.L.Rev. 425 \(1994\)](#).

Embedded alert software: Weapon against piracy or computer abuse? Robert C. Scheinfeld, 216 N.Y.L.J. 1 (Aug. 13, 1996).

Hacking through the Computer Fraud and Abuse Act. [31 U.C. Davis L.Rev. 283 \(1997\)](#).

Regulating internet advertising. Richard Raysman and Peter Brown, 215 N.Y.L.J. 3 (May 14, 1996).

The 1984 Federal Computer Crime Statute: A partial answer to a pervasive problem. Joseph B. Tompkins, Jr. and Linda A. Mar, 6 Computer/L.J. 459 (1986).

What victims of computer crime should know and do. Stephen Fishbein, 210 N.Y.L.J. 1 (Nov. 12, 1993).

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

NOTES OF DECISIONS

Constitutionality [1](#)

Intent [3](#)

Loss or damage [4](#)

Thing of value [5](#)

Unauthorized access or use [2](#)

[1. Constitutionality](#)

Fact that computer fraud statute does not have mens rea requirement for damages element of offense does not render such statute unconstitutional. [U.S. v. Sablan, C.A.9 \(Guam\) 1996, 92 F.3d 865.](#)

[2. Unauthorized access or use](#)

Defendant's transmission of computer "worm" constituted accessing federal interest computer without authorization under statute punishing anyone who intentionally accesses without authorization federal interest computers and damages or prevents authorized use of information in those computers causing loss of \$1,000 or more; defendant used computer program that transfers and receives electronic mail and program that permits person to obtain limited information about users of another computer to release "worm" into group of national networks that connected university, governmental, and military computers around the country and use of those features was not in any way related to their intended function. [U.S. v. Morris, C.A.2 \(N.Y.\) 1991, 928 F.2d 504](#), certiorari denied [112 S.Ct. 72, 502 U.S. 817, 116 L.Ed.2d 46.](#)

Internet dating service was entitled to temporary restraining order (TRO) prohibiting a former programmer from "hacking" the dating service's website and diverting its clients and users to a porn site; dating service had a likelihood of success on the merits of its claim that former programmer was responsible for alleged violations of the Computer Fraud and Abuse Act, and showed irreparable harm in the damage to the goodwill of its services, while programmer and operator of porn site would suffer no legitimate harm from issuance of TRO nor would the public. [YourNetDating, Inc. v. Mitchell, N.D.Ill.2000, 88 F.Supp.2d 870.](#)

Internet site operators' maintenance of membership with Internet service provider in order to use that membership to harvest e-mail addresses of provider's customers and send bulk e-mails to those customers, in violation of provider's terms of service, violated Computer Fraud and Abuse Act, which prohibits individuals from exceeding authorized access. [America Online, Inc. v. LCGM, Inc., E.D.Va.1998, 46 F.Supp.2d 444.](#)

Agency had reasonable cause to believe that employee, who had altered computer contracts, had committed crime, so as to invoke crime provision, even though employee claimed that alterations were not to defraud government, but only to show lack of security safeguards; relevant criminal statute only required proof of use of computer system for any unauthorized purpose. [Sawyer v.](#)

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

18 USCA § 1030
18 U.S.C.A. § 1030

[Department of Air Force, M.S.P.B.1986, 31 M.S.P.R. 193.](#)

3. Intent

Computer fraud statute did not require government to prove that defendant intentionally damaged computer files, but only that defendant intentionally accessed computer without authorization. [U.S. v. Sablan, C.A.9 \(Guam\) 1996, 92 F.3d 865.](#)

4. Loss or damage

Statute which punishes anyone who intentionally accesses without authorization federal interest computers and damages or prevents authorized use of information in those computers causing loss of \$1,000 or more does not require Government to demonstrate that defendant intentionally prevented authorized use and thereby caused loss. [U.S. v. Morris, C.A.2 \(N.Y.\) 1991, 928 F.2d 504](#), certiorari denied [112 S.Ct. 72, 502 U.S. 817, 116 L.Ed.2d 46.](#)

Designer of allegedly defective microcode used in computer floppy-diskette controllers could be held liable, under Computer Fraud and Abuse Act provision prohibiting transmission of code which intentionally causes damage to protected computers, for third party's sales of computers incorporating controllers which contained defective code; designer could have reasonably anticipated such sales. [Shaw v. Toshiba America Information Systems, Inc., E.D.Tex.1999, 91 F.Supp.2d 926.](#)

Statute making it an offense to cause damage to a protected computer, by knowingly causing the transmission of a program, information, code, or command, resulting in a specified loss to one or more "individuals," encompasses damage sustained by a business entity as well as by a natural person. [U.S. v. Middleton, N.D.Cal.1999, 35 F.Supp.2d 1189.](#)

5. Thing of value

Defendant could not be convicted of computer fraud in connection with his browsing of confidential taxpayer files, even though he exceeded authorized access to a federal interest computer, as he did not obtain "anything of value." [U.S. v. Czubinski, C.A.1 \(Mass.\) 1997, 106 F.3d 1069.](#)

18 U.S.C.A. § 1030

18 USCA § 1030

END OF DOCUMENT

CA PENAL § 502

West's Ann.Cal.Penal Code § 502

WEST'S ANNOTATED CALIFORNIA CODES
PENAL CODE
PART 1. OF CRIMES AND PUNISHMENTS
TITLE 13. OF CRIMES AGAINST PROPERTY
CHAPTER 5. LARCENY [THEFT]

Current through end of 1999-2000 Reg.Sess.
and 1st Ex.Sess. and Nov. 7, 2000, election.

§ 502. Unauthorized access to computers, computer systems and computer data

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

CA PENAL § 502

West's Ann.Cal.Penal Code § 502

storage and retrieval, communication, and control.

(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(11) "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system,

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

CA PENAL § 502

West's Ann.Cal.Penal Code § 502

or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

(d)(1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed four hundred dollars (\$400), by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars (\$5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars (\$400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

CA PENAL § 502

West's Ann.Cal.Penal Code § 502

(3) Any person who violates paragraph (6) or (7) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars (\$1,000).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars (\$5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars (\$5,000), by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (8) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars (\$10,000), or by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not one thousand dollars.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(e)(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

CA PENAL § 502

West's Ann.Cal.Penal Code § 502

[Section 1714.1 of the Civil Code.](#)

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of [Section 3294 of the Civil Code](#), the court may additionally award punitive or exemplary damages.

(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h)(1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or provided that the value of supplies or computer services, as defined in paragraph (4) of subdivision (b), which are used does not exceed an accumulated total of one hundred dollars (\$100).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

CA PENAL § 502

West's Ann.Cal.Penal Code § 502

paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

CREDIT(S)

1999 Main Volume

(Added by Stats.1987, c. 1499, § 3. Amended by Stats.1989, c. 1076, § 1; Stats.1989, c. 1110, § 1; Stats.1989, c. 1357, § 1.3; Stats.1998, c. 863 (A.B.1629), § 3.)

2001 Electronic Update

(Amended by Stats.1999, c. 254 (A.B.451), § 3; Stats.2000, c. 634 (A.B.2232), § 1; Stats.2000, c. 635 (A.B.2727), § 2.)

HISTORICAL AND STATUTORY NOTES

2001 Electronic Update

1999 Legislation

Stats.1999, c. 254, rewrote subd. (h), which had read:

"(h)(1) Subdivision (c) does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment.

"(2) Paragraph (3) of subdivision (c) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer program, or data when acting outside the scope of his or her lawful employment, so long as the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or so long as the value of supplies and computer services, as defined in paragraph (4) of subdivision

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

CA PENAL § 502

West's Ann.Cal.Penal Code § 502

(b), which are used do not exceed an accumulated total of one hundred dollars (\$100)."

Section 1 of Stats.1999, c. 254, provides:

"This act shall be known and may be cited as the 'Officer Don Burt Act of 1999.'"

2000 Legislation

Stats.2000, ~~§~~, in subd. (b)(8), inserted ", or the denial of access to legitimate users of a computer system, network, or program"; in subd. (d), in the introductory paragraph of par. (3), substituted "(6) or (7)" for "(6), (7), or (8)", in subpar. (A) of par. (3), changed the dollar amount from \$250 to \$1,000 and rewrote par. (4), redesignating it as pars. (4) and (5); and, in subd. (e), rewrote par. (1), in par. (2), deleted "to a prevailing party" following "fees", and added pars. (4) and (5), relating to punitive damages and the limitations period. Prior to amendment, subs. (d)(4) and (e)(1) read:

"(d)(4) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

"(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding two hundred fifty dollars (\$250).

"(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment."

"(e)(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of [Section 1714.1 of the Civil Code](#)."

Under the provisions of § 3 of Stats.2000, c. 635, the 2000 amendments of this section by c. 634 (A.B.2232) and c. 635 (A.B.2727) were given effect and incorporated in the form set forth in § 2 of c. 635.

An amendment of this section by § 1 of Stats.2000, c. 635, failed to become operative under the provisions of § 3 of that Act.

An amendment of this section by § 1.5 of Stats.2000, c. 634, failed to become operative under the provisions of § 2 of that Act.

Section affected by two or more acts at the same session of the legislature, see [Government](#)

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

CA PENAL § 502

West's Ann.Cal.Penal Code § 502

[Code § 9605.](#)

1999 Main Volume

Section 1 of Stats.1987, c. 1499, provides:

"This act shall be known and may be cited as the 'Comprehensive Computer Data Access and Fraud Act.' "

The 1989 amendment, in subd. (b), rewrote the definition of computer network and added the definition of computer contaminant; in subd. (c), substituted "(h)" for "(i)" in the introductory paragraph and added par. (8); in subd. (d)(3), substituted "(7) or (8)" for "or (7)"; inserted subd. (e)(3); deleted subd. (g) and redesignated former subs. (h) to (k) as subs. (g) to (j); rewrote subd. (g); in subd. (h)(2) inserted "supplies and" and "an accumulated total of"; in subd. (i), substituted "(h)" for "(i)"; and added subd. (k).

Amendment of this section by § § 2, 3, and 4 of Stats.1989, c. 1076, failed to become operative under the provisions of § 6 of that Act.

Amendment of this section by § § 2, 3, and 4 of Stats.1989, c. 1110, failed to become operative under the provisions of § 7 of that Act.

Under the provisions of § 7 of Stats.1989, c. 1357, the 1989 amendments of this section by c. 1076, c. 1110, and c. 1357 were given effect and incorporated in the form set forth in § 1.3 of c. 1357. An amendment of this section by § § 1, 1.1, and 1.2, of Stats.1989, c. 1357, failed to become operative under the provisions of § 7 of that Act.

Stats.1998, c. 863, § 3, added subs. (b)(11), (c)(9), and (d)(4), and made nonsubstantive changes throughout the section.

Former § 502, added by Stats.1979, c. 858, § 1, amended by Stats.1981, c. 837, § 1; Stats.1983, c. 1092, § 292; Stats.1984, c. 949, § 2; Stats.1985, c. 571, § 1, relating to the same subject matter, was repealed by Stats.1987, c. 1499, § 2.

Former § 502, added by Stats.1871-72, c. 455, p. 684, § 1, made former § § 339, 342, and 343 applicable to junk dealers. The section was reenacted as § 344 (repealed).

Derivation: Former § 502, added by Stats.1979, c. 858, § 1, amended by Stats.1981, c. 837, § 1; Stats.1983, c. 1092, § 292; Stats.1984, c. 949, § 2; Stats.1985, c. 571, § 1.

West's Ann. Cal. Penal Code § 502

CA PENAL § 502

END OF DOCUMENT

Copr. © West 2001 No Claim to Orig. U.S. Govt. Works

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

REGISTER.COM, INC.,

Plaintiff,

00 Civ. 5747 (BSJ)

v.

Order

VERIO, INC.,

Defendant.

BARBARA S. JONES

UNITED STATES DISTRICT JUDGE

Introduction

Plaintiff Register.com, a registrar of Internet domain names, moves for a preliminary injunction against the defendant, Verio, Inc. ("Verio"), a provider of Internet services. Register.com relies on claims under Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a); the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, as amended; as well as trespass to chattels and breach of contract under the common law of the State of New York. In essence Register.com seeks an injunction barring Verio from using automated software processes to access and collect the registrant contact information contained in its WHOIS database and from using any of that information, however accessed, for mass marketing purposes.

I. Findings of Fact

The Parties

Plaintiff Register.com is one of over fifty domain name registrars for customers who wish to register a name in the .com, .net, and .org top-level domains. As a registrar it contracts

with these second-level domain ("SLD") name holders and a registry, collecting registration data about the SLD holder and submitting zone file information for entry in the registry database. In addition to its domain name registration services, Register.com offers to its customers, both directly and through its more than 450 co-branded and private label partners, a variety of other related services, such as (i) web site creation tools; (ii) web site hosting; (iii) electronic mail; (iv) domain name hosting; (v) domain name forwarding, and (vi) real-time domain name management. Register.com has invested over \$15 million dollars in equipment, software, service fees, and human resources in designing, developing, and maintaining its website and the computer systems necessary to host Register.com's Internet-based services. (See Gardos Decl. ¶ 6). It has also spent in excess of \$25 million on advertising and brand promotion in the year 2000 alone, including through print, radio, and television media. (See Mornell Decl. ¶ 31).

In order to give its customers control over their receipt of commercial solicitations, Register.com provides them with the opportunity to "opt-in" during the domain name registration process to receiving sales and marketing communications from Register.com or its co-brand or private label partners. Customers who do not opt-in to such communications are not solicited by Register.com or its co-brands. Significantly,

Register.com's co-brand and private label partners have contracted with Register.com for the right to have their services featured on the www.register.com website. (See Mornell Decl. ¶ 18).

Defendant Verio is one of the largest operators of web sites for businesses and a leading provider of comprehensive Internet services. Although not a registrar of domain names, Verio directly competes with Register.com and its partners to provide registration services and a variety of other Internet services including website hosting and development. Verio recently made a multimillion dollar investment in its computer system and facilities for its expanded force of telephone sales associates in its efforts to "provide recent domain name registration customers with the services they need, at the time they need them." (Eden Decl. ¶ 31).

The WHOIS database

To become an accredited domain name registrar for the .com, .net, and .org domains, all registrars, including Register.com are required to enter into a registrar Accreditation Agreement ("Agreement") with the Internet Corporation for Assigned Names and Numbers ("ICANN").¹ Under that Agreement, Register.com, as

¹ ICANN was created in 1998 to assume the U.S. Government's responsibilities for the management of the Internet Domain Name System ("DNS"). It is a private, not-for-profit corporation initiated by the Department of Commerce to privatize the Domain Name System in a manner that increases competition and

well as all other registrars, is required to provide an on-line, interactive WHOIS database. This database contains the names and contact information -- postal address, telephone number, electronic mail address and in some cases facsimile number -- for customers who register domain names through the registrar. The Agreement also requires Register.com to make the database freely accessible to the public via its web page and through an independent access port called port 43. These query-based channels of access to the WHOIS database allow the user to collect registrant contact information for one domain name at a time by entering the domain name into the provided search engine.²

The primary purpose of the WHOIS database is to provide necessary information in the event of domain name disputes, such

facilitates international participation in its management. (See Ex. B to McPherson Decl.). Network Solutions, Inc. ("NSI") formerly enjoyed a monopoly as the only domain name registrar. NSI still operates and maintains the top-level domain name servers and zone files which enable the other registrars to access the DNS and to transmit domain name registration information for the .com, .net, and .org top level domain names to the System.

