COOKIES AND THE COMMON LAW: ARE INTERNET ADVERTISERS TRESPASSING ON OUR COMPUTERS?

MICHAEL R. SIEBECKER*

I. INTRODUCTION

Are Internet advertisers trespassing on our computers? The question arises due to the increasing reliance upon cookie technology by Internet advertising firms as the primary means to match online ads with the specific interests and characteristics of individual Internet users.[1]

It seems that whenever we visit a Web site, we are barraged with an increasing number of blinking banner advertisements hocking products and services of every imaginable sort. More than *sixty billion* advertisements per month are carefully selected for us and sent to our computers by a single Internet advertising firm, DoubleClick, Inc.[2] In order to increase the effectiveness of the ads, DoubleClick deposits small text files or "cookies" on our computers in addition to sending us the banner advertisements. Like most other Internet advertisers, DoubleClick uses cookie files to collect and maintain detailed consumer profiles that reflect the online practices, preferences and other personal characteristics of each individual who surfs the Web. Based on those detailed consumer profiles, DoubleClick places on the pages of affiliated sites various banner advertisements of client

* President's Fellow, Columbia University; Adj. Assistant Professor, Hunter College; B.A., Yale University; J.D., LL.M., M.Phil., Columbia University. I wish to thank Lee-Ford Tritt, Robert Amdur and Jethro Lieberman for their helpful comments and kind criticisms.

1. Gregg M. Fishbein & Susan E. Ellingstad, *Internet Privacy: Does the Use of "Cookies" Give Rise to a Private Cause of Action for Invasion of Privacy in Minnesota?*, 27 WM. MITCHELL L. REV. 1609, 1610 (2001).

2. See DoubleClick's Web site at *http://www.doubleclick.com/us/product/online/dfa/* for a description of the company's online advertising technology and performance.

companies that target the specific interests of individuals who happen to visit any DoubleClick affiliated site. Since its inception, DoubleClick alone has placed billions of targeted banner advertisements for client companies on sites across the Internet and some estimate that those ads have been viewed by a majority of all Internet users.[3] To date, DoubleClick has compiled perhaps as many as 100 million user profiles in its databases and, with more than 11,000 affiliated commercial Web sites, DoubleClick remains the largest Internet advertising firm in the world.[4]

Claiming that the use of cookies trampled on a variety of privacy and property rights, groups of Internet users recently brought a series of class action suits to prevent DoubleClick from placing cookies on our computers. In *In re DoubleClick, Inc. Privacy Litigation* and three other class actions directed at DoubleClick affiliates or similar entities, Internet users raised various federal statutory and common law causes of action, including trespass to chattels. But in each of those cases, the courts focused almost exclusively on the statutory claims and demonstrated an unwillingness to interpret the existing federal statutes in a way that covered cookie technology. As a result, three of the cases were dismissed entirely and one was severely curtailed. In none of these cases, however, did the courts address how common law trespass to chattels principles might apply to cookie technology.

Therefore, the project here is to address in a rather comprehensive fashion the simple question of whether the use of cookie technology exposes Internet advertisers to liability on trespass to chattels grounds. In light of the current reticence of courts to interpret existing statutes in a manner that covers cookies, an investigation of how common law tort principles might apply to cookie technology seems especially important. In the end, the examination reveals that a very strong case supports imposing liability on DoubleClick and other Internet advertisers based on a common law theory of trespass to chattels. And while the purpose here is not to suggest that common law claims should supplant statutory causes of action, framing a claim based on common law trespass to chattels principles could provide certain strategic advantages that a statutory framework might not afford.

In order to examine fully whether or not Internet advertisers might be liable under common law trespass to chattels, Part II ("Cookies and the

3. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001).

4. *See id.* at 502, 505; Jason Williams, *Personalization vs. Privacy: The Great Online Cookie Debate*, EDITOR & PUBLISHER, Feb. 28, 2000, at 26–27.

Internet") examines the basic structure of cookie technology and the role cookies play in Internet advertising. Part III ("Cookies and the Courts") discusses *In re DoubleClick, Inc. Privacy Litigation* and the three other federal cases in which Internet users attempted to raise both statutory and common law claims, including trespass to chattels. After examining how the courts disposed of those four cases based on a technical interpretation of certain federal statutes, Part III also briefly surveys the scant state and federal case law that addresses cookie technology in any other respect. Considering no court has yet to discuss cookie technology in the context of trespass, Part IV ("Trespass and the Internet") details the basic elements of a trespass claim and attempts to gain some guidance from how courts have applied trespass principles to other aspects of Internet communication. Using the facts of *DoubleClick* as a platform for analysis, Part V ("DoubleClick Revisited") examines how common law trespass to chattels principles and case law might apply to the use of cookies by Internet advertisers. After discovering that trespass to chattels provides a rather accommodating theory within which to construct a claim against Internet advertisers, Part VI ("Cookies, Class Actions and the Common Law") discusses some practical and strategic considerations that might affect the ultimate usefulness of the common law as the basis for a class action suit. Finally, Part VII ("Concluding Thoughts") suggests not only that a very strong case exists against Internet advertisers for trespassing on our computers, but also that framing a class action suit in terms of trespass principles would most likely provide distinct strategic advantages over current statutory claims.

II. COOKIES AND THE INTERNET

In the mid-1990s, Netscape developed a technology that enabled a Web site to tailor the appearance of the site to any particular visitor.[5] Upon each visit to a Web site or a page within that site, a person's computer leaves certain electronic tracks or markers. Taken together, those markers create a trail of information commonly referred to as "clickstream data." Clickstream data may include basic information, such as the type of computer an individual used to access the Internet, the kind of Internet browser utilized and the identification of each site or page visited. In addition, were an individual to disclose certain information during the visit,

5. *See* F. LAWRENCE STREET & MARK P. GRANT, LAW OF THE INTERNET § 2.1 (2001); Hal Berghel, *Caustic Cookies*, 44 COMMS. ACM, May 2001, at 19; Michael Nelte & Elton Saul, *Cookies: Weaving the Web into a State*, ACM CROSSROADS: STUDENT MAG., Fall 2000, *available at* http://www.acm.org/crossroads/xrds7-1/cookies.html (last modified Jan. 12, 2001).

the clickstream data may also include more personalized details, such as passwords, e-mail addresses or credit card numbers. Centralized Web site servers, however, simply lack the capacity to store and sift through the vast amounts of clickstream data generated by every visitor to a site. In an effort to sidestep the need for centralized data storage, Netscape developed special text files called "cookies" as a means for a Web site to collect and store clickstream data on the hard drive of each visitor's computer. By accessing, reading and editing the cookies that a Web site stores on an individual's computer, a Web site can maintain detailed records about a particular individual over a period of time. In turn, those records can be used to create dynamic Web pages that respond to individual profiles and preferences, whether used for commercial or other purposes.[6]

A. WHAT IS A COOKIE?

In technical terms, a cookie is a small text file that an Internet server deposits on the hard drive of an individual's computer.[7] The text file itself typically occupies less than four kilobytes of memory. Internet browser programs (such as Microsoft Internet Explorer or Netscape Navigator) differ with respect to the storage capacity allotted to cookie files. Netscape Navigator, for instance, permits the storage of no more than three hundred cookies at any time.[8] Recent versions of Microsoft Internet Explorer, however, use up to two percent of memory capacity for cookie text files.[9]

The cookie text files themselves consist of strings of "name-value" pairs that reduce to code various pieces of information about an individual's computer, the browsing choices a person makes while accessing a Web site and any additional information a person discloses

6. GEORGE B. DELTA & JEFFREY H. MATSUURA, LAW OF THE INTERNET §§ 6.03, 6.22, 6.23 (2d ed. 2002); Jonathan Stearn, *The 10 Common Myths of Cookies*, COMPUTER FRAUD & SEC., July 1998, at 13–14.