² The Agreement also obligates Register.com to provide third parties with bulk access to the same WHOIS data pursuant to a license agreement. The bulk access license entitles the licensee to receive weekly -- in one transmission -- an electronic copy of the same WHOIS information that is provided continuously through Register.com's web page and its access port 43. The Agreement allows Register.com to charge a \$10,000 yearly fee for the license. Register.com has imposed the same mass marketing prohibition on the use the bulk license data. (See Eden Depo. at 34).

as those arising from cybersquatting or trademark infringement. (See Rony Decl. ¶ 18, Ex. B to McPherson Decl. at 13). The parties also agree that the WHOIS data may be used for market research.

Specifically, section II.F.5 of Register.com's Accreditation Agreement with ICANN requires that:

In providing query-based public access to registration data as required by Sections II.F.1 and II.F.4, Registrar shall not impose terms and conditions on use of the data provided except as permitted by ICANN-adopted policy. Unless and until ICANN adopts a different policy, Registrar shall permit use of data it provides in response to queries for any lawful purposes except to: (a) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (spam); or (b) enable high volume, automated, electronic processes that apply to Registrar (or its systems).

(Ex. E to McPherson Decl.) (emphasis added).

Originally Register.com's terms and conditions for users of its WHOIS database were substantially the same. In April 2000, however, Register.com implemented the following more restrictive terms of use governing its WHOIS database:

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone; or (2) enable high volume, automated, electronic processes that apply to Register.com (or its systems). The compilation, repackaging, dissemination or other use of this data is expressly prohibited without the prior written consent of Register.com. Register.com reserves the right to modify these terms at any time. By submitting this query, you agree to

abide by these terms.

(Ex. 27 to Pl.'s Sept. 8, 2000 Motion) (emphasis added).³

Verio's Project Henhouse

In late 1999, to better target their marketing and sales efforts toward customers in need of web hosting services and to reach those customers more quickly, Verio developed an automated software program or "robot."⁴ With its search robot, Verio accessed the WHOIS database maintained by the accredited registrars, including Register.com, and collected the contact information of customers who had recently registered a domain name. Then, despite the marketing prohibitions in Register.com's terms of use, Verio utilized this data in a marketing initiative known as Project Henhouse and began to contact and solicit

³ ICANN in its amicus submission dated September 22, 2000 through Louis Touton, its General Counsel, stated that:

To the extent that Register.com is using this legend to restrict otherwise lawful use of the data for mass unsolicited, commercial advertising or solicitations by direct mail or telephone (and not just by electronic mail), it is ICANN's position that Registrar.com (sic) has failed to comply with the promise it made in Section II.F.5 of the Registrar Accreditation Agreement.

(ICANN Amicus Br. at 11).

⁴ Before the development of its search robot, Verio relied primarily on banner and print ads, and briefly on predictive dialing in its marketing efforts. Under the predictive dialing approach, Verio purchased potential customer leads, then contacted those leads by telephone, using a computer dialer and connecting the call to a telemarketer when a potential customer answered. (See Ayers Depo. at 33-34, 75-76).

Register.com's customers, within the first several days after their registration, by e-mail, regular mail, and telephone.

Verio's Search Robots

In general, the process worked as follows: First, each day Verio downloaded, in compressed format, a list of all currently registered domain names, of all registrars, ending in .com, .net, and .org. That list or database is maintained by Network Solutions, Inc. ("NSI") and is published on 13 different "root zone" servers. The registry list is updated twice daily and provides the domain name, the sponsoring registrar, and the nameservers for all registered names. Using a computer program, Verio then compared the newly downloaded NSI registry with the NSI registry it downloaded a day earlier in order to isolate the domain names that had been registered in the last day and the names that had been removed. After downloading the list of new domain names, only then was a search robot used to query the NSI database to extract the name of the accredited registrar of each new name.⁵ That search robot then automatically made successive queries to the various registrars' WHOIS databases, via the port 43 access channels, to harvest the relevant contact information for each new domain name registered. (See Eden Depo. at 26-30;

⁵ Although Register.com and ICANN have also criticized Verio's use of its search robot to collect the registrar names from NSI's computer system (see ICANN Amicus Br. at 15), that issue is not before the Court.

Eden Decl. ¶¶ 36-38). Once retrieved, the WHOIS data was deposited into an information database maintained by Verio. The resulting database of sales leads was then provided to Verio's telemarketing staff.

Marketing History

Beginning in January, 2000, Register.com learned that Verio was e-mailing its customers to solicit business. Register.com through its Director of Strategic Initiatives Lauren Gavisser complained to Eric Eden, Director of Sales and Channel Operations of Verio, citing an e-mail received by a customer which identified Verio as the sender but stated "[b]y now you should have received an email from us confirming the registration of your domain name(s) ... you have taken the first step towards having your own website ... the next step is to set up a hosting account ..." (Ex. 4 to Pl.'s Sept. 8, 2000 Motion). Gavisser advised Eden that the e-mail had misled the customer into thinking that Verio had an affiliation with or sponsorship from Register.com. (See Ex. 5 to Pl.'s Sept. 8, 2000 Motion). Eden replied that "our intention is not to mislead people. The e-mail that was sent resulted from a system problem." Id. He promised to correct it.

Register.com continued to get complaints about e-mail and telephone solicitations by Verio from its customers and co-brand partners through January. In March 2000 Gavisser again contacted

Eden to complain that Register.com was still receiving numerous complaints, including that a number of telephone messages similar to the following were left with Register.com customers: "This is [name of telemarketer] calling from Verio regarding the registration of [customer's domain name]. Please contact me at your earliest convenience." (Ex. 44 to Pl.'s Sept. 8, 2000 Motion).

On May 5, 2000 Register.com's lawyers wrote to Verio's General Counsel requesting that Verio immediately cease and desist from this marketing conduct. Register.com complained generally that the use of its mark as well as the timing of the solicitations was harming its good will and specifically warned Verio that it was violating the terms of use it had agreed to in submitting its WHOIS queries by sending "mass unsolicited, commercial advertising or solicitations via e-mail (spam)." (Ex. E to McPherson Decl.).

On May 9, 2000 Verio, through an Associate Counsel, communicated that it had stopped using the Register.com mark or any other similar mark or phrase which would lead to confusion and had ceased accessing the WHOIS database for the purpose of marketing through e-mail. (See Ex. 7 to Pl.'s Sept. 8, 2000 Motion). In an effort to confirm settlement of the dispute, Register.com's lawyers sent Verio a terms letter for it to sign and acknowledge. In that letter Register.com specifically

required Verio to cease use of the WHOIS database for not just e-mail marketing, but also direct mail and telemarketing. Verio refused to sign and although it ceased e-mail solicitation, it continued to use the WHOIS contact information for telemarketing purposes into July 2000. (See Ex. 14 to Pl.'s Sept. 8, 2000 Motion, Ayers Depo. at 56).

Accordingly, Register.com commenced this lawsuit and moved for a temporary restraining order and preliminary injunction on August 3, 2000. On August 4, 2000, Verio sought expedited discovery and agreed on August 9, 2000 to enter into a stipulated temporary restraining order with Register.com which prevents it from accessing Register.com's WHOIS database by using a search robot and prevents Verio from using any data obtained from Register.com to solicit Register.com's customers. Prior to the Court's September 15, 2000 hearing, the Court asked ICANN to submit an amicus curiae brief outlining its position with respect to the parties' dispute. The Court granted the parties' request to respond to ICANN's brief, which responses were received on September 28, 2000.

II. Discussion

This dispute centers on both Verio's end use of the WHOIS data and its use of the automated search robot. While Register.com acknowledges its obligation to provide public access to its customers' contact information, it has developed "terms of

use" which prohibit third parties, such as Verio, from using the contact information for any mass marketing purpose - whether by e-mail, regular mail or telephone. Register.com also argues that the use of automated software to access the WHOIS database violates its terms of use and harms its computer systems.

Verio admits both the use of the WHOIS data for marketing purposes and the use of the search robot. Verio also concedes that its end use of the information violates the marketing restriction imposed by Register.com, but argues that this restriction should not be enforced because -- at a minimum -- direct mail and telephone marketing are permissible uses under the terms of the Accreditation Agreement Register.com signed with ICANN.⁶ Verio argues that by imposing these impermissible anti-marketing restrictions Register.com is in breach of that Agreement. Verio also argues that the use of the robot is not prohibited by Register.com's terms of use and claims that

⁶ Verio contests Register.com's assertion that its particular use of e-mail to solicit Register.com's customers constitutes the "spamming" that is prohibited by the ICANN agreement. The Court need not determine whether Verio's e-mails constitute "spam" because it is Register.com's terms of use, rather than ICANN's, that are at issue here. Register.com's terms do not specifically prohibit "spam", but rather simply prohibit the use of WHOIS data for mass, unsolicited e-mail. Verio's e-mails clearly violate Register.com's terms of use. Verio's unsolicited e-mail solicitations are "mass" by any definition of the term. Even though the e-mails are not sent simultaneously with one mouse click, as Verio argues, they are sent in massive quantities over a short period of time, and thus fit the definition of "mass" e-mails.

Register.com has not proven that the robot causes any harm, let alone irreparable harm, to Register.com's computer systems.

III. Standard For Injunctive Relief

In order to obtain a preliminary injunction, a plaintiff must demonstrate both (1) that it will suffer irreparable harm if the motion is not granted and (2) either (a) a likelihood that it will succeed on the merits of the action or (b) a sufficiently serious question going to the merits of the litigation and the balance of hardships tipping decidedly in plaintiff's favor.

See L. & J.G. Stickleby, Inc. v. Canal Dover Furniture Co., 79 F.3d 258, 261-62 (2d Cir. 1996).

The purpose of a preliminary injunction is to keep the parties, while the suit is pending, as much as possible in the respective positions they occupied when the suit began and to preserve the Court's ability to render a meaningful decision after a trial on the merits. See WarnerVision Entertainment v. Empire of Carolina, Inc., 101 F.3d 259, 261-62 (2d Cir. 1996). A preliminary injunction is an extraordinary and drastic measure that should not be routinely granted, see Mazurek v. Armstrong, 520 U.S. 968 (1997), because it is "one of the most drastic tools in the arsenal of judicial remedies." Hanson Trust PLC v. SCM Corp., 774 F.2d 47, 60 (2d Cir. 1985). The granting of a preliminary injunction is within the equitable discretion of the trial judge. Societe Comptoir De L'Industrie Cotonniere

Etablissements Boussac v. Alexander's Dep't Stores, Inc., 299
F.2d 33 (2d Cir. 1962).

IV. Register.com's Claims

The heart of Verio's defense is that this Court should refuse to enforce Register.com's terms of use. Accordingly, the Court turns to a discussion of Register.com's breach of contract claim.

A. Breach of Contract

Register.com imposes conditions on the access to and end use of data contained in its WHOIS database. It publishes those terms of use on the home page of its Internet website and conditions entry into the WHOIS database on assent to those terms. As noted above, Verio concedes that it violated Register.com's posted restriction on the use of WHOIS data for direct mail and telephone marketing purposes. Verio contends however that violating Register.com's restrictions on the use of WHOIS data for marketing purposes did not constitute a breach of contract for two reasons. First, Verio argues that the promises Register.com made to ICANN in the Agreement have created a privilege in Verio to access the WHOIS database, and that it may interpose the Agreement as a defense to any claim by Register.com that Verio violated an access or use restriction broader than those permitted in the Accreditation Agreement. Second, Verio argues that even if Register.com's terms of use are enforceable,

Verio has never manifested any assent to those terms. Neither defense is availing.

With respect to Verio's first argument, the ICANN Accreditation Agreement specifically disclaims any intention to vest rights in a third-party beneficiary. Section II.S.2 of the Agreement reads: "No Third-Party Beneficiaries. This Agreement shall not be construed to create any obligation by either ICANN or Registrar to any non-party to this agreement, including any SLD holder." (Ex. 27 to Pl.'s Sept. 8, 2000 Motion). Verio argues that while II.S.2 might prevent it from using the Agreement as the basis for a contract cause of action against Register.com, II.S.2 does not foreclose the possibility that the contract grants Verio a defense to this cause of action by creating a privilege or immunity in Verio to access the WHOIS data free from any restrictions which would violate Register.com's promises to ICANN.

However, the authority cited by Verio in support of this argument is unpersuasive. Verio cites 4 Corbin on Contracts § 780 at 67-70, Rochester Tel. Co. v. Ross, 195 N.Y. 429 (1909), Continental Corp. v. Gowdy, 186 N.E. 244 (Mass. 1933), Fidelity-Phenix Fire Ins. Co. of New York v. Forest Oil Corp., 141 So. 2d 841 (La. Ct. App. 1962) and Baurer v. Devenes, 121 A. 566 (Conn. 1923). Most importantly, as Register.com has pointed out, none of the authority cited by Verio addresses a contract containing a

clause similar to II.S.2 of the Agreement specifically disclaiming any intention to benefit a third party. The Accreditation Agreement, unlike the agreements discussed in the above-cited cases, is clear and unambiguous, and creates no right in Verio to breach its agreement to abide by Register.com's terms of use for accessing its WHOIS data. Moreover, the cases are distinguishable on other grounds as well.

Rochester Tel. Co. v. Ross, 195 N.Y. 429 (1909) involved a telephone company which, in consideration for being granted a monopolistic franchise to provide telephone service in Rochester, agreed with the city franchisor not to charge subscribers more than \$48 per year. Public utilities such as telephone companies occupy a different position than other private companies by virtue of their monopolistic position and by virtue of the necessity of the service they provide. The Restatement (Second) of Torts § 259 (1965) provides that:

One who has a right to the use of a facility of a public utility is privileged to make any reasonable use of the chattels of the utility that is or is reasonably believed to be necessary to the enjoyment of the facility.

Although Verio does make the argument that it is privileged to access Register.com's WHOIS database, Verio has not specifically argued that the port 43 access facility is a public

utility' similar to telephone service. Even if Verio were to make that argument, it would fail. Comment (a) to § 259 defines a public utility as:

[A] person, corporation, or other association carrying on an enterprise for the accommodation of the public, the members of which have the right as such to use its facilities. Instances of a public utility are common carriers, common innkeepers, telegraph and telephone companies, and gas and electric light companies.

New York courts define a public utility as:

A privately owned and operated business ... which is engaged in regularly supplying the public with some commodity or service which is of public consequence [and] need ... The test for determining if a concern is a public utility is whether it has held itself out as ready, able and willing to serve the public.

See City of New York v. New York State Dept. of Health, 623 N.Y.S. 2d 491, 496 (Sup. Ct. 1995) (citing Black's Law Dictionary, 1232 (6th Ed. 1990)). The provision of port 43 access to WHOIS data is not "a commodity or service which is of public consequence and need" and therefore Register.com is not acting as a public utility in agreeing to provide port 43 access. Cf. Island Online, Inc. v. Network Solutions, Inc., No. 99 Civ. 6848 (DGT) 2000 WL 1661435, at *17 (E.D.N.Y. Nov. 6, 2000) (noting that "the Internet is, by no stretch of the imagination, a traditional and exclusive public function. For most of its history, its growth and development have been nurtured by and

⁷ In its brief opposing the motion, Verio refers to Register.com's port 43 access channel as a "public resource" and a "public facility." (See Def.'s Opp. Memo. at 21 & 22.)

realized through private action."); Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1025, 1024 (S.D. Ohio 1997)

(holding that under Ohio law, public utility analysis demands that the entity "devote[] an essential good or service to the general public" and holding that defendant had not demonstrated that Internet service provider qualified as public utility).