7. Contrary to some common reports and court opinions, cookies are not computer programs. *See, e.g.*, Marshall Brain, *How Internet Cookies Work*, at 1, HOWSTUFFWORKS, *available at* http://howstuffworks.com/cookie.htm (last visited Apr. 5, 2003); Viktor Mayer-Schönberger, *The Cookie Concept*, COOKIECENTRAL.COM, *available at* http://www.cookiecentral.com/content.phtml?area=2&id=1. *But see DoubleClick*, 154 F. Supp. 2d at 502–03 ("Cookies are computer programs commonly used by Web sites to store useful information . . . .").

8. If a server attempted to deposit an additional cookie once the three hundred cookie file limit had been reached, the browser would automatically delete the oldest cookie file to prevent exceeding the cookie storage limit. *See* Charles F. Luce, Jr., *Internet Privacy: Spam and Cookies: How to Avoid Indigestion While Binging at the World Wide Automat*, 27 COLO. LAW. 27, 30 (1998); Stearn, *supra* note 6, at 14.

9. Cliff Allen, *Stale Cookies*, CLICKZ TODAY, Dec. 28, 1999, *available at* http://www.clickz.com/article.php/819721.

during a particular visit. While some cookies may contain minimal information, others may record a wide array of "user-profiling information, IP numbers, shopping cart contents, user IDs, user-selected preferences, serial numbers, frequencies of contact with companies, demographics, purchasing histories, credit-worthiness, ... social security numbers and other personal identifiers, credit card numbers, phone numbers, and addresses."[10] In addition to that user specific information, the name-value pairs include basic parameters regarding the range of servers and sites that can access the cookie from an individual's hard drive as well as the cookie expiration date.[11]

Depending on the expiration date, cookies can be classified as "session" or "persistent." Session cookies expire when a user exits the browser at the end of an online session. Persistent cookies remain stored on an individual's computer until a particular expiration date, perhaps years in the future. While session cookies may be useful for one-time online surveys or other inquiries that require only brief storage of limited information, persistent cookies permit the aggregation of personal information over an extended period of time whenever an individual returns to a site that can access the cookie files.[12]

B. HOW DOES A COOKIE GET PLACED ON A COMPUTER?

In order to access a Web site or to navigate from page to page within a site, a person's Internet browser must send a request to the server that operates the Web site. In common parlance, your browser might ask for example, "Please send the Yahoo home page" or "Please send the Yahoo page containing the results for my search." Upon receiving the request, the server transmits to the user's computer the information that constitutes the Web site or page requested.

Of course, the communication between the server and a person's computer does not occur in polite English. Instead, both the information requests and responses follow a special formatting protocol called Hypertext Markup Language ("HTML"), a protocol that controls the formatting of almost all material that appears on the Web. For a Web site that utilizes cookies, the cookie gets embedded into the HTML message

10. *See* Berghel, *supra* note 5, at 19–20. *See also* DELTA & MATSUURA, *supra* note 6, at §§ 6.22, 6.23.

11. *See* ERIK WILDE, WILDE'S WWW: TECHNICAL FOUNDATIONS OF THE WORLD WIDE WEB 124–25 (1999).

12. *See* U.S. GAO, INTERNET PRIVACY: IMPLEMENTATION OF FEDERAL GUIDANCE FOR AGENCY USE OF COOKIES 3 (Apr. 2001).

that a server sends back to the computer requesting a Web site. So along with the HTML formatted graphics, sound or other information that constitutes the Web site, the server sends a "Set-Cookie" command to deposit a special text file—a cookie—on the user's computer.[13]

C. HOW DOES A COOKIE WORK ONCE DEPOSITED?

Once an individual's hard drive contains a cookie for a particular Web site, each time a person navigates through that site and requests a different page, the server gains access to the current cookie text. In essence, the contents of the cookie file are attached to every subsequent request back to the server for a different Web page. Upon receiving the cookie contents that get embedded into the browser's request, the server may alter the cookie text to reflect new or updated information (such as the new page visited or any personal details disclosed on the page prior to sending the request). Along with the new page the user requested, the server would send a revised cookie file that replaces the old text. Thus, once deposited on a user's computer, cookies facilitate a flow of communication back and forth between an individual's computer and the server that maintains a Web site.[14]

D. WHAT PURPOSES DO COOKIES SERVE?

Web sites use cookies for a variety of commercial and other purposes. Many Web sites utilize cookies to store ID's and passwords in order to alleviate the need for individuals to remember them on subsequent visits.[15] Depending on the data collected in the cookies, Web developers may also use cookies to customize the appearance of the site to the preferences or profiles of each visitor. For instance, if a user fills out an online form that lists her name, address and hobbies, that information will be written into the cookie text for that site. Subsequent site pages may welcome the user by name, present information related to the visitor's geographic area or display items connected to the individual's recorded interests. If a person makes an online purchase, the site may also contain an on-going shopping history and suggest similar items that the person might like to buy.[16]

13. *See* Berghel, *supra* note 5, at 20; Nelte & Saul, *supra* note 5.

14. Berghel, *supra* note 5, at 19–20; Brain, *supra* note 7, at 2–4; Mayer-Schönberger, *supra* note 7, at 1; NETSCAPE, SUPPORT DOCUMENTATION, PERSISTENT CLIENT STATE HTTP COOKIES, *available at* http: www.netscape.com/newsref/std/cookie_spec.html.

15. Stearn, *supra* note 6, at 14.

16. *See* Berghel, *supra* note 5, at 20; Mayer-Schönberger, *supra* note 7, at 1; Stearn, *supra* note 6, at 14.

At the purely commercial end of the spectrum, cookies play a crucial role in Internet advertising. When a person visits a commercial Web site, "banner" advertisements often appear in a designated portion of the page displayed.[17] Rather than storing banner advertisements on local servers, most Web sites utilize outside advertising companies, such as DoubleClick, to select and generate ads on the site's behalf.[18] The process typically occurs in four stages. First, a user's browser sends a request to a Web site's server for the contents of the site. Second, when the server responds, the contents include an image (a "banner") that cannot be displayed until the user's browser makes a separate request to the advertising company's server. Third, in the request to the advertising company's server, the original Web site is identified along with the contents of any cookie file related to that site. Finally, the advertising firm returns to the user's browser an appropriate banner ad (determined by an evaluation of the cookie text files to which the advertising firm gains access) and also typically sets a cookie of its own on the user's hard drive.[19]

The widespread exchange of cookie information provides Internet advertising firms with incredibly rich sources of information about consumer preferences and identities. By aggregating the cookie files received across affiliated client Web sites, Internet advertisers may build detailed consumer profiles that include much more information than any single client site might maintain.[20] Those profiles allow the advertisers to place ads on client sites that may seem unconnected to the particular Web site visited, but nonetheless may accurately target the user's prior online activity. For example, a person who once visited a golf Web site might find banner advertisements for golf clubs when later visiting a site wholly unrelated to sports of any kind.[21] Perhaps more important, Internet advertising firms could potentially market the profiles they cull together as valuable commodities in themselves, useful to a wide range of companies that may or may not conduct business over the Internet.

Towards that end, as part of a marketing effort to attach specific name and address information to any anonymous Internet profiles collected from its clients' cookies, DoubleClick recently acquired Abacus Direct Corp.

17. *See* Marc S. Roth, *Beware of Cookies: Do Marketers That Track a User's Online Activities Threaten Privacy?*, Nat'l L.J., Aug. 20, 2001, at C1; Alan Zeichick, *Getting the Inside Track: How Advertisers Use Cookies to Target Consumers and Understand Their Behavior*, RED HERRING, Mar. 20, 2002, *available at* 762001 WL 25558545.

18. Nelte & Saul, *supra* note 5.

19. *See id*. *See also* Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1156 (W.D. Wash. 2001).

20. Brain, *supra* note 7, at 7; Roth, *supra* note 17, at C1.

21. DELTA & MATSUURA, *supra* note 6, at 6.35; Nelte & Saul, *supra* note 5.

Abacus was a traditional direct marketing company that had already collected and maintained a comprehensive database of "names, addresses, telephone numbers, retail purchasing habits and other personal information on approximately ninety percent of American households."[22] But because that proposed combination of anonymous Internet profiles with traditional direct marketing data raised a great deal of public concern over privacy violations, DoubleClick chose not to offer for outside sale the combination of its sophisticated profiles with the Abacus Direct data.[23] Regardless of DoubleClick's particular decision, however, cookies provide a potentially powerful tool for advertisers to collect detailed consumer profiles that can be packaged and sold as an independent commodity.

III. COOKIES AND THE COURTS

Although cookie technology plays an increasingly important—and controversial—role in the evolution of Internet commerce, very few courts have addressed cookie technology in any respect. Moreover, in the even smaller handful of cases where cookie technology actually represents the primary focus of the controversy, courts have not yet ruled on the merits of any common law claims, including trespass. At most, courts have provided some limited guidance regarding the application of certain federal statutes to the use of cookies in Internet commerce. In discussing the failure of the courts to address trespass to chattels claims raised by Internet users, however, the intent is not to criticize the method of statutory construction employed by the courts. Instead, the goal is simply to point out that regardless of the interpretive perspective adopted, courts have in fact concluded that the problems associated with cookie technology generally fall outside the ambit of the particular statutes considered. Therefore, to the extent that interpretations of existing statutes fail to reach cookie technology, a gap might exist in the law that common law trespass to chattels principles could fill.

A. *IN RE DOUBLECLICK, INC. PRIVACY LITIGATION*

In re DoubleClick, Inc. Privacy Litigation arguably represents one of the most significant recent decisions regarding privacy, property and the Internet. In the spring of 2001, a federal court in the Southern District of

22. *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 505 (S.D.N.Y. 2001).

23. *Id.* at 505; DELTA & MATSUURA, *supra* note 6, at 6.35, 6.36 (stating that "[i]n response to the claims, Doubleclick has indicated that it will modify its policies to avoid creation of databases containing personally identifiable information"); Brain, *supra* note 7, at 7.

New York granted a motion to dismiss a variety of consolidated class action suits brought against DoubleClick by Internet users across the country.[24] The class alleged that DoubleClick's practice of depositing cookies on the computer hard drives of Internet users in order to collect personalized consumer profiles violated several federal statutes and state laws. With respect to federal law, the class claimed that DoubleClick violated the Electronic Communications Privacy Act ("ECPA"), the Federal Wiretap Act ("Wiretap Act") and the Computer Fraud and Abuse Act ("CFAA").[25] With respect to state law, the class argued that DoubleClick's use of cookies to collect consumer specific information rendered the company liable under the common law doctrines of invasion of privacy, unjust enrichment and trespass, as well as under certain sections of the New York General Business Law.

The district court dismissed all of the federal law claims on a variety of technical grounds. Addressing the ECPA claim first, the court noted that the ECPA primarily "aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications."[26] After examining the legislative history in order to parse the precise provisions of the ECPA, the court determined that collection of data through the use of cookies fell under an exception to the statutory prohibition otherwise applicable.[27] The court held that the ECPA did not prohibit the data collection, because the cookie-based communications between the Internet users and DoubleClick affiliated Web sites were, in the court's assessment, "intended for" those Web sites. Moreover, the cookie information sent directly to DoubleClick similarly fell outside the ambit of the ECPA, because the court found that cookie text information was not in "electronic storage" as required for application of the ECPA.[28] Even if the cookie text data were in "electronic

24. *DoubleClick*, 154 F. Supp. 2d at 500.

25. *See* Fraud and Related Activity in Connection With Computers, 18 U.S.C. § 1030 (2000); Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. §§ 2511–22 (2000); Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701–11 (2000).

26. *DoubleClick*, 154 F. Supp. 2d at 507. The ECPA provision identifies prohibited criminal conduct as follows:

> (a) Offense. Except as provided in subsection (c) of this section, whoever (1) intentionally accesses without authorization a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such system shall be punished . . . .

Id. at 507 (quoting 18 U.S.C. § 2701(a)).

27. *Id*. at 507 ("Exceptions. Subsection (a) of this section does not apply with respect to conduct authorized—. . . (2) by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user") (citing 18. U.S.C. § 2701(c)).

28. *Id*. at 511–14. *See also supra* note 26 and accompanying text.

storage," though, the court determined that the cookies simply enabled DoubleClick to access its own communications and therefore the collection would be "authorized" under the ECPA.[29]

Turning to the Federal Wiretap Act, the court determined that DoubleClick's collection of data about individual users through cookies once again fell under an exception to the statutory prohibitions.[30] Even if DoubleClick otherwise might have been liable under the statute for intercepting electronic communications,[31] the court found that DoubleClick had received appropriate "consent" from its client Web sites to intercept the information contained in the cookie texts.[32] Having received that consent, DoubleClick could not be held criminally or civilly liable without a showing that "'such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or any State.'"[33] Although the court decided not to address any of the state common law tort claims raised by the class,[34] the court still found that "plaintiffs have failed to allege" any criminal or tortious purpose motivating DoubleClick. Therefore, the court concluded the DoubleClick's use of cookies to collect personal consumer data was exempt from the provisions of the Wiretap Act.

With respect to the Computer Fraud and Abuse Act, the court yet again found an exception that enabled DoubleClick to evade any statutory sanctions. As noted by the district court, the CFAA imposes liability on anyone who "'intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication . . . .'"[35] Rather than addressing the merits of the claim under the substantive provisions of the statue, the court pointed out that the CFAA applies only in instances where alleged damages exceed $5,000.[36]

29. *Id*. at 513–14.

30. *Id*. at 514–19.

31. *Id*. at 514 ("The Wiretap Act provides for criminal punishment and a private right of action against: 'any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept wire, oral, or electronic communication . . .'" (citing 18 U.S.C. § 2511(1)(a))).

32. *Id*. (citing 18 U.S.C. § 2511(2)(d)).

33. *Id*.

34. *See infra* note 37 and accompanying text.

35. *Doubleclick*, 154 F. Supp. 2d at 519 (quoting 18 U.S.C. § 1030).

36. *Id*. at 520–21 (noting that "[the CFAA] limits the 'damage' civilly recoverable to the following instances: '(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 $5,000 in value*

Determining that there were insufficient facts alleged to establish the damage "plaintiffs incurred from DoubleClick's access to any particular computer, over one year's time" could meet the minimum threshold, the court dismissed the claim as outside the scope of the statute's protection.[37]

Upon dismissing each of the federal claims, the district court simply declined to exercise supplemental jurisdiction over any of the state law claims. Having pored over legislative histories, statutory niceties and the precise details of cookie technology in dismissing the federal causes of action, the court followed a much shorter jurisdictional route and dismissed all of the state law claims as well.[38] Thus, while the court granted DoubleClick's motion to dismiss the entire complaint, the court did not rule on the merits of any state law claim—including common law trespass.

B. *IN RE INTUIT PRIVACY LITIGATION*

While the *DoubleClick* litigation focused on the potential liability of an advertising firm that placed targeted banner ads on affiliated Web sites, a district court in California recently addressed whether or not a primary Web site operator violated computer users' privacy rights by implanting cookie files on their computers. In *In re Intuit Privacy Litigation*, a class of computer users brought a number of federal and state claims against Intuit, a company that operated a Web site called "Quicken.com."[39] The class complained that by placing cookie files on the hard drives of individuals who visited the Quicken.com site, Intuit violated the Electronic Communications Privacy Act, the Federal Wiretap Act and the Computer Fraud and Abuse Act—the same federal statutes raised in the *DoubleClick* litigation. In addition, the class advanced a state common law cause of action based on the doctrine of unjust enrichment as well as claims arising under the California Constitution. In a decision handed down just weeks after the opinion in *DoubleClick*, the district court granted in part and denied in part Intuit's motion to dismiss the complaint.