Accordingly, Verio has no privilege on that basis to breach its agreement to abide by Register.com's WHOIS terms of use.

In Continental Corp. v. Gowdy, 186 N.E. 244 (Mass. 1933), the Court permitted the directors of a corporation to interpose a bond contract to which they were not a party as a defense to an action on the bonds. However, the bonds indicated on their face that they were without recourse to the directors, and thereby specifically provided for the defense asserted. Gowdy therefore is factually and analytically distinguishable from this case, where no defense was specifically provided to Verio and indeed the Agreement specifically states that it creates duties solely between the parties. Fidelity-Phenix Fire Ins. Co. of New York v. Forest Oil Corp., 141 So. 2d 841 (La. Ct. App. 1962) is analytically similar to Gowdy and therefore provides no support to Verio's position. See generally id. (allowing non-party to insurance contract to enforce insurer's explicit waiver of subrogation rights).

Accordingly, the Agreement does not grant Verio a defense to

Register.com's breach of contract claim for Verio's violation of the terms of use restrictions Register.com places on access to its WHOIS database.⁸

Reasoning that the terms of the Accreditation Agreement represent quasi-regulatory standards, Verio argues that Register.com's more restrictive terms of use also violate public policy. This argument must fail because ICANN is not a governmental body. No government entity has undertaken to regulate the Internet and no statutory scheme exists to provide the framework for Verio's policy arguments. See Compuserve, 962 F. Supp. at 1026. Rather, as discussed above, the Department of Commerce's establishment of ICANN signified a movement away from nascent public regulation of the Internet and toward a consensus-based private ordering regime. Indeed, the Department of Commerce's Statement of Policy on the Management of Internet Names and Addresses, also known as the "White Paper," expressly states:

[T]he Department of Commerce has determined that it should issue a general statement of policy, rather

⁸ The Court notes that ICANN may terminate Register.com's accreditation under section II.N.4 of the Agreement for its breach of the Agreement. ICANN urges this Court "to promote the integrity of the ICANN process by allowing the contractually specified exclusive remedies for [Register.com's] breach to operate as they were intended." To date this Court is unaware of any decision by ICANN with respect to the issue of Register.com's breach. However, ICANN's inaction does not grant Verio the right to breach its contract with Register.com.

than define or impose a substantive regulatory regime for the domain name system. As such, this policy statement is not a substantive rule, does not contain mandatory provisions, and does not itself have the force and effect of law.

(Ex. B. to McPherson Decl.). Accordingly, the Accreditation Agreement represents a private bargain between ICANN and Register.com and does not provide Verio with any privilege or defense.

Nor can Verio argue that it has not assented to Register.com's terms of use. Register.com's terms of use are clearly posted on its website. The conclusion of the terms paragraph states "[b]y submitting this query, you agree to abide by these terms." (Ex. 27 to Pl.'s Sept. 8, 2000 Motion). Verio does not argue that it was unaware of these terms, only that it was not asked to click on an icon indicating that it accepted the terms. However, in light of this sentence at the end of Register.com's terms of use, there can be no question that by proceeding to submit a WHOIS query, Verio manifested its assent to be bound by Register.com's terms of use, and a contract was formed and subsequently breached.

Register.com alleges that the breach has resulted in irreparable harm: in lost opportunities to sell competing services to its opt-in customers, and to its reputation and good will with customers and co-brand partners, who have threatened to take their business elsewhere if Register.com cannot protect the

WHOIS contact information.

The classic remedy for breach of contract is an action at law for monetary damages. If the injury complained of can be compensated by an award of monetary damages, then an adequate remedy at law exists and no irreparable injury may be found as a matter of law. However, the Second Circuit has recognized that even where damages are available, irreparable harm may be found where those damages are clearly difficult to assess and measure. The Second Circuit Court's opinion Ticor Title Ins. Co. v. Cohen, 173 F.3d 63, 69 (2d Cir. 1999) captures precisely why damages in this case are incalculable and the harm resulting from the breach is irreparable. The Court wrote, in finding irreparable harm resulting from the breach of a covenant not to compete in an employment contract, "[i]nitially, it would be very difficult to calculate monetary damages that would successfully redress the loss of a relationship with a client that would produce an indeterminate amount of business in years to come." See id. at 69.

Neither this Court nor the parties to this action could calculate with any precision the amount of the monetary loss which has resulted and which would result in the future from the loss of Register.com's relationships with customers and co-brand partners. Register.com has therefore demonstrated that Verio's past and future breaches have resulted and will result in

irreparable harm. See also Gulf & Western Corp. v. Craftique Productions, Inc., 523 F. Supp. 603, 607 (1981) ("even in situations where damages are available, irreparable harm may be found if damages are 'clearly difficult to assess and measure.'") (citing Danielson v. Local 275, Laborers Int'l Union of North America, 479 F.2d 1033, 1037 (2d Cir. 1973)).

Register.com has demonstrated both a likelihood of success on the merits of its breach of contract claim with respect to Verio's use of WHOIS data for marketing purposes, and has demonstrated irreparable harm resulting from the breach. Accordingly, it is entitled to an injunction against any future use by Verio of information taken from its WHOIS database for marketing by e-mail, direct mail or telephone."

B. Trespass To Chattels

Register.com argues that Verio's use of an automated software robot to search the "WHOIS" database constitutes trespass to chattels. Register.com states that it has made its computer system available on the Internet, and that "Verio has used 'software automation' to flood that computer system with traffic in order to retrieve the contact information of Register.com customers for the purpose of solicitation in knowing violation of Register.com's posted policies and terms of use."

(Pl.'s Mem. of Law at 36.)

The standard for trespass to chattels in New York is based upon the standard set forth in the Restatement of Torts:

One who uses a chattel with the consent of another is subject to liability in trespass for any harm to the chattel which is caused by or occurs in the course of any use exceeding the consent, even though such use is not a conversion.

City of Amsterdam v. Goldreyer, Ltd., 882 F. Supp. 1273 (E.D.N.Y. 1995) (citing Restatement (Second) of Torts, § 256 (1965)).

As an initial matter, the Court does not believe that Register.com's terms of use forbid the particular use of the search robot at issue here. Register.com's posted policies and terms of use require a party who seeks access to its WHOIS database to agree that it will not "use this data to ... enable high volume, automated, electronic processes that apply to Register.com (or its systems)." Register.com argues that use of a search robot is prohibited by that term of use. The Court disagrees.

The terms state that under no circumstances may one "use this data [the WHOIS data] to ... enable high volume, automated, electronic processes that apply to Register.com." The temporal aspect of this term is important because it only bars future automated processes. Although Verio uses an automated process to collect the WHOIS data, it does not then use the collected data to enable an automated process that applies to Register.com's

systems. Once Verio's software robot secures the WHOIS information from Register.com's systems, it has completed its automated process with respect to Register.com's systems. The robot does not then use that WHOIS data to "enable high volume, automated, electronic processes that apply to Register.com (or its systems)," it simply deposits the data into a database.

However, despite the fact that Register.com's terms of use may not specifically forbid this use of a search robot by Verio and such use does not therefore constitute a breach of contract, it is clear since at least the date this lawsuit was filed that Register.com does not consent to Verio's use of a search robot, and Verio is on notice that its search robot is unwelcome.

(Pl.'s V.C. ¶ 36)

Accordingly, Verio's future use of a search robot to access the database exceeds the scope of Register.com's consent, and Verio is liable for any harm to the chattel (Register.com's computer systems) caused by that unauthorized access. See Compuserve, 962 F. Supp. at 1024 (holding that defendants' continued use after CompuServe notified defendants that it no longer consented to the use of its proprietary computer equipment was a trespass) (citing Restatement (Second) of Torts §§ 252 and 892A(5)).

Having established that Verio's access to its WHOIS database by robot is unauthorized, Register.com must next demonstrate that

Verio's unauthorized access caused harm to its chattels, namely its computer system. To that end, Robert Gardos, Register.com's Vice President for Technology, submitted a declaration estimating that Verio's searching of Register.com's WHOIS database has resulted in a diminishment of 2.3% of Register.com's system resources. (See Gardos Decl. ¶ 32.) However, during discovery, the basis for Gardos' estimations of the impact Verio's search robot had on Register.com's computer systems was thoroughly undercut. Gardos admitted in his deposition that he had taken measurements of neither the capacity of Register.com's computer systems nor the portion of that capacity which was consumed by Verio's search robots. Furthermore, when describing how he arrived at his conclusion that Verio's search robots occupied a certain percentage of Register.com's systems capacity, Mr. Gardos testified that the numbers he used were "all rough estimates." (Gardos Depo. at 76).

Although Register.com's evidence of any burden or harm to its computer system caused by the successive queries performed by search robots is imprecise, evidence of mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels. "A trespasser is liable when the trespass diminishes the condition, quality, or value of personal property." Ebay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal 2000) (citing

Compuserve, 962 F. Supp. at 1022). "The quality or value of personal property may be 'diminished even though it is not physically damaged by defendant's conduct.'" Id. Though it does correctly dispute the trustworthiness and accuracy of Mr. Gardos' calculations, Verio does not dispute that its search robot occupies some of Register.com's systems capacity.

Although Register.com was unable to directly measure the amount by which its systems capacity was reduced, the record evidence is sufficient to establish the possessory interference necessary to establish a trespass to chattels claim. As the eBay Court wrote:

BE argues that its searches present 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 only use 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.

(100 F. Supp. 2d at 1071.) (emphasis added).

Furthermore, Gardos also noted in his declaration "if the strain on Register.com's resources generated by Verio's searches becomes large enough, it could cause Register.com's computer systems to malfunction or crash" and "I believe that if Verio's

searching of Register.com's WHOIS database were determined to be lawful, then every purveyor of Internet-based services would engage in similar conduct." (Gardos Decl. ¶¶ 33, 34). Gardos' concerns are supported by Verio's testimony that it sees no need to place a limit on the number of other companies that should be allowed to harvest data from Register.com's computers. (See Ayers Depo. at 71). Furthermore, Verio's own internal documents reveal that Verio was aware that its robotic queries could slow the response times of the registrars' databases and even overload them. (See Ex. 29 & to Pl.'s Sept. 8, 2000 Motion). Because of that possibility, Verio contemplated cloaking the origin of its queries by using a process called IP aliasing. (See id.; see also Ex. 64 to Pl.'s Sept. 8, 2000 Motion).

Accordingly, Register.com's evidence that Verio's search robots have presented and will continue to present an unwelcome interference with, and a risk of interruption to, its computer system and servers is sufficient to demonstrate a likelihood of success on the merits of its trespass to chattels claim.

There is no adequate remedy at law for an ongoing trespass and without an injunction the victim of such a trespass will be irreparably harmed. The eBay court specifically held that eBay was entitled to preliminary injunctive relief based on the claim that if such relief were denied, other companies would be encouraged to deploy search robots against eBay's servers and

would further diminish eBay's server capacity to the point of denying effective access to eBay's customers. See id. at 1071-72.

The same reasoning applies here. Register.com, through Mr. Gardos, has expressed the fear that its servers will be flooded by search robots deployed by competitors in the absence of injunctive relief. Register.com has therefore demonstrated both a likelihood of success on the merits of its trespass to chattels claim and the existence of irreparable harm, and is entitled to a preliminary injunction against Verio based upon that claim.

C. Computer Fraud And Abuse Act
§§ 1030(a)(2)(C) and (a)(5)(C)

The issue of the scope of Verio's authorization to access the WHOIS database is also central to the Court's analysis of Register.com's claims that Verio is violating two discrete provisions of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 et seq.¹⁰

Register.com claims both that the use of software robots to harvest customer information from its WHOIS database in violation of its terms of use violates 18 U.S.C. §§ 1030(a)(2)(C) and (a)(5)(C), and that using the harvested information in violation of Register.com's policy forbidding the use of WHOIS data for

¹⁰ Remedies under this criminal code provision include injunctive relief under 18 U.S.C. § 1030(g).

marketing also violates those sections. That is, that both Verio's method of accessing the WHOIS data and Verio's end uses of the data violate the CFAA.

1. Verio's Use of Search Robots

Both §§ 1030(a)(2)(C) and (a)(5)(C) require that the plaintiff prove that the defendant's access to its computer system was unauthorized, or in the case of § 1030(a)(2)(C) that it was unauthorized or exceeded authorized access. However, although each section requires proof of some degree of unauthorized access, each addresses a different type of harm. Section 1030(a)(2)(C) requires Register.com to prove that Verio intentionally accessed its computers without authorization and thereby obtained information. Section 1030(a)(5)(C) requires Register.com to show that Verio intentionally accessed its computer without authorization and thereby caused damage.

As discussed more fully in the context of the trespass to chattels claim, because Register.com objects to Verio's use of search robots they represent an unauthorized access to the WHOIS database.

The type of harm that Register.com alleges is caused by the search robots, including diminished server capacity and potential system shutdowns, is better analyzed under § 1030(a)(5)(C), which specifically addresses damages to the computer system. Pursuant

to the pertinent part¹¹ of § 1030(e) (8), "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information that (A) causes loss aggregating at least \$5000 in value during any 1-year period to one or more individuals."

On this record Register.com has demonstrated that Verio's unauthorized use of search robots to harvest registrant contact information from Register.com's WHOIS database has diminished server capacity, however slightly, and could diminish response time, which could impair the availability of data to clients trying to get registrant contact information. Moreover, Register.com has raised the possibility that if Verio's robotic queries of Register.com's WHOIS database were determined to be lawful, then other vendors of Internet services would engage in similar conduct. This Court finds that it is highly probable that other Internet service vendors would also use robots to obtain this potential customer information were it to be permitted. The use of the robot allows a marketer to reach a potential client within the first several days of the domain name

¹¹ None of the other provisions of § 1030(e) (8) are relevant to this case. Section 1030(e) (8) (B) covers impairment or modification of data or systems affecting "the medical examination, diagnosis, treatment, or care of one or more individuals;" § 1030(e) (8) (C) covers impairment or modification of data or systems causing "physical injury to any person," and 1030(e) (8) (D) covers impairment or modification of data or systems which "threatens public health or safety."

registration, an optimal time to solicit the customer for other services. In contrast, if instead of using a search robot the service vendor obtains registrant contact information pursuant to a bulk license, the vendor must wait to receive the information on a weekly basis. As Eric Eden, the director of operation Henhouse wrote in an e-mail to a Verio employee "[c]onsistent testing has found that the faster we approach someone after they register a domain name, the more likely we are to sell them hosting." (Ex. 40 to Pl.'s Sept. 8, 2000 Motion).

If the strain on Register.com's resources generated by robotic searches becomes large enough, it could cause Register.com's computer systems to malfunction or crash. Such a crash would satisfy § 1030(a)(5)(C)'s threshold requirement that a plaintiff demonstrate \$5000 in economic damages¹² resulting from the violation, both because of costs relating to repair and lost

¹² Register.com relies upon lost revenue from Verio's exploitation of the WHOIS data for marketing purposes to constitute the damages required under § 1030(a)(5)(C). Although lost good will or business could provide the loss figure required under § 1030(a)(5)(C), it could only do so if it resulted from the impairment or unavailability of data or systems. The good will losses cited by Register.com are not the result of the harm addressed by § 1030(a)(5)(C). How Verio uses the WHOIS data, once extracted, has no bearing on whether Verio has impaired the availability or integrity of Register.com's data or computer systems in extracting it. Accordingly, because violating an anti-marketing restriction on the end use of data harms neither the data nor the computer and therefore does not cause the type of harm that § 1030(a)(5)(C) addresses, the specific good will damages cited by Register.com cannot satisfy its burden under § 1030(a)(5)(C).

data and also because of lost good will based on adverse customer reactions.