With respect to the ECPA, the Court refused to dismiss the cause of action. Intuit claimed that the ECPA applied only to unauthorized third party access to an "electronic communication."[40] Because Intuit was not a third party but rather the primary entity with whom visitors to its

during any 1-year period to one or more individuals'") (citing 18 U.S.C. § 1030(e)(8)) (emphasis in the original).

37. *Id*. at 526.

38. *Id*.

39. *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001).

40. *Id*. at 1275.

Quicken.com site communicated, Intuit contended it could not be held liable under the statute.[41] Rejecting Intuit's construction of the ECPA, the court stated that the ECPA generally prohibited the unauthorized access of electronic data and did not apply exclusively to third parties.[42] In addition, Intuit argued that the cookies were not "in electronic storage" as required for the statute's prohibitions to apply. Taking the class members allegations as true for purposes of deciding the motion to dismiss, the court simply found that the class had sufficiently alleged that the data accessed by Intuit was "in electronic storage."[43] Thus, while the court in *DoubleClick* dismissed the ECPA cause of action based on technical statutory grounds, the *Intuit* Court adopted a different statutory construction and preserved the ECPA claim.

Despite rejecting Intuit's argument regarding the application of the ECPA, the court granted Intuit's motion to dismiss the remaining federal claims. Regarding the Wiretap Act, the Court insulated Intuit from liability by applying the same statutory exemption cited in *DoubleClick*.[44] As the court explained, the Wiretap Act does not impose any penalties on a party to a communication for intercepting electronic data as long as the party receives consent and provided the data was not intercepted for the purpose of committing a criminal or tortious act.[45] According to the court, plaintiffs' failure "to state any facts in their complaint which support the allegation that Defendant intercepted electronic communications for the purpose of committing a tortious or criminal act" mandated dismissal of the Wiretap claim.[46] Even though the class cited various tortious acts related to implanting and retrieving cookie files on user hard drives, the court stated "it is unclear to the court how intercepting Plaintiffs' electronic communications could have conceivably facilitated the placement of cookies on Plaintiffs' computers."[47] Based on that rather circular interpretation of the statutory language, the court dismissed the Wiretap Act claim.

Again relying on a statutory technicality, the court also dismissed the Computer Fraud and Abuse Act cause of action. Adopting the same analytical approach as the *DoubleClick* Court, the district judge noted that

41. *Id*. at 1275–77.

42. *Id*. at 1277–78. *See also supra* notes 25–28 regarding the specific provisions of the ECPA.

43. *Intuit*, 138 F. Supp. 2d at 1275.

44. *Id*. at 1278–79. *See also supra* notes 30–31 and accompanying text regarding the specific provisions of the Wiretap Act.

45. *Intuit*, 138 F. Supp. 2d at 1278.

46. *Id*.

47. *Id*.

the CFAA covers only claims for "loss aggregating at least $5,000 in value" during any single year.[48] After engaging in a detailed discussion of what might constitute "loss" under the statute, the court concluded that plaintiffs did not allege facts sufficient to support a "reasonable inference" that the class could surmount the minimum damage threshold.[49] As a result, the court dismissed the CFAA claim.

With respect to the state common law and constitutional claims, the court denied Intuit's motion to dismiss. Because the court preserved plaintiffs' cause of action under the ECPA, the court decided to exercise supplemental jurisdiction over the remaining state law claims as well. Since Intuit moved to dismiss the state law claims on jurisdictional grounds alone, the court did not need to address the substance of any state law claims. Instead, the court simply allowed the state constitutional and common law claims (which in any event did not include trespass to chattels) to continue without additional comment.

C. *CHANCE V. AVENUE A, INC.*

Addressing a slight wrinkle to the facts in *DoubleClick*, a federal district court recently examined whether or not an Internet advertising "subcontractor" could be held liable for depositing cookie files on the hard drives of Internet users. In *Chance v. Avenue A, Inc.*, a group of Internet users brought a suit against an Internet advertising firm for depositing and accessing cookie files on the hard drives of Internet users in order to create appropriately targeted banner advertisements for client Web sites.[50] In addition to placing targeted banner ads on Web sites directly affiliated with Avenue A, however, Avenue A also acted as a subcontractor for DoubleClick and placed targeted banner advertisements on DoubleClick affiliated sites as well.[51] In essence, for certain Web sites that had entered into an agreement with DoubleClick to provide banner advertisements on their sites, the advertisements would be placed by Avenue A rather than DoubleClick itself. Adopting a similar strategy pursued by the classes in *DoubleClick* and *Intuit*, the plaintiffs in *Avenue A* claimed that Avenue A's actions violated the Electronic Communications Privacy Act, the Federal Wiretap Act and the Computer Fraud and Abuse Act. With respect to state law, plaintiffs raised a number of common law causes of action based on

48. *Id.* at 1279–81 (citing 18 U.S.C. §1030(e)(8)(A)). *See also supra* note 36 regarding the specific provisions of the CFAA.

49. *Intuit*, 138 F. Supp. 2d at 1281.

50. Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001).

51. *Id.* at 1156–57.

invasion of privacy, trespass and unjust enrichment, in addition to several state statutory claims for deceptive and unfair business practices.

Embracing the analysis of the *DoubleClick* court, the district court dismissed the ECPA claims against Avenue A. At the outset, the court noted that the ECPA "was intended to cover such mid-1980s technological facilities as telephone companies, email servers, and bulletin boards" and expressed some doubt regarding whether plaintiffs' computers were in fact "'facilities through which an electronic communication service is provided'", as necessary for the ECPA prohibitions to apply.[52] Even if plaintiffs' computers were covered under the ECPA, however, the court ultimately relied on the same statutory exception central to the ruling in *DoubleClick*. According to the court, the exchange of data contained in the cookie text files fell under an explicit statutory exemption, because the communications at issue were "'intended for'" Avenue A and "'authorized'" by plaintiffs.[53] While acknowledging the factual wrinkle that existed where Avenue A acted as a advertising subcontractor for DoubleClick, the court concluded that "[a]lthough this is a significant factual difference from DoubleClick, it leads to the identical legal conclusion."[54] Because DoubleClick was authorized to access the cookie text files, "the rerouting is irrelevant after that initial authorization."[55] In the opinion of the court, since any Web site that plaintiffs contacted had authorized Avenue A or DoubleClick to access the communications between those Web sites and individual computer users, the ECPA imposed no liability.

Once again insulating Avenue A from liability under a statutory exception, the court dismissed the Wiretap Act claim as well. While acknowledging that the Wiretap Act prohibits the intentional interception of any wire, oral or electronic communication, the court noted the same statutory exception that controlled the analysis in *DoubleClick* and *Intuit*. As explained by the court, the "exception requires a party to the communication to consent to the interception and that the interception be without any criminal or tortious purpose."[56] Citing the decision in *DoubleClick*, the court concluded that Avenue A had received the necessary consent from Internet users under the same analysis the court

52. *Id*. at 1160 (citing 18 U.S.C. § 2701). *See also supra* notes 25–28 regarding the specific provisions of the ECPA.

53. *Chance*, 165 F. Supp. 2d at 1160–61 (citing 18 U.S.C. § 201(c)(2)).

54. *Id*. at 1161.

55. *Id*.

56. *Id*. at 1162. *See also supra* notes 30–31 regarding the specific provisions of the Wiretap Act.

applied with respect to the ECPA.[57] Moreover, despite plaintiffs' allegations that Avenue A committed various tortious acts under state law, the court construed the statute not only to require a demonstration of criminal or tortious purpose but also that such purpose must be either the "'primary motivation'" or the "'determinative factor in the actor's motivation for intercepting'" the communication.[58] Therefore, even if plaintiffs were successful in maintaining a state tort claim, that liability would not trigger the prohibitions in the Wiretap Act absent some additional demonstration of an overriding tortious intent motivating Avenue A's business practices. After stating "[i]t is simply implausible that the entire business plan of one of the country's largest Internet media companies would be 'primar[ily] motivated' by a tortious or criminal purpose," the court determined that Avenue A fell squarely within the statutory exception and dismissed the Wiretap Act claim.[59]

With respect to the CFAA, the court continued to follow the approach of the *DoubleClick* and *Intuit* rulings by shielding Avenue A from liability on the basis of a statutory technicality. Referring to the *DoubleClick* decision, the court noted that "[t]he CFAA requires that the $5,000 threshold of damage be met in order to state a valid cause of action."[60] While acknowledging each instance that Avenue A accessed a cookie file on plaintiffs' hard drives constituted a "singular act," those singular acts could not be aggregated to meet the $5,000 damage threshold. Instead, plaintiffs would have to demonstrate that a single, isolated exchange of a cookie text file caused damage surpassing the minimum threshold in order for the CFAA prohibitions to apply.[61] Because the court determined that "[p]laintiffs have not shown any facts that prove an aggregate damage of over $5,000 for any single act of the Defendant, from either the initial placement of an Avenue A cookie or a subsequent accessing of this cookie," the CFAA claim could not stand.[62]

Having dismissed each of the federal statutory claims, the court declined to exercise supplemental jurisdiction over remaining "novel and complex issues of state law."[63] Thus, without addressing the merits of

57. *See Chance*, 165 F. Supp. 2d at 1162.

58. *Id.* (citing *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 514–15 (S.D.N.Y. 2001)) (quoting United States v. Dale, 991 F.2d 819, 841–42 (D.C. 1993)).

59. *Id*. at 1163.

60. *Id*. at 1158. *See also supra* note 36 regarding the specific provisions of the CFAA.

61. *See Chance*, 165 F. Supp. 2d at 1159–60.

62. *Id*. at 1159.

63. *Id*. at 1163.

plaintiffs' state law claims, the court granted Avenue A's motion for summary judgment on all of the federal and state claims alike.

D. *IN RE PHARMATRAK, INC. PRIVACY LITIGATION*

Examining yet another minor twist of the facts in *DoubleClick*, a Massachusetts federal court recently addressed whether or not an Internet tracking firm and its clients could be held liable for using cookies to build detailed profiles of Web site visitors. In *In re Pharmatrak, Inc. Privacy Litigation*, various Internet users filed a class action against five drug companies and Pharmatrak, an Internet monitoring company, for using cookie technology to collect detailed health and consumer profiles on individuals who accessed the client drug company sites.[64] According to the class, cookies were used clandestinely to gather a variety of personalized information, including "names, addresses, telephone numbers, dates of birth, sex, insurance status, medical conditions, education levels, and occupations . . . email communications, including user names, email addresses and subject lines from emails."[65] Just as in *DoubleClick*, *Intuit* and *Avenue A*, the class alleged that depositing cookie files on the hard drives of individual Internet users not only violated the ECPA, the Wiretap Act and the CFAA but also rendered plaintiffs liable under various state law claims, including trespass to chattels.

In keeping with the approach originally articulated in *DoubleClick*, the district court granted Pharmatrak's motion for summary judgment on the ECPA claim. Frequently citing *DoubleClick* and *Avenue A*, the court determined that the computers of individual Internet users were not "'facili[ties] through which an electronic communication service is provided.'"[66] While acknowledging that individuals use personal computers and phone lines to access the Internet, the court concluded that it "is not enough for the purposes of the ECPA. The relevant *service* is Internet access, and the service is provided through ISPs and other servers, not though [sic] Plaintiffs' PCs."[67] In addition, citing the same statutory exception employed in *DoubleClick* and *Avenue A*, the court noted that Pharmatrak had received sufficient authorization from its client Web sites to monitor communications between those sites and individual Internet users. Therefore, even if the computers of Internet users were covered by the ECPA, the court concluded that the ECPA would still not impose

64. *In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 5–6 (D. Mass. 2002).
65. *Id*. at 9.
66. *Id*. at 13. *See also supra* notes 25–28 regarding the specific provisions of the ECPA.
67. *Pharmatrak*, 220 F. Supp. 2d at 13 (emphasis in the original).

liability on Pharmatrak.[68] Further echoing the analysis of *DoubleClick*, the court announced that the ECPA did not prohibit Pharmatrak from placing cookie files on the hard drives of individual Internet users, because the files were not in "electronic storage" as required by the same technical reading of the ECPA articulated in *DoubleClick*.[69] Finally, based on the insistence of the class that the drug companies did not authorize Pharmatrak to collect the personal consumer information that Pharmatrak actually obtained, the court determined that the client drug companies could not have intended to access that personal information without authorization, as required by the ECPA.[70] Thus, based on the statements of the class, the court concluded that the drug companies lacked "the necessary intent under this punitive statute."[71]

In granting Pharmatrak's motion for summary judgment on the Wiretap Act claim, the Massachusetts district court again closely followed the approach adopted in *DoubleClick* and *Avenue A*. The basic inquiry centered on whether or not Pharmatrak had received sufficient consent from the drug company Web sites to fall under the statutory exception provided in the Wiretap Act.[72] As explained by the court, liability under the Wiretap Act does not arise where one party to a communication has given consent to its interception and the communication was not intercepted for the purpose of committing a criminal or tortious act.[73] While conceding that the drug companies contracted with Pharmatrak to obtain certain consumer data, the class urged the court to limit the scope of consent that Pharmatrak received to the "assembly of anonymous, aggregate information" and not to include the "collection of personally identifiable information."[74] But after detailing the facts and analyses of *DoubleClick* and *Avenue A*, the court concluded "it is irrelevant to the purposes of the Wiretap Act whether the Pharmaceutical Defendants knew the precise mechanisms of Pharmatrak's service or not. It is sufficient that the Pharmaceutical Defendants were parties to communications with Plaintiffs and consented to the monitoring services provided by Defendant

68. *Id*. at 13–14.
69. *Id*. at 14.
70. *Id*.
71. *Id*.
72. Because the class withdrew the wiretap claims against the drug companies, the court only addressed how the provisions of the Wiretap Act applied to Pharmatrak. *See Pharmatrak*, 220 F. Supp. 2d at 11–12.
73. *See id.* at 12. *See also supra* notes 30–31 regarding the specific provisions of the Wiretap Act.
74. *See Pharmatrak*, 220 F. Supp. 2d at 11.

Pharmatrak."[75] Since the class had failed to demonstrate any tortious or criminal intent behind the interception of the cookie files, the court granted Pharmatrak's summary judgment motion on the Wiretap Act claim.

Finally, with respect to the CFAA, the court shielded Pharmatrak and the drug companies from liability using the same technical limitation relied upon in *DoubleClick*, *Intuit* and *Avenue A*. After explaining that the CFAA limits recovery to losses aggregating at least $5,000 in any one year period, the court examined what constitutes a "loss" under the statute.[76] While the court embraced a rather flexible interpretation of the kind of damages that might qualify to meet the minimum statutory threshold, the court stressed that those losses must arise from a single act.[77] Because the class could not demonstrate that each transfer of a cookie file caused at least $5,000 in losses, the court determined that the CFAA did not impose liability on Pharmatrak or its client drug companies.[78]

Upon granting Pharmatrak's motion for summary judgment with respect to each of the federal statutory claims, the court simply decided not to retain jurisdiction over the remaining state law issues. Thus, although the court did not evaluate the underlying merits of any common law claims, the court dismissed without comment all the remaining state law causes of action.