A potential harm which cannot be addressed by a legal or equitable remedy following a trial, such as the loss of customers that might result from a system shutdown or slowed response times complained of here, constitutes an irreparable injury. See Instant Air Freight Co. v. C.F. Air Freight, Inc., 882 F.2d 797, 799-800 (3rd Cir. 1989); Cyber Promotions, Inc. v. Apex Global Info. Servs., 1997 U.S. Dist. LEXIS 15344 at *7 (E.D. Pa. Sept. 30, 1997). A showing that a plaintiff may suffer a substantial loss of business if relief is not granted meets the standards for interim relief. See Doran v. Salem Inn, 422 U.S. 922 (1975).

Because Register.com has demonstrated that Verio's access to its WHOIS database by means of an automated search robot is unauthorized and caused or could cause \$5000 in damages by impairing the availability of data or the availability of its computer systems, Register.com has established both irreparable harm and a likelihood of success on the merits of its claim that Verio's use of the search robot violated § 1030(a)(5)(C) of the Computer Fraud And Abuse Act. Register.com is therefore entitled to injunctive relief based upon this claim.

2. Verio's Use of WHOIS Data For Marketing Purposes

With respect to its use of Register.com's WHOIS data for e-

mail, direct mail and telephone marketing, Verio argues that such an act can only be analyzed under § 1030(a)(2)(C)'s provision assessing liability where a party exceeds authorized access and obtains information it is not entitled to obtain. Verio argues that because it is authorized to access the WHOIS database for some purposes its access was authorized. Verio then argues that its conduct must meet the Act's specific definition of conduct that "exceeds authorized access." Pursuant to the definition contained in § 1030(e)(6) of the CFAA, "the 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 accessor is not entitled to obtain or alter." 18 U.S.C. § 1030(e)(6) (emphasis added). Verio then argues that this definition does not contemplate a violation of end use restrictions placed on data as "exceeding authorized access," and therefore that Verio has not violated § 1030(a)(2)(C).

Again, neither party disputes that Verio is not authorized under Register.com's terms of use to use the data for mass marketing purposes, and neither party disputes that Verio is authorized to obtain the data for some purposes. However, Verio's distinctions between authorized access and an unauthorized end use of information strike the Court as too fine. First, the means of access Verio employs, namely the automated search robot, is unauthorized. Second, even if Verio's means of

access to the WHOIS database would otherwise be authorized, that access would be rendered unauthorized ab initio by virtue of the fact that prior to entry Verio knows that the data obtained will be later used for an unauthorized purpose.

Accordingly, the Court finds that Verio's access to the WHOIS database was unauthorized and that Verio violated § 1030(a)(2)(C) by using that unauthorized access to obtain data for mass marketing purposes. As discussed above, the harvesting and subsequent use of that data has caused and will cause Register.com irreparable harm. Therefore, because Register.com has demonstrated a likelihood of success on the merits of its claim that Verio's use of its WHOIS data for mass marketing purposes violates § 1030(a)(2)(C) of the Computer Fraud And Abuse Act and has demonstrated irreparable harm stemming from that violation, Register.com is entitled to injunctive relief based on that claim.

D. Lanham Act

Section 43(a) of the Lanham Act prohibits any false designation of origin which

is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities with another person.

15 U.S.C. § 1125(a)(1). In order to prove its Lanham act claims, Register.com must demonstrate that it has a valid mark entitled

to protection and that Verio's conduct is likely to cause confusion concerning the source or sponsorship of Verio's services. See, e.g., Morningside Group Ltd. v. Morningside Capital Group, LLC, 182 F.3d 133, 137 (2d Cir. 1999).

Verio does not dispute that Register.com has a valid and protectible mark. It does however dispute Register.com's claims that its customers were or will continue to be confused about Verio's relationship to Register.com because of Verio's marketing practices. Verio also argues that if confusion occurred or is likely to occur in the future, it is not the type of confusion actionable under the Lanham Act.

To begin with, Verio's solicitation of Register.com's customers evolved over the course of project Henhouse. Initially, some of Verio's e-mail solicitations mentioned Register.com's name and contained the phrase "first step," which is similar to "first step on the web," a phrase for which Register.com has sought trademark protection. (See, e.g., Ex. 14 to Pl.'s Sept. 8, 2000 Motion). These e-mails, because they use Register.com's marks, were clearly likely to cause confusion as to whether there was some affiliation or sponsorship between Verio and Register.com, and therefore violated the Lanham Act. And, by a letter dated May 9, 2000, Verio agreed not to refer to the Register.com mark or any other similar mark in its future solicitations.

Register.com maintains that even without these references, Verio's subsequent solicitations violated the Lanham Act. While Verio's later phone solicitations did not mention the Register.com or "first step" marks, they did indicate that the caller from Verio was calling "regarding your recently registered domain name" or "regarding the registration of [domain name]. Please contact me at your earliest convenience ... If I don't hear from you in a couple days, I will call back." (See Exs. 44 & 45 to Pl.'s Sept. 8, 2000 Motion). Whether these solicitations violate the Lanham Act is a closer question. Although Verio does not employ any of Register.com's marks in these communications, the Court finds that the phrasing does create the impression that the reason for the call is related to the registration of the domain name, rather than the solicitation of web hosting services for the new domain name. The Court also finds that the impression that Verio telemarketers are calling because of some problem with the domain name registration could lead to confusion with respect to whether there is some affiliation or sponsorship between Verio and Register.com. In fact, Register.com presented evidence of actual customer confusion stemming from this practice. (See Pl.'s Ex. 12 "The telephone message seemed to me to imply that there was some problem with the name I had just registered"). Accordingly, such phrasing violates the Lanham Act.

Register.com also seems to claim that Verio's solicitations violate the Lanham Act regardless of their content because of the short time between the customers' registration of a domain name with Register.com and the solicitation by Verio. Register.com alleges that because of the timing its customers are under the mistaken impression that Verio is affiliated with Register.com and because of that give greater consideration to these solicitations than they otherwise would.

However, to make out a claim under § 43(a) sufficient to entitle it to injunctive relief, Register.com must show that (1) Verio makes material misrepresentations about the nature, characteristics or geographic origin of its services; (2) it uses the false or misleading representations "in commerce" (3) it makes the representations in the context of commercial advertising or commercial promotion; and (4) that Register.com is likely to be damaged by the misrepresentations. See Towers Financial Corp. v. Dun & Bradstreet, Inc., 803 F.Supp. 820, 823 (S.D.N.Y. 1992) (citing McNeil-P.C.C., Inc. v. Bristol Myers Squibb Co., 938 F.2d 1544, 1548-49 (2d Cir. 1991)); National Artists Management Co. v. Weaving, 769 F. Supp. 1224, 1230 (S.D.N.Y. 1991); McCarthy on Trademarks, § 27.04(1)(a).

Register.com cannot claim that rapid timing alone constitutes a violation of the Lanham Act where Verio neither makes a false or misleading representation about the origin of

its services nor uses Register.com's mark in its solicitations. See Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619, 625 (6th Cir. 1996) ("the defendants' use of a protected mark or their use of a misleading representation is a prerequisite to the finding of a Lanham Act violation."). It is not enough that Register.com's customers might be confused as to any affiliation between Register.com and Verio because of Verio's rapid solicitation. To state a claim under § 43(a), Register.com must show not only that its customers are confused, but that they have been misled by some representation made by Verio.

Register.com is correct that some of Verio's solicitations were in the past misleading on their face and violated the Lanham Act. Register.com is also correct that some of Verio's more recent solicitations, although they did not use any protected mark, created confusion as to whether Verio was calling because of some problem with the customer's domain name registration, which resulted in confusion with respect to whether Verio and Register.com were affiliated in any way. Accordingly, the Court finds on the current record that Register.com is likely to succeed on the merits of its claims of unfair competition and false designation of origin under § 43(a) of the Lanham Act with respect to any e-mail, telephone, or direct mail solicitation that uses the "Register.com" or "first step on the Web" marks or any similar marks. Register.com is also likely to succeed on

Lanham Act claims based on Verio's solicitations that suggest that Verio is calling with regard to the registration of the domain name or any problem arising from that registration. As more fully discussed in the context of the breach of contract claim, these Lanham Act violations may result in the irreparable harm of lost client relationships.

Accordingly, the Court enjoins Verio from any future use in its e-mail, direct mail, or telephone solicitations of the marks Register.com or "first step on the web" or any similar mark. Furthermore, the Court enjoins Verio from indicating in any affirmative way that it is calling regarding the registration of the customer's domain name, rather than in regard to the provision of web-hosting or other services related to the domain name.

V. Injunction

For the foregoing reasons and pursuant to Fed. R. Civ. P. 65, it is hereby ORDERED, that pending a final decision on the merits of plaintiff's claims, defendant Verio Inc., its officers, agents, servants, employees, successors and assigns, all persons acting in concert or participation with Verio, and/or acting on its behalf or at its direction (collectively, "Verio"), are enjoined from engaging in the following activities:

1. Using or causing to be used the "Register.com" mark or the "first step on the web" mark or any other designation

similar thereto, on or in connection with the advertising, marketing, or promotion of Verio and/or any of Verio's services;

2. Representing, or committing any act which is calculated to or is likely to cause third parties to believe that Verio and/or Verio's services are sponsored by, or have the endorsement or approval of Register.com;

3. Accessing Register.com's computers and computer networks in any manner, including, but not limited to, by software programs performing multiple, automated, successive queries, provided that nothing in this Order shall prohibit Verio from accessing Register.com's WHOIS database in accordance with the terms and conditions thereof; and

4. Using any data currently in Verio's possession, custody or control, that using its best efforts, Verio can identify as having been obtained from Register.com's computers and computer networks to enable the transmission of unsolicited commercial electronic mail, telephone calls, or direct mail to the individuals listed in said data, provided that nothing in this Order shall prohibit Verio from (i) communicating with any of its existing customers, (ii) responding to communications received from any Register.com customer initially contacted before August 4, 2000, or (iii) communicating with any Register.com customer whose contact information is obtained by Verio from any source other than Register.com's computers and

ACCA's 2001 ANNUAL MEETING

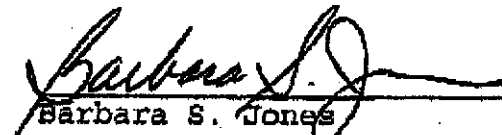
ADDING VALUE

computer networks.

VI. Bond

Pursuant to Fed. R. Civ. P. 65(c), plaintiff is ordered to provide security in the amount of \$250,000.

SO ORDERED:


Barbara S. Jones
UNITED STATES DISTRICT JUDGE

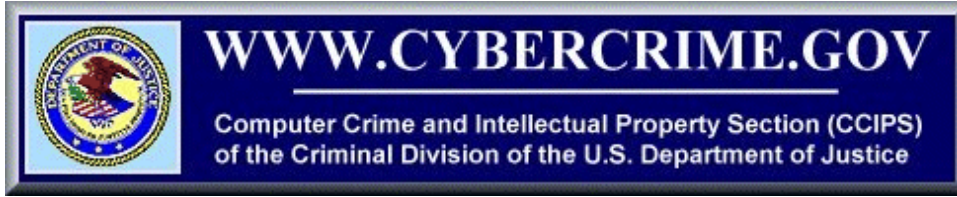
New York, New York
December 8, 2000

Attorney General Ashcroft
Speaks Out on Computer Crime



[Watch the Video](#)
[Read the Text](#)

[Text Only Version](#)



★

Search for: [Hints ...](#)
 Personalized information if you are a...

Want to receive news of updates to the cybercrime.gov website? Send a blank message to: cybercrime-subscribe@topica.com and we will add you to our email list!
[\(Mailing list privacy information\)](#)

Parent or Student

Computer Crime (e.g., hacking): [Policy](#) · [Cases](#) · [Guidance](#) · [Laws](#) · [Documents](#)

Intellectual Property Crime: [Policy](#) · [Cases](#) · [Guidance](#) · [Laws](#) · [Economic Espionage](#) · [Documents](#)

Cybercrime Documents: [Press Releases](#) · [Speeches](#) · [Testimony](#) · [Letters](#) · [Reports](#) · [Manuals](#)

General Information	Other Cybercrime Legal and Policy Issues
<ul style="list-style-type: none"> • How to Report Internet-related Crime • What does CCIPS do? • Inviting CCIPS Attorneys to Speak to You • Law Enforcement Coordination for High-Tech Crimes • Hiring Opportunities with the Computer Crime and Intellectual Property Section • Additional Information on the Department of Justice Web Site Relevant to Legal Issues and Computers or the Internet • Kidspage: Internet Do's and Don'ts • Cyber Ethics • Other Government Initiatives to Combat Cybercrime 	<ul style="list-style-type: none"> • Electronic Commerce: Legal Issues • Encryption and Computer Crime • Federal Code Related to Cybercrime • Intellectual Property Crime • International Aspects of Computer Crime • Privacy Issues in the High-Tech Context • Prosecuting Crimes Facilitated by Computers and by the Internet • Protecting Critical Infrastructures • Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations • Speech Issues in the High-Tech Context

New Updates:

[Former Corning Inc. Employee Charged with Theft of Trade Secrets in Rochester, New York \(July 31, 2001\)](#)

[Orange County, California Computer Hacker Pleads Guilty to Hacking University Computers, Defrauding Western Union \(August 1, 2001\)](#)

[Five Charged in Los Angeles with Fraud In Internet Auctions \(July 31, 2001\)](#)

[Final Draft of Council of Europe Convention on Cybercrime Released: Text and Frequently Asked Questions Document Posted on cybercrime.gov](#)



<http://www.cybercrime.gov/cccases.html>

Computer Crime and Intellectual Property Section (CCIPS)

Computer Intrusion Cases

Below is a summary chart of recently prosecuted computer cases. Many cases have been prosecuted under the computer crime statute, [18 U.S.C. §1030](#). This listing is a representative sample; it is not exhaustive. Click on the name of the case to read a press release about the case.