E. OTHER COOKIE CASES

In addition to the four decisions in *DoubleClick*, *Intuit*, *Avenue A* and *Pharmatrak*, courts have addressed cookie technology in only a few other cases. And in those cases, the discussion of cookie technology was only ancillary to the controlling issues. For instance, in a recent patent infringement case involving a method for placing purchase orders over the Internet, the Federal Circuit Court mentioned only in passing how cookies played a role in one aspect of the purchasing system at issue.[79] In *Putnam Pit, Inc. v. City of Cookeville*, a district court considered, among many other issues, whether or not a newspaper, Web page and editor had a First Amendment right to gain access to certain cookie files of city employees (contained on city computers) that would help determine if those employees had used city computers to browse Internet sites that were

75. *Id*. at 12.
76. *See id*. at 14–15. *See also supra* note 36 regarding the specific provisions of the CFAA.
77. *See Pharmatrak*, 220 F. Supp. 2d at 15.
78. *Id*.
79. Amazon.Com, Inc. v. BarnesandNoble.Com, Inc., 239 F.3d 1343, 1365 (Fed. Cir. 2001).

inconsistent with government functions.[80] In only a cursory reference, a district court in Kansas noted that cookie files, along with a host of other types of electronically recorded information, fell within a broad discovery order related to the production of computer data.[81] Finally, in an unpublished opinion of a California state appellate court, the court addressed certain contractual and procedural issues regarding a forum selection clause in a licensing agreement.[82] The class action suit against an Internet media firm actually involved a variety of statutory and common law claims (including trespass) related to the collection of consumer data through cookie technology.[83] But because the litigation was only in its beginning stages, the court simply addressed some initial procedural concerns without discussing the merits of any underlying claims.[84]

Given the increasing importance of cookie technology in the development of Internet commerce and the concomitant growing concerns about personal property and privacy, the dearth of cases that even mention cookies may seem surprising. But perhaps more surprising is that in the few cases where cookie technology itself represented a core concern, none of the opinions addressed the merits of any common law claims, including trespass. Instead, courts have provided only limited guidance on whether the use of cookies triggers liability under certain federal statutes. To date, with respect to cookies and the common law, courts remain silent.

IV. TRESPASS AND THE INTERNET

In light of the relative silence of courts regarding cookie technology, how is it possible to assess whether or not Internet advertisers are trespassing on our computers? An examination of the historical foundations of trespass to chattels, the anatomy of a basic trespass claim and the decisions of recent courts regarding the application of trespass principles to the Internet provides some rather clear guidance. In the end, that examination demonstrates that common law trespass to chattels principles provide a much firmer foundation upon which to base a claim against Internet advertisers than the statutory framework utilized in *DoubleClick*.

80. Putnam Pit, Inc. v. City of Cookeville, 23 F. Supp. 2d 822, 827 (M.D. Tenn. 1998), *aff'd in part and rev'd in part by*, 221 F.3d 834 (6th Cir. 2000).

81. Kleiner v. Burns, 48 Fed. R. Serv. 3d 644, 649 (D. Kan. 2000).

82. RealNetworks, Inc. v. Superior Court, 2001 WL 1527492 *1–*3 (Cal. Ct. App. 2001).

83. *See id.* at *1.

84. *See id.* at *3.

A. HISTORICAL FOUNDATIONS

Although trespass to chattels has a long history, the claim basically emerged as an outgrowth of the more serious tort of conversion. While conversion involves a substantial interference that requires compensation for the full value of the property at stake, trespass to chattels focuses on a much less significant intrusion on personal property interests. As Dean Prosser explained, trespass to chattels permits recovery for

> interferences with the possession of chattels which are not sufficiently important to be classed as a conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels survives today, in other words, largely as a little brother of conversion.[85]

In essence, trespass to chattels captures a wide range of activities that affect our possessory interests in personal property, activities perhaps less serious than theft or destruction of the property itself but serious enough to warrant some relief nonetheless. While the usefulness of trespass to chattels has varied over time depending on the needs of society, as one court recently stated, "the tort has reemerged as an important rule of cyberspace."[86]

B. ANATOMY OF A TRESPASS

Trespass to chattels is a basic common law tort currently recognized in state and federal courts around the United States. Of course, given the evolving nature of the common law itself, the essential elements of a trespass to chattels claim may depend on the jurisdiction. Courts in one state may confront an issue in a manner that other states do not feel compelled to adopt. Despite some minor variances among jurisdictions, however, the basic anatomy of trespass to chattels remains rather straightforward.

1. Elements

As a general rule, a trespass to chattels occurs when an individual unjustifiably interferes with another person's chattel in a manner that causes some cognizable harm.[87] More specifically, according to the

85. PROSSER AND KEETON ON THE LAW OF TORTS §§ 14, 85–86 (W. Page Keeton et al. eds., 5th ed. 1984).

86. Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 247 (Ct. App. 2001), *review granted and opinion superseded*, 118 Cal. Rptr. 2d 546 (2002) (decision without published opinion).

87. RESTATEMENT (SECOND) OF TORTS § 217 (1965). *See also* DAN B. DOBBS, THE LAW OF TORTS 122–23 (West Group 2000).

Restatement, a trespass to chattels "may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another."[88] While appearing to define a rather broad range of activities that might constitute trespass to chattels, the Restatement limits liability to instances in which the interference resulted in actual damage. Based on the extant case law and the principles set forth in the Restatement, a basic cause of action for a trespass to chattels seems to consist of the following four essential elements.

Tangible Property. Trespass to chattels involves only tangible property. While the requirement of tangibility may seem all too obvious, courts have recently expanded the kinds of tangible property to which a trespass to chattels claim might apply. In early cases, courts limited trespass to chattels claims to common goods that could be carried away by another and somewhat later began to include property that could be damaged even if not taken (such as farm animals that were killed or injured).[89] More recently, however, courts have extended the notion of chattels to include computer networks, telephone databases, electrical signals and other communications systems.[90] Some scholars even advocate extending trespass claims to intangible property, such as business goodwill or uncollected sales commissions.[91] Although tangibility currently remains an essential element of a trespass claim, "the requirement of a tangible has been relaxed almost to the point of being discarded."[92] In the context of potential trespass claims involving computer cookies, the increasing malleability of the element of tangibility represents an important development. Why? Even if tangibility represents a lingering technical hurdle, courts continue to embrace a flexible interpretation of what constitutes tangible property in a way that accommodates modern technological advances.

Dispossession or Interference. An actionable trespass requires either dispossession or interference with the chattel. With respect to the first

88. RESTATEMENT (SECOND) OF TORTS § 217 (1965). *See also* DOBBS, *supra* note 87, at 122–23; STUART M. SPEISER, CHARLES F. KRAUSE & ALFRED W. GANS, THE AMERICAN LAW OF TORTS § 23:23, at 666–67 (1990).

89. PROSSER AND KEATON *supra* note 85, at 86. *See also* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Ct. App. 1996).

90. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); *Thrifty-Tel*, 46 Cal. App. 4th at 1559, 1566–67.

91. Val D. Ricks, *The Conversion of Intangible Property: Bursting the Ancient Trover Bottle with New Wine*, 1991 BYU L. REV. 1681 (1991).

92. *Thrifty-Tel*, 46 Cal. App. 4th at 1567 n.6.

prong, the dispossession may be actual or constructive. It is not necessary for an individual to have exclusive possession of another's property in order for a trespass to occur. Instead, partial or temporary possession may still satisfy the requirement if the rightful owner could lawfully reclaim full possession of the chattel.[93] As stated in the Restatement, dispossession:

> may be committed by intentionally (a) taking a chattel from the possession of another without the other's consent, or (b) obtaining possession of a chattel from another by fraud or duress, or (c) barring the possessor's access to a chattel, or (d) destroying a chattel while it is in another's possession, or (e) taking the chattel into the custody of the law.[94]

Therefore, even without actually carrying off a particular piece of personal property, constructive dispossession will sustain a trespass claim. Regardless of whether the dispossession was long, short, partial, total, actual or constructive, an actionable trespass exists as long as the rightful owner maintains an uninterrupted right to exclusive possession of the chattel.[95]

Interference, in contrast, involves any sort of impairment or damage to the chattel short of dispossession. This alternative to dispossession represents a significant expansion of the early concept of trespass and has continued to provide a basis for extending trespass to new types of property interests.[96] In contrast to the concept of dispossession that covers circumstances in which a person deprives another of property altogether, interference addresses instances in which property interests are impaired but the goods themselves are not taken. Along those lines, interference covers cases in which animals are beaten, goods are used without permission or items are moved from one place to another.[97] Moreover, courts continue to embrace an increasingly elastic notion of what constitutes interference. Even in the absence of any person actually touching a chattel, courts have sustained trespass claims arising from migrating dust, microscopic chemical particles, smoke, sound waves and

93. SPEISER ET AL., *supra* note 88, § 23:24, at 680–81. *See, e.g.*, Ill. Bell Tel. Co. v. Miner, 136 N.E.2d 1, 6 (Ill. Ct. App. 1956).

94. RESTATEMENT (SECOND) OF TORTS § 221. *See also* DOBBS, *supra* note 87, at 138.

95. *Id.* at 124.

96. *See* PROSSER AND KEATON, *supra* note 85, at 85.

97. *Id*. For a general description of the degree of interference trespass to chattels requires, see also Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1277 (N.D. Iowa 2000); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998).

other electronic signals, to name just a few examples.[98] Finally, the interference itself does not even need to be substantial for a trespass claim to survive. To the contrary, even some minor interference "which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel."[99] Rather than serving as a severe limitation, then, the requirement of interference provides a rather generous platform upon which to construct a trespass to chattels claim.

Intent. While trespass to chattels originated as a strict liability tort, the intent to dispossess or intermeddle with the property of another represents an essential element of a modern trespass to chattels claim.[100] Still, the intent requirement remains minimal and does not need to reflect any wrongful motive. Instead, simply demonstrating that another voluntarily acted in the interference or dispossession satisfies the intent element. Even if the interference occurred by mistake, sufficient intent exists to sustain a trespass claim as long as the mistaken act itself was voluntary. As Prosser explains:

> [I]t is no defense that the defendant believed the goods to be his own, so long as the defendant voluntarily interfered with them by the act which constituted the trespass. As in the case of trespass to land and conversion, the property right is protected at the expense of an innocent mistake.[101]

Wholly accidental interference, however, will not satisfy the intent element. For example, where a contractor accidentally strikes a deeply buried telephone cable during an excavation project, no cause of action for trespass to the cable will arise, if the contractor never intended to touch the cable.[102] Thus, while the intent element is not terribly difficult to satisfy, even in the absence of any desire to harm or invade the property interests of

98. *See generally* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (discussing electronic signals); Ream v. Keen, 838 P.2d 1073 (Or. 1992) (involving smoke); Bradley v. Am. Smelting & Ref. Co., 709 P.2d 782 (Wash. 1985) (addressing microscopic particles from chemical treatment); Wilson v. Interlake Steel Co., 649 P.2d 922 (Cal. 1982) (concerning sound waves); Roberts v. Permanente Corp., 10 Cal. Rptr. 519 (Ct. App. 1961) (involving migrating dust particles).

99. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000). *See also* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Ct. App. 1996) (citing RESTATEMENT (SECOND) OF TORTS § 217).

100. PROSSER AND KEATON, *supra* note 85, at 86.

101. *Id.* at 86–87. *See also* FOWLER V. HARPER, FLEMING JAMES, JR. & OSCAR S. GRAY, THE LAW OF TORTS § 2.4 (2d ed. 1996) ("Trespassers act at their peril and are liable even for accidental harm to the property or to its possessor.").

102. *See* DOBBS, *supra* note 87, at 123. *See also* Mountain States Tel. & Tel. Co. v. Horn Tower Const. Co., 363 P.2d 175, 176–77 (Colo. 1961); RESTATEMENT (SECOND) OF TORTS § 217 (cmts. a, b) (1965).

another, purely accidental touching or other interference will not give rise to a valid trespass claim.

Damage. The need for actual harm provides an important difference between trespass to land and trespass to chattels. Even if some unauthorized entry onto another person's land does not cause any actual damage, an actionable trespass to land still occurs. In contrast, a property owner cannot recover under a trespass to chattels claim unless some legally recognizable harm results.[103] But what constitutes legally recognizable harm? According to the Restatement, sufficient harm exists to support liability for trespass to chattels, if:

> (a) he dispossesses the other of the chattel, or (b) the chattel is impaired as to its condition, quality or value, or (c) the possessor is deprived of the use of the chattel for a substantial time, or (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.[104]

In the case of dispossession, the Restatement further explains that a rightful owner may recover at least nominal damages even if there were no impairment of the condition, quality or value of the chattel and even if the dispossession was brief.[105] That basic description of the categories of cognizable harm set forth in the Restatement provides a general guide for courts to determine if a prima facie cause of action exists for a trespass to chattels claim.[106]

Measuring the value of any harm resulting from a trespass, however, presents a special challenge.[107] But that valuation problem remains distinct from the determination that sufficient harm exists to support a trespass to chattels claim at the outset. Thus, even if interference with another's chattel results in only minimal actual damage, the trespass claim may still survive.[108] Therefore, what matters for purposes of maintaining a trespass to chattels claim is not the monetary value of the harm suffered. Instead, in order for a trespass to chattels claim to survive, the harm suffered must

103. DOBBS, *supra* note 88, at 124; HARPER, *supra* note 101, at 141–46.

104. RESTATEMENT (SECOND) OF TORTS § 218 (1965).

105. *Id*. § 218 (cmt. d).

106. *See, e.g*., eBay Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000) (quoting the Restatement at length); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998) (citing generously to the Restatement); Am. Online Inc. v. IMS, 24 F. Supp. 2d 548, 548, 550 (E.D. Va. 1998) (citing the Restatement); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1016, 1021–23 (S.D. Ohio 1997) (using the Restatement in its analysis); Terrell v. Rowsey, 647 N.E.2d 662, 666 (Ind. Ct. App. 1995) (borrowing from the Restatement).

107. *See infra* notes 150–56 and accompanying text.

108. *Bidder's Edge*, 100 F. Supp. 2d at 1071–72.

simply fall under the basic categories of harm currently recognized as sufficient to support a claim.

2. Consent and Authorization

Even upon satisfying all the elements of a trespass to chattels claim, no liability would result if the purported trespasser acted with sufficient authorization or consent.[109] Of course, it would seem rather odd if the law permitted us to pursue a trespass claim against those whom we asked to handle our belongings. Imagine filing a trespass to chattels claim against the local plumber not because the plumber did a poor job fixing your leaky faucet but simply because your sink was touched in order to complete the work.

Still, giving consent to use or possess a chattel does not entirely eliminate the possibility of trespass. To the contrary, a cause of action may still arise if the potential trespasser exceeds the scope of the authorization originally provided, the consent was obtained fraudulently, or some revocation or modification of the consent occurred.[110] Whether or not a revocation or modification actually occurred represents a question of fact particular to any case, but

> consent may be terminated by the lapse of time or the happening of some event that limited and restricted the consent, by the communication by the plaintiff to the defendant of his unwillingness that the defendant deal further with the chattel, or by the transfer of the other's possessory interest in the chattel of which the defendant has knowledge.[111]

To the extent a person receives adequate consent to interfere with another's belongings, then, no trespass claim can arise. But in the absence

109. The Restatement and many courts consider the lack of authorization to be an essential element of a trespass to chattels claim. *See IMS*, 24 F. Supp. 2d at 550; *LCGM*, 46 F. Supp. 2d at 451–52; RESTATEMENT (SECOND) OF TORTS § 217(b) (1965). Other courts treat the issue of consent as a defense rather than as a basic element. *See* MARSHALL S. SHAPO, BASIC PRINCIPLES OF TORT LAW 56 (1999). Regardless of the differing pleading postures, however, the basic concept of consent remains consistent.