Computer Crimes Case Chart	Interest Harmed	Est. Dollar Loss	Target	Perpetrator Charged		Geo-graphy	Punishment		Other
				Juvenile	Group		Int'l?	Sentence in Months	
Colloquial Case Name (District) Press Release Date	Confid. (C) Integrity (I) Avail. (A)		Private, Public or Threat to Public Health or Safety						
U.S. v. Diekman II (C.D. CA) August 1, 2001			Private				TBD	TBD	second offense, see Diekman I
U.S. v. Carpenter (D. MD) July 24, 2001	CIA		Private				TBD	TBD	IRS computer sabotage
U.S. v. Ivanov II (C.D. CA) June 20, 2001	CIA		Private			✓	TBD	TBD	Russian hacker, also charged in Conn.
U.S. v. McKenna (D. N.H.) June 18, 2001	CIA	13K	Private				6	13K	disgruntled former employee
U.S. v. Oquendo (S.D. NY) June 13, 2001	CIA	60K	Private				27	96K	first fed. comp. hacking case in S.D. NY
U.S. v. Ivanov (D. Conn.) May 7, 2001	CIA		Private			✓	TBD	TBD	Russian hacker, also charged in Calif.
U.S. v. Sullivan (W.D. NC) April 13, 2001	IA	100K	Private				24	194K	disgruntled former employee
U.S. v. Osowski (N.D. CA) April 4, 2001	C	6.3M	Private				TBD	TBD	Cisco accountant stole stock from company
U.S. v. Morch (N.D. CA) March 21, 2001	C	5K	Private				36 prob.	0	employee theft of proprietary company info.
U.S. v. Ventimiglia (M.D. FL) March 20, 2001	IA	209K	Private				60 prob.	233K	disgruntled GTE employee
U.S. v. Dennis									denial of service attacks

(D. Alaska) January 22, 2001	A		Public				6	5K	against E.D. NY court
U.S. v. Sanford (N.D. TX) December 6, 2000	CIA	45K	Private, Public	✓	✓	✓	60 prob.	45K	"HV2K" hacking group member
U.S. v. Torricelli (S.D. NY) December 1, 2000	CI		Private, Public		✓		TBD	TBD	"#conflict" hacking group member
U.S. v. Diekman I (C.D. CA) November 7, 2000	CI	23K	Public				TBD	TBD	hacked into NASA computers; see Diekman II
U.S. v. "cOmrade" (S.D. FL) September 21, 2000	CA	41K	Public	✓			6	0	first juvenile hacker to receive prison sentence
U.S. v. Gregory (N.D. TX) September 6, 2000	C	1.5M	Private		✓		26	154K	"Global Hell" hacking group member
U.S. v. Zezov et al. (S.D. NY) August 14, 2000	C		Private			✓	TBD	TBD	hacker from Kazakhstan
U.S. v. Lloyd (D. N.J.) May 9, 2000	IA	10M	Private				TBD	TBD	disgruntled former employee
U.S. v. Davis (E.D. WI) March 1, 2000	CA		Public		✓		6	8K	"Global Hell" hacking group member
U.S. v. Iffih (D. Mass) February 23, 2000	CA		Public				TBD	TBD	hacked into federal gov't computers
U.S. v. Miffleton (N.D. TX) December 20, 1999	CI	90K	Private		✓		21	3K	member of "The Darkside Hackers"
U.S. v. Smith (D. N.J.) December 9, 1999	IA	80M	Private, Public			✓	TBD	TBD	"Melissa" virus creator
U.S. v. Alibris (D. Mass) November 22, 1999	C		Private		✓		--	250K	corporation
U.S. v. Burns (E.D. VA) November 19, 1999	CIA	40K	Private, Public			✓	15	36K	designed "Web Bandit" program
U.S. v. Lindsly (N.D. TX) September 16, 1999	C		Private, Public		✓		41	10K	"Phone Masters" hacking group ringleader
U.S. v. Mitnick (C.D. CA) August 9, 1999	CI	1M	Private				68	4K	notorious hacker
U.S. v. Kashpureff (E.D. NY) March 19, 1998	A		Private				TBD	TBD	
U.S. v. Tenebaum (Israel) March 18, 1998	C		Private, Public			✓	12 prob.	17K	Israeli hacked U.S. military computers
U.S. v. An Unnamed Juvenile (D. Mass) March 18, 1998	CA		Threat to Public Health or Safety	✓			TBD	TBD	FAA control tower disabled

Glossary

For the purposes of the computer crime case chart, the following words or phrases are defined.

Interest Harmed - This category refers to the type of interest that was compromised by the computer crime:

Confidentiality - A breach of confidentiality occurs when a person knowingly accesses a computer without

authorization or exceeding authorized access. Confidentiality is compromised when a hacker views or copies proprietary or private information, such as a credit card number or trade secret.

Integrity - A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered or destroyed without authorization. For example, viruses and worms alter source code in order to allow a hacker to gain unauthorized access to a computer.

Availability - A breach of availability occurs when an authorized user is prevented from timely, reliable access to data or a system. A popular example of this is a denial of service attack.

Est. Dollar Loss - The estimated amount of damage that occurs as a result of the computer crime. The estimates in this table are rounded down from figures provided by law enforcement agents on the case.

Target - This category indicates whether the computer crime targeted a private individual or corporation or a public governmental agency. It also indicates whether there was a threat to public health or safety:

Threat to public health or safety occurs when a hacker targets or compromises data or a system within the national critical infrastructure (e.g., power grids, air traffic control, classified government data).

Perpetrator Charged - Indicates whether the defendant is a juvenile or part of an organized group.

Geography -

International - Indicates that the computer crime originated from a foreign country or was conducted on an international scale.

Punishment -

Sentence in months - refers to prison sentence or probation.

Fine, Forfeiture, Restitution - the combined amount that the defendant must pay in fine, forfeiture or restitution.

Other - This column provides interesting or helpful information about the case, such as a defendant's affiliation with an organized hacking group or the nationality of a foreign defendant.

Below is a list of press releases from recently prosecuted computer crime cases, including the cases summarized in the chart above.

- [Orange County, California Computer Hacker Pleads Guilty to Hacking University Computers, Defrauding Western Union \(August 1, 2001\)](#)
- [Lusby, Maryland Man Pleads Guilty to Sabotaging IRS Computers \(July 24, 2001\)](#)
- [Russian Computer Hacker Indicted in California for Breaking into Computer Systems and Extorting Victim Companies \(June 20, 2001\)](#)
- [Hampton, New Hampshire Man Convicted and Sentenced for Hacking into Former Employer's Computer Server \(June 18, 2001\)](#)
- [New York City Computer Security Expert Sentenced to 27 Months' Imprisonment for Computer Hacking and Electronic Eavesdropping \(June 13, 2001\)](#)
- [Russian National Arrested and Indicted in Connecticut for Penetrating U.S. Corporate](#)

Computer Networks, Stealing Credit Card Numbers, and Extorting the Companies by Threatening to Damage Their Computers (May 7, 2001)

- Orange County Computer Hacker Arrested In Scheme to Use Stolen Credit Cards to Make Wire Money Transfers via Western Union (April 18, 2001)
- Former Lance, Inc. Employee, from North Carolina Sentenced to 24 Months and Ordered to Pay \$194,609 Restitution in Computer Fraud Case (April 13, 2001)
- Two Men from California Indicted on Conspiracy to Commit Computer and Wire Fraud via Unauthorized Access to Cisco Stock (April 4, 2001)
- Former Cisco Employee Pleads Guilty to Exceeding Authorized Access to Obtain Information from Cisco's Computer Systems (March 21, 2001)
- Ex-GTE Employee Pleads Guilty to Intentionally Damaging Protected GTE Computers (March 20, 2001)
- New York City Computer Security Expert Convicted by Jury of Computer Hacking and Electronic Eavesdropping (March 7, 2001)
- Former Federal Court Systems Administrator Sentenced for Hacking Into Government Computer System (January 22, 2001)
- Hacker Pleads Guilty in New York City to Hacking into Two NASA Jet Propulsion Lab Computers Located in Pasadena, California (December 1, 2000)
- Orange County Man Pleads Guilty to Hacking into Government Computers (November 7, 2000)
- Texas Man is indicted for Unlawfully Accessing Computers of U.S. Postal Service, State of Texas, and Canadian Department of Defense (October 12, 2000)
- Man Suspected of Hacking into NASA Computers Taken into Federal Custody (September 21, 2000)
- Juvenile Computer Hacker Sentenced to Six Months in Detention Facility (September 21, 2000)
- "Global Hell" Hacker Sentenced to 26 Months Imprisonment (September 6, 2000)
- Three Kazak Men Arrested in London for Hacking into Bloomberg L.P.'s Computer System (August 14, 2000)
- "Darkside Hacker" Sentenced to 21 Months in Prison (July 24, 2000)
- Hacker Group Leader Arrested for Breaking into NASA Computers (July 12, 2000)
- Former Computer Network Administrator Guilty of Unleashing \$10 Million Programming "Timebomb" (May 9, 2000)
- Alaska Man Indicted for Alleged Attack on United States Court Computer Systems (April 19, 2000)
- Second "Global Hell" Hacker Pleads Guilty; Patrick Gregory Faces up to Five Years in Prison for Conspiracy to Commit Telecommunications Fraud and Computer Hacking (April 12, 2000)

- [Chad Davis, "Global Hell" Hacker, Sentenced to Six Months in Prison, Three Years Probation, for Air Force Network Hacks \(March 1, 2000\)](#)
 - [Boston Computer Hacker Charged with Illegal Access and Use of United States Government and Private Systems \(February 23, 2000\)](#)
 - ["Darkside Hacker" Pleads Guilty in Federal Court After Stealing National Internet Company Passwords \(December 20, 1999\)](#)
 - [Creator of 'Melissa' Computer Virus Pleads Guilty in New Jersey to State and Federal Charges \(December 9, 1999\)](#)
 - [Internet Service Provider Charged with Intercepting Customer Communications and Possessing Unauthorized Password Files \(November 22, 1999\)](#)
 - ["Web Bandit" Sentenced to 15 Months Imprisonment, 3 Years of Supervised Release, for Hacking USIA, NATO, Web Sites \(November 19, 1999\)](#)
 - ["Phone Masters" Ringleaders Sentenced to Prison; 41-Month and Two-Year Terms to be Served by Telecommunications Hackers \(September 16, 1999\)](#)
 - [Kevin Mitnick Sentenced to Nearly Four Years in Prison; Computer Hacker Ordered to Pay Restitution to Victim Companies Whose Systems Were Compromised \(August 9, 1999\)](#)
 - [Eugene E. Kashpureff Pleaded Guilty to Unleashing Software on the Internet That Interrupted Service for Tens of Thousands of Internet Users Worldwide \(March 19, 1998\)](#)
 - [Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers \(March 18, 1998\)](#)
 - [Juvenile Computer Hacker Cuts off FAA Tower At Regional Airport -- First Federal Charges Brought Against a Juvenile for Computer Crime \(March 18, 1998\)](#)
 - [Former Chief Computer Network Program Designer Arraigned for Alleged \\$10 Million Computer "Bomb" \(February 17, 1998\)](#)
-

- [More Information on: Computer Crime](#)
- [More Information on: Computer Crime Cases](#)
- [More Information on: Computer Crime Guidance](#)
- [More Information on: Computer Crime Laws](#)
- [More Information on: Computer Crime Documents](#)



<http://www.cybercrime.gov/ivanovIndict.htm>

U.S. Department of Justice

*United States Attorney
District of Connecticut
Connecticut Financial Center
157 Church Street
P.O. Box 1824
New Haven, Connecticut 06510
(203) 821-3700
Fax (203) 773-5376*

**Press Release
For Immediate Release
May 7, 2001**

Russian National Arrested and Indicted for Penetrating U.S. Corporate Computer Networks, Stealing Credit Card Numbers, and Extorting the Companies by Threatening to Damage Their Computers

May 7, 2001

John A. Danaher, III, United States Attorney for the District of Connecticut, announced that on May 3, 2001, a federal grand jury sitting in Bridgeport returned a superseding indictment charging ALEKSEY IVANOV, a/k/a "subbsta," age 20, of Chelyabinsk, Russia, with conspiring with other individuals to commit various computer-related "hacking" offenses. Specifically, IVANOV is charged with conspiring to make unauthorized intrusions into computer systems owned by companies in the United States, including one in Connecticut, transmitting threats to damage those computer systems, extortion, and stealing credit card numbers and merchant account numbers.

IVANOV was arrested on November 10, 2000, when he and an associate traveled to Seattle, Washington to meet with representatives of Invita Security, Inc., an undercover company established by the FBI offices in New Haven, Connecticut, and Seattle, Washington.

The superseding indictment alleges that, from at least December 1999 through March 2000, IVANOV and others conspired to commit various federal crimes, including: accessing without authorization the computer systems owned by Online Information Bureau ("OIB"), Inc., of Vernon, Connecticut, and Good News Internet Service, of Cincinnati, Ohio; transmitting threats to damage these computer systems; attempting to extort money and employment from these companies; and fraudulently possessing fifteen or more unauthorized access devices. The indictment indicates that the conspirators had contacted these companies in early 2000 in an effort to further their extortionate schemes.

The indictment also alleges that IVANOV committed several substantive offenses. Specifically, it alleges that IVANOV accessed a computer owned by OIB without authorization to further an intended fraud and obtain something of value, and that he accessed a computer without authorization for the purpose of

commercial advantage and private financial gain, as well as to further a criminal act. Further, the indictment charges that IVANOV transmitted a threat to cause damage to computers owned by OIB in an attempt to extort money, employment, and property from the company. The indictment also alleges that IVANOV attempted to obtain property from OIB by threatening to access its computer systems, download and steal financial and other data, conduct unauthorized transfers of funds, destroy data, and otherwise damage OIB and its business, unless OIB paid IVANOV money and hired IVANOV as a security consultant. IVANOV is also charged with possession with intent to defraud over 10,000 access devices (i.e., credit card numbers and merchant account numbers).

Since the time of the intrusions and contacts by the conspirators in early 2000, both OIB and Good News have taken and continue to take measures to address the security of their computer systems and customers.

The conspiracy, computer fraud, computer hacking and computer extortion counts in the the indictment carry maximum penalties of up to five years' imprisonment and fines of up to \$250,000. The maximum sentence for the interference with commerce by extortion count is 20 years' imprisonment and a fine of \$250,000; and the credit card fraud charge provides for a maximum penalty of up to 10 years' imprisonment and a fine of \$250,000.

United States Attorney Danaher stressed that an indictment is only a charge and is not evidence of guilt. The defendant is entitled to a fair trial at which it is the Government's burden to prove the defendant's guilt beyond a reasonable doubt.

This case is being investigated by the Federal Bureau of Investigation and is being prosecuted by Assistant United States Attorneys Mark G. Califano and Shawn J. Chen.

###

- [More information on: Ivanov's other indictment in California](#)
- [More information on: Computer Crime](#)
- [More information on: Computer Crime Cases](#)

Want to receive news of updates to the cybercrime.gov website?

Send a blank message to: cybercrime-subscribe@topica.com and we will add you to our email newsletter list.
([Mailing list privacy information](#))

Go to . . . [CCIPS Home Page](#) || [Justice Department Home Page](#)

Last updated June 21, 2001

usdoj-crm/mis/jam



<http://www.cybercrime.gov/MorchPlea.htm>

U.S. Department of Justice

*United States Attorney
Northern District of California
450 Golden Gate Avenue
11th Floor, Federal Building
Box 36055
San Francisco, California 94102
(415) 436-7200
FAX:(415) 436-7234*

**Press Release
For Immediate Release
March 21, 2001**

The United States Attorney's Office for the Northern District of California announced that former Cisco Systems, Inc. employee Peter Morch pled guilty today to exceeding his authorized access to Cisco's computer systems and obtaining information valued at more than \$5,000.

Mr. Morch, a resident of San Francisco and a citizen of Canada and Denmark, was charged in a Criminal Information filed on March 13, 2001, with one count of exceeding authorized access to a protected computer and obtaining information valued at more than \$5,000, in violation of 18 U.S.C. §§ 1030(a)(2)(C) & 1030(c)(2)(B)(iii).

In pleading guilty, Mr. Morch admitted that in September and October 2000 while employed at Cisco Systems-Petaluma, but shortly before his resignation from the company, he intentionally exceeded his authorized access to the computer systems of Cisco Systems by logging into the computer system both as an administrator and under his own username from a workstation belonging to another Cisco software engineer. He did so in order to obtain proprietary information that he knew he was not authorized to have, and he used the other engineer's computer because it had a writable CD drive capable of "burning" CDs.

Mr. Morch admitted that he burned a number of CDs on the other employee's computer, using writable CDs that he obtained from the shelf above his computer monitor, and obtained material that included Cisco proprietary materials relating to both released Cisco products and then-ongoing developmental projects.

According to an affidavit filed in the case Mr. Morch was a team leader for a research and development project pertaining to voice-over and optical networking. The day before he left Cisco, Mr. Morch copied Cisco project ideas, general descriptions, requirements, specifications, limitations of design, and procedures to overcome the design difficulties for a voice-over and optical networking software product. Shortly after, Mr. Morch started working at Calix Networks, a potential competitor with Cisco. According to the affidavit, Mr. Morch copied Cisco's proprietary information onto a Calix laptop and the Calix network. Calix cooperated fully with the investigation.

The sentencing of Mr. Morch is scheduled for June 27, 2001 at 2:30 pm before U.S. District Court Judge Maxine M. Chesney in San Francisco. The maximum statutory penalty for each count in violation of 18 U.S.C. §§ 1030(a)(2)(C) & 1030(c)(2)(B)(iii) is five years imprisonment and a fine of \$250,000.

However, the actual sentence will be dictated by the Federal Sentencing Guidelines, which take into account a number of factors, and will be imposed in the discretion of the Court.

The prosecution is the result of a six-month investigation by special agents of the Federal Bureau of Investigation. Joseph E. Sullivan and Jonathan Howden fo the Computer Hacking and Intellectual Property (CHIP) Unit are the Assistant U.S. Attorneys who prosecuted the case.

A copy of this press release and key court documents filed in the case may also be found on the U.S. Attorney's Office's website at www.usaondca.com.

All press inquiries to the U.S. Attorney's Office should be directed to Assistant U.S. Attorney Matthew J. Jacobs at (415)436-7181.

###

- [More information on: Morch's Arrest](#)
- [More information on: Computer Intrusion Cases](#)
- [More information on: Computer Crime Documents](#)

Go to . . . [CCIPS Home Page](#) || [Justice Department Home Page](#)

Last updated May 03, 2001
usdoj-crm/mis/jam



<http://www.cybercrime.gov/OQUENDOconvict.htm>

U.S. Department of Justice
United States Attorney
Southern District of New York
MARVIN SMILON, HERBERT HADAD
PUBLIC INFORMATION OFFICE
(212) 637-2600

ROBERT R. STRANG
(212) 637-2214
JOSHUA G. BERMAN
(212) 637-2334

FBI
JOSEPH A. VALIQUETTE
(212) 384-2715
JAMES M. MARGOLIN
(212) 384-2720

Press Release
For Immediate Release
March 7, 2001

**New York City Computer Security Expert Convicted by Jury of Computer Hacking
and Electronic Eavesdropping**

MARY JO WHITE, the United States Attorney for the Southern District of New York, and BARRY W. MAWN, Assistant Director in Charge of the New York FBI Office, announced that JESUS OQUENDO was convicted in Manhattan federal court today on charges of computer hacking and electronic eavesdropping in the first ever federal computer hacking trial in the Southern District of New York. OQUENDO was convicted following a one-week trial in a case developed and investigated by the Computer Crime Squad of the New York Office of the FBI.

According to the evidence at the trial, OQUENDO worked as a computer security specialist at a company called Collegeboardwalk.com during the first half of 2000. Collegeboardwalk.com shared office space and computer network with one of its investors, Five Partners Asset Management LLC ("Five Partners"), a venture capital company based in Manhattan. As a result of this access, OQUENDO altered the start-up commands on the Five Partner's network to send automatically the password file from the Five Partner's system to him at an e-mail account he controlled each time the Five Partner's computer system was rebooted.

According to the evidence at trial, after Collegeboardwalk.com failed as a business, OQUENDO began accessing the Five Partner's network remotely over the Internet through a secure shell account he illegally installed on the victim's network. He also began storing hacking programs and other information in a computer directory that was no longer being used by Five Partners. Additionally, in August 2000, he secretly installed what is known as a "sniffer" program that intercepted and recorded electronic traffic on the Five Partner's network, including unencrypted passwords. This sniffer program was then programmed to e-mail these intercepted communications to OQUENDO each morning at 4 A.M. at a second secret email account that he had registered under a false name.

By installing this sniffer program, OQUENDO was able to take advantage of the fact that one of the legitimate users on the Five Partner's network also had a computer account on a second victim, RCS Computer Experience ("RCS"), which is also based in Manhattan, and which specializes in selling computer equipment at retail locations and over the Internet to individuals located throughout the United States. OQUENDO's sniffer program on the Five Partner's computer intercepted this legitimate user's password when the user logged into the RCS network to check the database file RCS maintained to record and track all of its sales and inventory (the "RCS Database").

The trial evidence showed that on August 2 and 3, 2000, OQUENDO connected to the Internet from his home and again remotely entered the Five Partner's network. Using the legitimate user's password, OQUENDO then broke into the RCS network. While on the RCS network, OQUENDO sent the RCS password file to his secret e-mail account, sought to install a similar sniffer program on the RCS system, and issued a series of commands that deleted the entire RCS database, costing RCS approximately \$60,000 to repair. Finally, OQUENDO left the victim a taunting message on its network: "Hello, I have just hacked into your system. Have a nice day."

Ms. WHITE stated: "This case demonstrates that defendants cannot maliciously damage the property of others and eavesdrop on their internal communications and expect to hide behind the anonymity of the Internet. The privacy of individuals will be protected and computer hacking will not be tolerated."

United States District Judge LORETTA PRESKA, who presided at the trial, scheduled June 12, 2001, for the sentencing of OQUENDO. OQUENDO faces a maximum sentence of five years in prison, a maximum fine of \$250,000, or twice the gross gain or loss resulting from the crime, on each of the two charges in the Indictment -- illegal computer intrusion, or hacking, and electronic eavesdropping. OQUENDO, 27, lives in Queens, New York.

Assistant United States Attorneys ROBERT R. STRANG and JOSHUA G. BERMAN are in charge of the prosecution.

01-34

###

- [More information on: Computer Crime Documents](#)
- [More information on: Computer Intrusion Cases](#)

Go to . . . [CCIPS Home Page](#) || [Justice Department Home Page](#)

Last updated March 8, 2001
usdoj-crm/mis/jam



<http://www.cybercrime.gov/reporting.htm>

Computer Crime and Intellectual Property Section (CCIPS)

How to Report Internet-Related Crime

Internet-related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement.

Some federal law enforcement agencies that investigate domestic crime on the Internet include: the [Federal Bureau of Investigation \(FBI\)](#), the [United States Secret Service](#), the [United States Customs Service](#), the [United States Postal Inspection Service](#) and the [Bureau of Alcohol, Tobacco and Firearms \(ATF\)](#). Each of these agencies has offices conveniently located in every state to which crimes may be reported. Contact information regarding these local offices may be found in local telephone directories. In general, federal crime may be reported to the local office of an appropriate law enforcement agency by a telephone call and by requesting the "Duty Complaint Agent."

Each law enforcement agency also has a headquarters (HQ) in Washington, D.C., which has agents who specialize in particular areas. For example, the FBI and the U.S. Secret Service both have headquarters-based specialists in computer intrusion (i.e., computer hacker) cases. In fact, the FBI HQ hosts an interagency center, the [National Infrastructure Protection Center \(NIPC\)](#), created just to support investigations of computer intrusions. The NIPC Watch number for reporting computer crimes is 202-323-3205. The U.S. Secret Service's Electronic Crimes Branch may be reached at 202-406-5850. The FBI and the Customs Service also have specialists in intellectual property crimes (i.e., copyright, software, movie, or recording piracy, trademark counterfeiting). Customs has a nationwide toll-free hotline for reporting at 800-BE-ALERT, or 800-232-2538.

The FBI investigates violations of federal criminal law generally. Certain law enforcement agencies focus on particular kinds of crime. Other federal agencies with investigative authority are the [Federal Trade Commission](#) and the [U.S. Securities and Exchange Commission](#).

To determine some of the federal investigative law enforcement agencies that may be appropriate for reporting certain kinds of crime, please refer to the following table:

Type of Crime	Appropriate federal investigative law enforcement agencies
Computer intrusion (i.e. hacking)	FBI local office; NIPC (202-323-3205); U.S. Secret Service local office
Password trafficking	FBI local office; NIPC (202-323-3205); U.S. Secret Service local office
Copyright (software, movie, sound recording) piracy	FBI local office; if imported, U.S. Customs Service local office (800-BE-ALERT, or 800-232-2538)
Theft of trade secrets	FBI local office
Trademark counterfeiting	FBI local office; if imported, U.S. Customs Service local office (800-BE-ALERT, or 800-232-2538)
Counterfeiting of currency	U.S. Secret Service local office; FBI local office
Child Pornography or Exploitation	FBI local office; if imported, U.S. Customs Service local office (800-BE-ALERT, or 800-232-2538)
Child Exploitation and Internet Fraud matters that have a mail nexus	U.S. Postal Inspection local office
Internet fraud	The Internet Fraud Complaint Center ; FBI local office; U.S. Secret Service local office; Federal Trade Commission; if securities fraud, Securities and Exchange Commission
Internet harassment	FBI local office
Internet bomb threats	FBI local office; ATF local office
Trafficking in explosive or incendiary devices or firearms over the Internet	FBI local office; ATF local office

The Internet Fraud Complaint Center (IFCC)

The IFCC is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). This Web site provides a mechanism for victims of Internet fraud to report on-line fraud to the appropriate law enforcement and regulatory authorities.

- [The Internet Fraud Complaint Center](#)

Other Government Initiatives to Combat Cybercrime

- [The Critical Infrastructure Assurance Office \(CIAO\)](#)
- [The National White Collar Crime Center \(NWCCC\)](#)
- [The President's Commission on Critical Infrastructure Protection \(PCCIP\)](#)
- [National Aeronautics and Space Administration \(NASA\)](#)

Go to . . . [CCIPS home page](#) || [Justice Department home page](#)

Updated page January 2, 2001
usdoj-crm/mis/mdf



<http://www.cybercrime.gov/ccips.html>

Computer Crime and Intellectual Property Section (CCIPS)

What does CCIPS do?

The Computer Crime and Intellectual Property Section ("CCIPS") attorney staff consists of about two dozen lawyers who focus exclusively on the issues raised by computer and intellectual property crime. Section attorneys advise federal prosecutors and law enforcement agents; comment upon and propose legislation; coordinate international efforts to combat computer crime; litigate cases; and train all law enforcement groups. Other areas of expertise possessed by CCIPS attorneys include encryption, electronic privacy laws, search and seizure of computers, e-commerce, hacker investigations, and intellectual property crimes.

A large part of CCIPS' strength derives from the diverse skills and the wide variety of experiences its lawyers have had before joining the Section. Before joining CCIPS, its attorneys have been computer scientists, state and federal prosecutors, and associates and partners at law firms. A substantial number of CCIPS' attorneys have received degrees in computer science, engineering, or other technical fields; about half came to CCIPS with prior government service. CCIPS began as the Computer Crime Unit of the former General Litigation and Legal Advice Section of DOJ's Criminal Division in 1991. CCIPS became a Section of the Criminal Division in 1996.

As Attorney General Janet Reno noted in her testimony on "Cybercrime" before the United States Senate Committee on Appropriations on February 16, 2000:

"The cornerstone of our prosecutor cybercrime program is the Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. CCIPS was founded in 1991 as the Computer Crime Unit, and was elevated into a Section in 1996. With the help of this Subcommittee, CCIPS has grown from five attorneys in January of 1996, to eighteen attorneys today. CCIPS works closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators" (CTCs) in U.S. Attorney's Offices around the country. Each CTC is given special training and equipment, and serves as the district's expert in computer crime cases.

"The responsibility and accomplishments of CCIPS and the CTC program include:

Litigating Cases:

"CCIPS attorneys have litigating responsibilities, taking a lead role in some computer crime and intellectual property investigations, and a coordinating role in many national investigations, such as the denial of service investigation that is ongoing currently. As law enforcement matures into the Information Age, CCIPS is a central point of contact for investigators and prosecutors who confront investigative problems with emerging technologies. This year, CCIPS assisted with wiretaps over computer networks, as well as traps and traces that require agents to segregate Internet headers from the content of the

packet. CCIPS has also coordinated an interagency working group consisting of all the federal law enforcement agencies, which developed guidance for law enforcement agents and prosecutors on the many problems of law, jurisdiction, and policy that arise in the online environment.

"Working with the U.S. Attorney's Office in the District of New Jersey and the FBI, as well as with state prosecutors and investigators, CCIPS attorneys helped ensure that David Smith, the creator of the Melissa virus, pled guilty to a violation of the computer fraud statute and admitted to causing damages in excess of \$80 million.

"CCIPS is also a key component in enforcing the "Economic Espionage Act," enacted in 1996 to deter and punish the theft of valuable trade secrets. CCIPS coordinates approval for all the charges under the theft of trade secret provision of this Act, and CCIPS attorneys successfully tried the first jury case ever under the Act, culminating in guilty verdicts against a company, its Chief Executive Officer, and another employee.

"The CTCs have been responsible for the prosecution of computer crimes across the country, including the prosecution of the notorious hacker, Kevin Mitnick, in Los Angeles, the prosecution of the hacker group "Global Hell" in Dallas, and the prosecution of White House web page hacker, Eric Burns, in Alexandria, Virginia.

Training

"CCIPS has spearheaded efforts to train local, state, and federal agents and prosecutors on the laws governing cybercrime, and last year alone gave over 200 presentations to a wide variety of audiences. In addition, CTCs across the country are training prosecutors and agents in their districts in a variety of fora.

"CCIPS also chairs the National Cybercrime Training Partnership (NCTP), a groundbreaking consortium of federal, state, and local entities dedicated to improving the technical competence of law enforcement in the information age. The NCTP has made great strides in creating a comprehensive prototype training curriculum for agents and prosecutors in a full range of infotech topics.

International

"The borderless nature of computer crime requires a large role for CCIPS in international negotiations. CCIPS chairs the G-8 Subgroup on High-tech Crime, which has established a 24 hours a day/7 days a week point of contact with 15 countries for mutual assistance in computer crime. CCIPS also plays a leadership role in the Council of Europe Experts' Committee on Cybercrime, and in a new cybercrime project at the Organization of American States.

Infrastructure Protection, Policy and Legislation

"CCIPS provided expert legal and technical instruction and advice for exercises and seminars to senior personnel on information warfare, infrastructure protection, and other topics for the Department of Defense, the National Security Agency, the Central Intelligence Agency, and others. Further, the Naval War College invited CCIPS to give a featured presentation at a high-level, invitation-only conference on cyberwarfare and international law. CCIPS also led the Department's efforts to counter cyberterrorism through its work on PDD-63, the Five-Year Counterterrorism Strategy, its support to the National Infrastructure Protection Center.

"CCIPS works on a number of policy issues raised at the intersection of law and technology. CCIPS attorneys meet regularly with a number of industry groups to discuss

issues of common concerns, and helped establish the Cybercitizen Partnership in cooperation with high-tech industries to help identify industry expertise which may be needed in a complex investigation, to initiate personnel exchanges and to help safeguard our children.

"CCIPS attorneys propose and comment on legislation that affects their high-tech mission.

"Other Sections of the Criminal Division – including the Fraud Section, the Child Exploitation and Obscenity Section, and the Terrorism and Violent Crime Section – are responding as crimes within their areas of expertise move online."

The complete text of the Attorney General's speech may be accessed via the link below:

- [Testimony by Attorney General Janet Reno before the United States Senate Committee on Appropriations \(February 16, 2000\)](#)

Go to . . . [CCIPS home page](#) || [Justice Department home page](#)

Updated page February 24, 2000
usdoj-crm/mis/mdf



<http://www.cybercrime.gov/ipcases.htm>

Computer Crime and Intellectual Property Section (CCIPS)

Intellectual Property Cases

Many cases have been prosecuted under the intellectual property statutes, such as [18 U.S.C. §§2318, 2319, and 2320](#). Below is a summary chart of recently prosecuted intellectual property cases. This listing is a representative sample; it is not exhaustive. Click on the name of the case to read a press release about the case

Computer Crimes Case Chart	Violation	Film, Music	Soft-Hardware	Est. Loss	Perpetrator charged-group?	Punishment		Other
Colloquial Case Name (District) Press Release Date						Incarceration or probation (months)	Fine Forfeiture Restitution	
U.S. v. Sklyarov (N.D. CA) July 17, 2001	DMCA		✓		✓	TBD	TBD	
U.S. v. Ngo (D. Utah) July 17, 2001	Trademark	✓			✓	10	0	
U.S. v. Tzeng (C.D. CA) June 15, 2001	Trademark		✓			TBD	TBD	
U.S. v. Gray (C.D. Ill.) June 14, 2001	Unauth. use of communications	✓			✓	TBD	TBD	Satellite TV Cards
U.S. v. Howland (D. Md.) June 13, 2001	Copyright		✓			TBD	TBD	
U.S. v. Bailey (S.D. Ind.) June 1, 2001	Copyright		✓	1.4M	✓	18	0	
U.S. v. "Pirates with Attitudes" (N.D. IL) May 15, 2001	Copyright		✓	1M	✓	TBD	TBD	NET Act Case
U.S. v. Stockton (D. OR) April 16, 2001	Copyright		✓	490K		12	100K	
U.S. v. Rivera (D. NJ) April 4, 2001	Unauth. use of communications	✓				TBD	TBD	Satellite TV Cards
U.S. v. Kislyansky (N.D. Ohio) April 3, 2001	Copyright		✓	15.5M	✓	18	570K	
U.S. v. Reeves (W.D. WA) March 23, 2001	Copyright	✓	✓			TBD	TBD	
U.S. v. Xie (D. MD) March 16, 2001	Copyright		✓	47K	✓	TBD	TBD	
U.S. v. Dipadova & Ford (N.D. SC) March 7, 2001	Trademark				✓	TBD	TBD	

ACCA's 2001 ANNUAL MEETING

ADDING VALUE

U.S. v. Ding (N.D. CA) March 6, 2001	Money Laundering		✓	160K		TBD	TBD	
U.S. v. Herr (C.D. CA) February 26, 2001	Copyright		✓	20K		14	0	
U.S. v. Hawkins (N.D. OH) February 23, 2001	Unauth. use of communications	✓				TBD	TBD	
U.S. v. Fastlane (N.D. IL) February 16, 2001	Copyright		✓	1M	✓	TBD	TBD	NET Act Case
U.S. v. Kennedy (D. RI) February 15, 2001	Unauth. use of communications	✓				14	0	
U.S. v. Baltutat (E.D. MI) January 30, 2001	Copyright		✓			36 prob.	✓	NET Act Case
U.S. v. Bynum (D. MD) January 29, 2001	Copyright	✓				24	460K	
U.S. v. Lirola et al (N.D. CA) January 5, 2001	Copyright		✓	900K	✓	TBD	900K Chevy Corvette & website	
U.S. v. Spatafore (N.D. CA) December 15, 2000	Copyright	✓				TBD	TBD	NET Act Case
U.S. v. Mou (C.D. CA) December 4, 2000	Trademark		✓	600K		12	660K	
U.S. v. Flick (N.D. OH) August 16, 2000	Unauth. use of communications	✓		250K		6	250K	
U.S. v. Poulson, Walid, Bauer, Angell, et al. (many districts) August 8, 2000	Unauth. use of communications	✓				TBD	TBD	
U.S. v. Hanafy et al. (N.D. TX) July 18, 2000	Trademark				✓	TBD	700K	Health / Safety threat
U.S. v. Platinum. Wu. Pham (E.D. NY) June 22, 2000	Trademark		✓		✓	TBD	TBD	
U.S. v. Antaramian & Hariri (C.D. CA) June 2, 2000	Copyright		✓		✓	TBD	TBD	
U.S. v. Marino et al. (S.D. CA) April 12, 2000				10M+	✓	41	10M	
U.S. v. Kablin (MA) February 23, 2000	Trademark					6	85K	
U.S. v. Thornton (DC) December 22, 1999	Copyright		✓	10K		60 prob.	✓	NET Act Case
U.S. v. Lee (HI) December 9, 1999	Trademark					10	0	
U.S. v. Levy (OR) November 23, 1999	Copyright	✓	✓	70K		24 prob.	0	NET Act Case
U.S. v. Desktop Sales, Inc. (N.D. IL) November 19, 1998	Trademark		✓	1.1M	✓	-	3.3M	

Glossary

For the purposes of the computer crime case chart, the following words or phrases are defined.

Violation – This category lists the section/s of the U.S.C. used in the defendant's indictment or conviction.

Trademark – 18 U.S.C. § 2320 bans trafficking in counterfeit goods or services.

Copyright – 18 U.S.C. § 2318 and § 2319 prohibit, respectively, trafficking in counterfeit labels and documentation, and infringing a copyright.

Unauthorized use of communications – 47 U.S.C. § 605 bans the unauthorized use of telecommunications services (such as satellite television programming) as well as the distribution of devices that enable such unauthorized use.

Digital Millenium Copyright Act – 17 U.S.C. § 1201 prohibits the circumvention of copyright protection systems.

Film, Music - Whether or not the film and music industry was affected by the IP crime. For example, a case involving distribution of bootleg copies of a Star Wars movie would be indicated with a checkmark in the "Film, Music" column, as would a case involving "cracked" DirecTV access cards.

Soft-/Hard-ware - Whether or not the software and hardware industry was affected by the IP crime. A case involving distribution of Adobe software on a WareZ site, or manipulated and remarked computer chips, would be indicated with a checkmark in the "Soft-/Hard-ware" column.

Estimated loss - The estimated amount of damage that occurs as a result of the IP crime. The estimates in this table are rounded down from figures provided by law enforcement agents on the case.

Perpetrator Charged - Indicates whether the defendant was allegedly operating within a larger, organized framework.

Punishment -

Incarceration or probation (months) - refers to number of months of incarceration (prison, home confinement) imposed on the defendant, or, if no incarceration was imposed, the number of months of probation.

Fine, Forfeiture, Restitution - the combined amount that the defendant must pay in fines, restitution and forfeiture.

Other - This column may be used for mentioning unusual aspects of the case.

A. Press Releases for Intellectual Property Rights Cases

Year 2001

- [Russian Man Charged in California under Digital Millenium Copyright Act with Circumventing Adobe eBook Reader \(July 17, 2001\)](#)
- [West Valley Man Sentenced to 10 Months in Federal Prison for Trafficking in Counterfeit Video Tapes \(July 17, 2001\)](#)
- [San Gabriel Valley, California Woman Arrested for Trafficking in Counterfeit Microsoft Computer Programs \(June 15, 2001\)](#)
- [Rantoul, Illinois Men Guilty in Satellite T.V. Sting \(June 14, 2001\)](#)
- [Bethesda, Maryland Man Pleads Guilty to Copyright Infringement \(June 13, 2001\)](#)

- [Second Man Sentenced in Indiana for Trafficking in Counterfeit Computer Software \(June 1, 2001\)](#)
- [Software Pirate Guilty of Copyright Infringement Under NET Act \(May 15, 2001\)](#)
- [Former Eugene, Oregon, Resident Sentenced to Prison for Criminal Copyright Infringement \(April 16, 2001\)](#)
- [Leonid and Michael Kislyansky Sentenced in Cleveland, Ohio on Organized Crime Software Piracy Case \(April 3, 2001\)](#)
- [Bergenfield, New Jersey Man Admits Selling Pirated Satellite TV Access Cards \(April 3, 2001\)](#)
- [Aberdeen, Washington Woman Arrested on Criminal Copyright Infringement Charges for Selling Unauthorized Copies of Sony Games and Movies Over the Internet \(March 23, 2001\)](#)
- [Two Former Maryland Residents Plead Guilty To Selling Copyrighted Computer Software Online \(March 16, 2001\)](#)
- [Operators of www.fakegifts.com Web Site Plead Guilty in South Carolina to Selling Counterfeit Luxury Goods Over the Internet \(March 7, 2001\)](#)
- [Two Indicted and Arrested in South Carolina for Trafficking in Counterfeit Luxury Goods over www.fakegifts.com Web site \(January 29, 2001\)](#)
- [Silicon Valley Businessman Pleads Guilty to Hiding Proceeds of Sales Counterfeit Computer Software \(March 6, 2001\)](#)
- [Man Pleads Guilty to Selling Counterfeit Microsoft Software\(February 26, 2001\)](#)
- [Former Police Lieutenant Sentenced for Distributing and Selling Satellite TV Interception Devices \(February 23, 2001\)](#)
- [Nine Indicted in Chicago in \\$1 Million "Fastlane" Software Piracy Conspiracy \(Feb. 16, 2001\)](#)
- [Thomas Kennedy was caught in Operation Smartcard.net, a nationwide "sting" set up by the Customs Service \(February 15, 2001\)](#)
- [Former Journalism Student Pleads Guilty to Software Copyright Infringement \(January 30, 2001\)](#)
- [Man Sentenced in Michigan for Offering Software Programs for Free Downloading on "Hacker Hurricane" Web site \(January 30, 2001\)](#)
- [Temple Hills Man Sentenced for Conspiracy to Distribute 23,892 Bootleg Videocassettes and 58,975 Compact Discs \(January 29, 2001\)](#)
- [Two Defendants Plead Guilty to Distribution and Sales of Counterfeit Copyrighted Computer Software and Forfeit Ownership of a Domain Name \(January 5, 2001\)](#)

Year 2000

- [Man Pleads Guilty to Internet Piracy of Star Wars Film \(December. 15, 2000\)](#)
- [Woman Sentenced to One Year in Prison for Trafficking in Counterfeit](#)

Computer Software (December 4, 2000)

- Ohio Man Sentenced on Conviction of Illegally Distributing Satellite Television Access Cards (November 16, 2000)
- Police Lieutenant Charged With selling and Distributing Satellite TV Interception Devices (October 18, 2000)
- Texas Woman Pleads Guilty to Trafficking Counterfeit Microsoft Software (September 25, 2000)
- Man Charged with Internet Piracy of Star Wars Film (September 20, 2000)
- Ohio Man Charged with Illegally Distributing Satellite Television Access Cards (August 18, 2000)
- Undercover Customs Operation Results In Charges And Pleas in Connection With Stolen Satellite Television (August 8, 2000)
- Federal Jury Convicts Four Individuals on Charges of Trademark Counterfeit, Conspiracy for Reselling Infant Formula (July 18, 2000)
- New York Electronic Crimes Task Force Arrests Two Individuals on Charges of Trafficking in Counterfeit Computer Chips and Software (June 22, 2000)
- Two Californians Arrested by FBI for Counterfeiting High-Security Computer Chips Used in Arcade Video Games (June 2, 2000)
- Texas Woman Charged with Running Ring That Trafficked in Counterfeit Software (May 23, 2000)
- U.S. Indicts 17 in Alleged International Software Piracy Conspiracy (May 4, 2000)
- Three Year Investigation Reveals Black Market Dealings in Counterfeit Sports and Celebrity Memorabilia (April 12, 2000)
- Norwood Man Pleads Guilty to Selling Counterfeit Clothing and Accessories (February 23, 2000)

Year 1999

- Eric Thornton Pleads Guilty to Charges Filed under the "No Electronic Theft" (Net) Act for Unlawful Distribution of Software on the Internet (December 22, 1999)
- Kent Aoki Lee Charged by Federal Grand Jury with Wire Fraud, Trademark Violations, and Selling Viagra over the Internet Without a Prescription (December 9, 1999)
- Defendant Sentenced for First Criminal Copyright Conviction Under the "No Electronic Theft" (NET) Act for Unlawful Distribution of Software on the Internet (November 23, 1999)
- First Criminal Copyright Conviction Under the "No Electronic Theft" (NET) Act for Unlawful Distribution of Software on the Internet (August 20, 1999)

Year 1998

- [Computer company pleads guilty and agrees to pay \\$3.3 million in fines and restitution for violation of IBM trademark \(November 19, 1998\)](#)

B. Operation "Counter Copy"

In early May, the Department of Justice and the Federal Bureau of Investigation released the first results of a nationwide law enforcement effort to crack down on trademark and copyright fraud, which is estimated to cost American businesses millions of dollars each year and cheat unsuspecting consumers who purchase counterfeit products. As a result of the joint effort, called Operation "Counter Copy," 35 indictments were returned since the beginning of April for copyright or trademark infringement. More information about Operation Counter Copy, including a press release and brief summaries of the cases, are available via the links below.

- [Summaries of Cases](#)
- [Press Release](#)

Click here for more information on:

- [Intellectual Property Policy and Programs](#)
- [Intellectual Property Cases](#)
- [Prosecuting Intellectual Property Crimes Guidance](#)
- [Criminal Intellectual Property Laws](#)
- [Economic Espionage Act](#)
- [Intellectual Property Documents](#)

Go to . . . [CCIPS home page](#) || [Justice Department home page](#)

Updated page August 2, 2001
usdoj-crm/mis/jam

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,
Plaintiff,

V.

KEVIN DAVID MITNICK, and LEWIS
DEPAYNE,
Defendants.

CR96- 881

INDICTMENT

(18 U.S.C. S 1029: Possession
of Unauthorized Access
Devices; 18 U.S.C.
S 1030(a)(4): Computer Fraud;
18 U.S.C. 1030(a)(5):
Causing Damage To Computers;
18 U.S.C. 1343: Wire Fraud;
18 U.S.C. 2511:
Interception of Wire or
Electronic Communications;
18 U.S.C. 2(a): Aiding and
Abetting; 18 U.S.C. 2(b):
Causing an Act to be Done]

The Grand Jury charges:

COUNTS ONE THROUGH FOURTEEN

(18 U.S.C. 1343, 2a, 2b]

INTRODUCTION

1. Beginning in or around June 1992 and continuing until February 1995, defendant KEVIN DAVID MITNICK, aided and abetted by defendant LEWIS DEPAYNE and others known and unknown to the Grand Jury, carried out a scheme to defraud, and to obtain property by means of false pretenses, representations and promises, by: (a) obtaining unauthorized access to computers belonging to numerous computer software and computer operating Systems manufacturers, cellular telephone manufacturers, Internet Service Providers, and educational institutions; and (b) stealing, copying, and misappropriating proprietary computer software belonging to the companies described below (collectively referred to as "the victim companies").

THE VICTIM COMPANIES

2. Motorola, Inc. ("Motorola") is an electronics and computer software manufacturer headquartered in Schaumburg, Illinois. Among other things, Motorola designs and manufactures computer software used to operate cellular telephones manufactured by Motorola. Motorola spends substantial sums in developing its computer software and maintains it as highly confidential proprietary information. In some instances, Motorola licenses its computer software for a fee.

3. Nokia Mobile Phones, Ltd. ("Nokia") is a mobile telephone manufacturer headquartered in Finland. Nokia also has offices in the United Kingdom and in the United States. Among other things, Nokia designs and manufactures computer software used to operate its mobile telephones. Nokia spends substantial sums in developing its computer software and maintains it as highly confidential proprietary information.

4. Fujitsu, Limited is an electronics and computer software company headquartered in Japan. Fujitsu America, Inc and Fujitsu Network Transmission Services, Inc. ("FNTS") are American subsidiaries of Fujitsu, Limited with offices in the United States (Fujitsu, Limited, Fujitsu America and FNTS are collectively referred to as "Fujitsu"). Among other things, Fujitsu designs and manufactures computer software used to operate cellular telephone networks. Fujitsu spends substantial sums in developing its computer software and maintains it as highly confidential proprietary information. In some instances, Fujitsu licenses its proprietary software for a fee.

5. Novell Inc. ("Novell") is a computer software company headquartered in Provo, Utah, with offices throughout the United States. Among other things, Novell designs and manufactures proprietary computer software. Novell spends substantial sums developing its computer software and maintains it as highly confidential proprietary information. Novell also licenses its proprietary software for a fee.

6. NEC, Limited is an electronics and computer software manufacturer headquartered in Japan. NEC America, Inc. is the American subsidiary of NEC, Limited,

headquartered in Irving, Texas, with offices throughout the United States (NEC, Limited and NEC America, Inc. are hereafter collectively referred to as "NEC"). Among other things, NEC designs and manufactures computer software used to operate cellular telephone networks. NEC spends substantial sums in developing its computer software and maintains it as highly confidential proprietary information. NEC also licenses its proprietary software for a fee.

7. Sun Microsystems, Inc. ("Sun") is a computer manufacturer headquartered in Mountain View, California, with offices throughout the United States and Canada. Among other things, Sun designs and manufactures software for computer operating systems. Sun spends substantial sums in developing its computer software and maintains it as highly confidential proprietary information. Sun also licenses its proprietary software for a fee.

THE INTERNET SERVICE PROVIDERS AND EDUCATIONAL INSTITUTIONS

8. Colorado SuperNet ("CSN.") is an Internet Service Provider headquartered in Denver, Colorado. For a fee, CSN provides customers with computer user accounts that customers may use to access other computer systems on the Internet.

9. Netcom On-Line Services ("Netcom") is an Internet Service Provider headquartered in San Jose, California. For a fee, Netcom provides customers with computer user accounts that customers may use to access other computer systems on the Internet.

10. The University of Southern California ("USC") is an educational institution located in Los Angeles, California. Among other things, USC owns, maintains and operates a number of computer8 for the authorized use of USC faculty, students, contractors, administrators and other authorized personnel. USC also provides internet access to authorized users.

THE SCHEME TO OBTAIN THE VICTIM COMPANIES' PROPRIETARY COMPUTER SOFTWARE

11. Between June 1992 and February 1995, defendant MITNICK, aided and abetted by defendant DEPAYNE and others known and unknown to the Grand Jury, in the Central District of

California and elsewhere, carried out a scheme to fraudulently obtain proprietary computer software belonging to the victim companies. Defendant MITNICK, aided and abetted by defendant DEPAYNE and others known and unknown to the Grand Jury, carried out the scheme, in part, as follows:

12. During the time relevant to this indictment, the victim companies developed computer software that they maintained as highly confidential proprietary information. The proprietary computer software was stored in computers belonging to the victim companies.

13. In order to circumvent computer security measures employed by the victim companies to safeguard their proprietary computer software, defendant MITNICK needed to obtain user accounts and corresponding passwords on victim companies' computers so that he could then access these computers as part of the scheme to obtain the victim companies' proprietary software.

14. Defendant MITNICK, aided and abetted by defendant DEPAYNE and others known and unknown to the Grand Jury, obtained confidential computer user accounts and corresponding secret passwords on victim companies' computers through the following means.

15. Defendants MITNICK and DEPAYNE, using aliases, deceived employees of the victim companies into providing them with user accounts and corresponding passwords by falsely representing that they were employees of the victim companies. In some instances, defendant MITNICK, using aliases, called the computer department of a victim company, posed as an employee of the victim company working on a special project, and then deceived computer department personnel into creating a new user account on the victim company's computers. Often, defendant MITNICK asked the computer department personnel for a user account which he could access from remote locations by dialing into the victim company's computers using a telephone and a computer "modem" (a device that allows computers to communicate over telephone lines). On other occasions, defendant MITNICK called employees of a victim company, impersonated computer department personnel, and then deceived the unsuspecting employees into providing him with their secret computer passwords.

16. To conceal his identity and avoid detection when making these fraudulent telephone calls, defendant MITNICK used stolen electronic serial numbers and mobile identification numbers to create numerous "clone" cellular telephones that allowed him to place unauthorized cellular telephone

calls that were billed to, and hence appeared to have been placed by, legitimate cellular telephone subscribers.

17. Defendant MITNICK, aided and abetted by others known and unknown to the Grand Jury, obtained other user accounts and corresponding passwords for victim companies' computers by: (a) using a computer program that intercepted and captured user account information and passwords of authorized users as they logged onto the computers of a victim company; (b) copying "encrypted" (or coded) electronic password files maintained on a victim company's computer to his own computer and then using computer software programs to "decrypt" (or decode) the information contained in the password files so that the passwords could be identified and used; and (c) intercepting or reading private electronic mail ("E-Mail") communications containing user account, password, and computer security information.

18. Defendant MITNICK used the fraudulently obtained user accounts and corresponding passwords to gain unauthorized access to the computers of the victim companies, and to computers belonging to Internet Service Providers and educational institutions. In order to conceal his identity, and to further avoid detection, defendant MITNICK used "clone" cellular telephones, computer modems, Internet connections from other victim companies, or stolen long distance calling card numbers to access the computers of the victim companies, the Internet Service Providers, and the educational institutions.

19. Once he obtained initial unauthorized access to a computer by using fraudulently obtained user accounts and passwords, defendant MITNICK circumvented internal computer security measures installed on victim companies' computers for the purpose of preventing regular users from accessing information stored in protected parts of the computer systems or in other authorized user's accounts. Specifically, defendant MITNICK ran unauthorized computer "hacking" programs on the computers of some of the victim companies, Internet Service Providers, and educational institutions that altered or replaced the existing legitimate programs installed on the computers of these entities.

20. Defendant MITNICK used unauthorized "hacking" programs to: (a) circumvent computer security to obtain unrestricted access to other user accounts and confidential information,

including E-Mail, stored on the computers of the victim companies, Internet Service Providers, and educational institutions; (b) disable computer logs that ordinarily provide a record of the dates and times when a computer is accessed; and (c) make his unauthorized entries into victim companies' computer systems invisible to computer department personnel responsible for maintaining and securing the computers of the victim companies, Internet Service Providers, and educational institutions.

21. By running unauthorized "hacking" programs, defendant MITNICK was able to obtain undetected "Superuser" status on the computers of the victim companies, Internet Service Providers and educational institutions. "Superuser" status permits a user to access all areas of a computer.

22. Defendant MITNICK used his "Superuser" status to: (a) obtain access to proprietary computer software and other confidential information stored in otherwise inaccessible areas of the computers of the victim companies; and (b) copy, misappropriate and transfer proprietary computer software, E-Mail, passwords, and personal information about victim company personnel.

23. Using computers and modems, defendant MITNICK electronically transferred the proprietary software from the victim companies' computers through misappropriated Internet user accounts, and then to computers belonging to USC, which he used to store the stolen proprietary software.

24. Defendant MITNICK, aided and abetted by defendant DEPAYNE and others known and unknown to the Grand Jury, also obtained proprietary computer software by: (a) deceiving victim company employees into transferring proprietary computer software to victim company computers and Internet Service Provider accounts that had been compromised by defendant MITNICK; and (b) deceiving victim company employees into mailing computer tapes and disks containing proprietary computer software to defendants MITNICK and DEPAYNE, posing as other victim company employees or authorized recipients of the proprietary computer software.

25. Defendant DEPAYNE aided and abetted defendant MITNICK through various means, including, but not limited to: (a) providing defendant MITNICK with cellular telephones; (b) assisting defendant MITNICK in converting cellular telephones into "clone~ cellular telephones by programming them with stolen electronic serial numbers and mobile identification

numbers; (c) maintaining an Internet account that defendant MITNICK used to transfer some of the fraudulently obtained proprietary computer software; (d) placing at least one pretext telephone call to a victim company posing as an employee of the victim company; and (e) attempting to have computer tapes containing proprietary computer software sent via express delivery to a hotel in Compton, California.

26. Through the means described above, defendant MITNICK, aided and abetted by defendant DEPAYNE, gained unauthorized access to numerous computer systems, and obtained, or attempted to obtain, proprietary computer software worth millions of dollars.

USE OF INTERSTATE AND FOREIGN WIRES

27. On or about the dates set forth below, in the Central District of California and elsewhere, defendant KEVIN DAVID MITNICK, aided and abetted by defendant LEWIS DEPAYNE and others known and unknown to the Grand Jury, for the purpose of executing the above described scheme to defraud and to obtain property by means of false and fraudulent pretenses, representations and promises, caused the following transmissions by wire communication in interstate and foreign commerce:

COUNT	VICTIM	DATE	WIRE TRANSMISSION
ONE	Novell	1/4/94	Telephone call from defendant MITNICK aka "Gabe Nault" in Colorado to San Jose, California
TWO	Nokia	1/26/94	Unauthorized electronic transfer of Nokia proprietary software from Salo, Finland to USC in Los Angeles, California
THREE	Nokia	2/4/94	Telephone call from defendant MITNICK aka "Mike" in the United States to Nokia in Finland
FOUR	Novell	2/13/94	Unauthorized electronic transfer of Novell proprietary software from Sandy, Utah through CSN in Denver, Colorado to USC in Los Angeles, California
FIVE	Motorola	2/19/94	Telephone call from defendant MITNICK aka "Earl Roberts" in Colorado to Motorola in Libertyville, Illinois
SIX	Motorola	2/20/94	Telephone call from defendant MITNICK in Colorado to Libertyville, Illinois
SEVEN	Motorola	2/21/94	Unauthorized electronic transfer of Motorola proprietary software from Libertyville, Illinois through CSN in Denver, Colorado and then to USC in Los Angeles, California

COUNT	VICTIM	DATE	WIRE TRANSMISSION
EIGHT	Fujitsu	4/15/94	Telephone call from defendant MITNICK aka "Chris Stephenson" in Colorado to Richardson, Texas
NINE	Fujitsu	4/15/94	Unauthorized electronic transfer of Fujitsu proprietary software from Richardson, Texas through CSN in Denver, Colorado to USC in Los Angeles, California
TEN	Nokia	4/21/94	Telephone call from defendant MITNICK aka "Adam Gould" in the United States to Nokia in Finland
ELEVEN	Fujitsu	4/26/94	Telephone call from defendant MITNICK in the United States to Fujitsu in Japan
TWELVE	Nokia	5/9/94	Telephone call by defendant DEPAYNE aka "K.P. Wileska" from Los Angeles, California to Nokia in Largo, Florida
THIRTEEN	NEC	5/9/94	Telephone call from defendant MITNICK aka "Greg" in the United States to NEC in Japan
FOURTEEN	NEC	5/10/94	Unauthorized electronic transfer of NEC proprietary software from Irving, Texas to USC in Los Angeles, California

COUNT FIFTEEN

[18 U.S.C. 5 1030(a)(4)]

28. The grand jury repeats and realleges paragraphs 1 through 26 as if fully set forth herein.

29. On or about February 21, 1994, within the Central District of California and elsewhere, defendant KEVIN DAVID MITNICK knowingly, and with the intent to defraud, accessed a Federal interest computer without authorization in order to carry out a scheme to defraud and obtained an object of value. Specifically, defendant MITNICK: (a) knowingly, and without Motorola's authorization, used computers in one state to access computers in another state belonging to Motorola; (b) duplicated and transferred proprietary computer software belonging to Motorola; and, (c) electronically transferred the proprietary software stolen from Motorola in Illinois, across state lines to computers located in Denver, Colorado, and then to computers located at USC, in Los Angeles, California.

COUNT SIXTEEN

(18 U.S.C. S 1030(a)(5))

30. The grand jury repeats and realleges paragraphs 1 through 26 as if fully set forth herein.

31. Between June 1993 and June 1994, in the Central District of California and elsewhere, defendant KEVIN DAVID MITNICK, using computers located outside California, knowingly, and without authorization, altered, damaged and destroyed information contained in, and prevented authorized use of, the computers of USC, located in Los Angeles, California. In altering, damaging, and destroying information contained in, and preventing authorized use of, the computers of USC, defendant MITNICK caused losses to one or more persons and entities aggregating more than \$1,000.

COUNT SEVENTEEN

[18 U.S.C. S 25113]

32. The grand jury repeats and realleges paragraphs 1 through 26 as if fully set forth herein.

33. In or around December 1993, in the Central Division of the District of Utah and

elsewhere, defendant KEVIN DAVID MITNICK knowingly and intentionally intercepted an electronic communication. Specifically, through the use of a computer and a computer modem, defendant MITNICK installed a program on the computers of Novell which permitted defendant MITNICK to capture electronic communications in the form of computer passwords being transmitted to the computers of Novell. Thereafter, defendant MITNICK used the unauthorized computer program to intercept electronic communications; namely, authorized computer passwords being transmitted to Novell computers by authorized users of Novell computers.

COUNTS EIGHTEEN THROUGH TWENTY-FIVE

(18 U.S.C. S 1029)

34. The grand jury repeats and realleges paragraphs 1 through 26 as if fully set forth herein.
35. On or about the dates set forth below, in the Central District of California, the Western District of Washington and elsewhere, defendant KEVIN DAVID MITNICK, knowingly and with intent to defraud possessed more than fifteen unauthorized access devices; namely, electronic files containing in excess of 15 names and corresponding passwords for accounts on the computers of the companies described below:

COUNT	DATE	UNAUTHORIZED PASSWORD FILES POSSESSED
EIGHTEEN	7/10/93	computer file containing in excess of 100 user names and corresponding passwords for accounts on Sun computers
NINETEEN	7/23/93	computer file containing in excess of 100 user names and corresponding passwords for accounts on Sun computers
TWENTY	12/1/93	computer file containing in excess of 20 user names and corresponding passwords for accounts on USC computers
TWENTY-ONE	12/20/93	computer file containing in excess of 50 user names and corresponding passwords for accounts on Novell computers
TWENTY-TWO	12/24/93	computer file containing in excess of 900 user names and corresponding passwords for accounts on Novell computers
TWENTY-THREE	2/22/94	computer file containing approximately 212 user names and corresponding passwords for accounts on Motorola computers
TWENTY-FOUR	4/16/94	computer file containing in excess of 50 user names and corresponding passwords for accounts on Fujitsu computers
TWENTY-FIVE	6/12/94	computer file containing in excess of 30 user names and corresponding passwords for accounts on NEC computers

A TRUE BILL

FOREPERSON

NORA M. MANELLA
United States Attorney
Central District of California

RICHARD E. DROOYAN
Assistant United States Attorney
Chief, Criminal Division

SEAN E. BERRY
Assistant United States Attorney
Chief, Major Frauds Section