110. RESTATEMENT (SECOND) OF TORTS §§ 228, 252A (1965); HARPER, *supra* note 101, § 2.4; Mark D. Robins, *Electronic Trespass: An Old Theory in a New Context*, 15 THE COMPUTER LAW., July 1998, at 1, 3–4.

111. HARPER, *supra* note 101, § 2.4. *See* RESTATEMENT (SECOND) OF TORTS §§ 228, 254 (1965). *See also* Am. Online, Inc., v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1277 (N.D. Iowa 2000); Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *7 (N.D. Cal. 1998); *Bidder's Edge*, 100 F. Supp. 2d at 1070 (noting that scope of consent to access a public site may be limited and conditioned); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Ct. App. 1996).

of sustained authorization, an intentional interference with the possessions of another will support a valid trespass action.

C. TRESPASS TO CHATTELS AND THE INTERNET

Even though courts have yet to address cookie technology in detail, existing case law in related areas provides significant guidance regarding the extension of trespass to chattels claims to the Internet. In contrast to the extraordinary dearth of cases pertaining specifically to cookies, a small but significant number of cases have already connected trespass to chattels and computer technology. At least so far, the particular subject matter of the trespass claims fall roughly into two categories: (i) unauthorized access to information and (ii) bulk e-mails or "spam."[112] An examination of how courts apply the basic common law principles in these two areas suggests that trespass to chattels could extend quite readily to cookie technology as well.

1. Unauthorized Access to Information

With respect to unauthorized access to information, trespass cases typically focus on unwanted electronic contact with computer systems or networks that contain valuable information. In *Thrifty-Tel, Inc. v. Bezenek*, one of the earliest computer trespass cases, a group of children obtained a confidential access code to gain entry into a telephone company's computer system.[113] Using a home computer and modem, the children then conducted random digit searches to obtain authorization codes for making long distance phone calls.[114] Rejecting the hackers' argument that the electronic access failed to constitute any real interference with the phone company's computer network, a California appellate court found the children's parents liable to the company on trespass to chattels grounds. Building upon a list of prior cases in which dust particles, microbes and even sound waves were found sufficient contacts to support a trespass action, the court embraced an even more flexible understanding of what constitutes interference or intermeddling. Noting that even the most indirect touching could support a valid trespass claim, the court concluded that "the electronic signals generated by the Bezenek boys' activities were

112. For a definition of "spam," see *Hotmail Corp.*, 1998 WL 388389, at *1 ("'Spam' is unsolicited commercial bulk e-mail akin to 'junk mail' sent through the postal mail. The transmission of spam is a practice widely condemned in the Internet Community. . .").

113. *Thrifty-Tel*, 54 Cal. Rptr. 2d at 471.

114. *Id.*

sufficiently tangible to support a trespass cause of action."[115] At least under the reasoning of *Thrifty-Tel*, then, no difference seems to exist between sending unwanted electronic signals to a computer network and physically touching the components that constitute the network itself.

Building upon the flexible approach adopted in *Thrifty-Tel*, some recent federal court decisions have extended the trespass to chattels doctrine to cover unauthorized "search robots" that scour data stored on servers throughout the Internet. In simple terms, an Internet "search robot" is a computer program that searches the Web sites of others in order to copy and retrieve desired information. Typically, search robots perform thousands of search commands each minute, far exceeding the ability of any individual to search the same Web sites manually.[116] Although the information gathered can prove commercially valuable to business entities that specialize in unique data packaging, the robotic searches can clog Internet traffic and slow the operation of the Web sites being scoured. In at least three cases to date, Web site operators have successfully relied on trespass to chattels claims to prevent the use of "search robots" from accessing the Web sites through unwanted electronic contacts.

In *eBay, Inc. v. Bidder's Edge, Inc.*,[117] a California district court granted a preliminary injunction against Bidder's Edge, an Internet auction aggregating warehouse that used computer search robots to access the popular online auction site owned by eBay. Although eBay's auction Web site explicitly prohibited the use of robotic search activity, Bidder's Edge conducted approximately 100,000 searches of the eBay Web site each day. Rejecting Bidder's Edge notion that no trespass could occur because eBay's site was generally accessible to the public, the court noted that eBay's servers were private property and eBay had granted access to the public only under certain conditions—conditions that expressly prohibited robotic searching.[118] Although the court acknowledged that Bidder's Edge might have been authorized to conduct individual searches, "[Bidder's Edge's] web crawlers exceeded the scope of any such consent when they began acting like robots by making repeated queries."[119] Under the holding of *Bidder's Edge*, then, making a Web site publicly available does not necessarily constitute implicit authorization for sending all types of electronic signals to another's computer network. Instead, the question of

115. *Id*. at 1568 n.6.
116. *Bidder's Edge*, 100 F. Supp. 2d at 1060–61.
117. *Id*. at 1058.
118. *Id*. at 1070.
119. *Id*.

authorization turns on the scope of authority granted, the frequency of the offensive electronic signals and the purposes for which those signals were sent.

On the issue of damages, even though eBay could not demonstrate much damage to its computer network due to the robotic searches, the court concluded that the use of even a portion of eBay's computer capacity provided sufficient damage. Adopting a broad approach, the court noted that the robotic searches conducted by Bidder's Edge "amount[] to use of eBay's computer systems"[120] and occupied some "portion"[121] of eBay's computer capacity. Even if the searches used only a small fraction of the overall capacity of eBay's network, Bidder's Edge "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 [Bidder's Edge] actions appear to have caused injury to eBay . . . ."[122] Moreover, from a prospective policy standpoint, the court noted that if the robotic searches were found legal, other companies employing robotic search programs would likely flood the eBay server "potentially to the point of denying effective access to eBay's customers."[123] According to that approach, the absence of significant and immediately quantifiable damages does not undermine the viability of a trespass claim. To the contrary, the mere threat of future damage could suffice to allow a trespass to chattels claim to continue. Following the ruling in *Bidder's Edge*, using unauthorized electronic signals to access even a small portion of a computer system may give rise to a valid trespass to chattels claim, regardless of any presently quantifiable damage caused by the signals themselves.

In another very similar federal case, *Register.com, Inc. v. Verio, Inc.*, the Southern District of New York granted a preliminary injunction to prevent the continued use of robotic searches of online data maintained by Register.com, an Internet domain name registration firm.[124] Verio, a corporation that provides various Internet services to other online companies, admitted using robotic searches to compile lists of potential customers from Register.com's online database. Register.com alleged that the robot searches flooded its system and slowed the server response time to other visitors. Although finding that Register.com's published policies

120. *Id.* at 1070.
121. *Id.* at 1071.
122. *Id*.
123. *Id*.
124. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 241, 255 (S.D.N.Y. 2000).

did not in fact prohibit the use of robotic searches, the court inferred that the act of filing suit revoked any implicit authorization that might have existed. As stated by the court, "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."[125] Moreover, even though Register.com could not provide any precise evidence that its computer system suffered any actual damage as a result of the robotic searches, the court noted that "evidence of mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels."[126] Citing *Bidder's Edge*, the court noted that "'[t]he quality or value of personal property may be "diminished even though it is not physically damaged by defendant's conduct."'"[127] Because Verio's search robot occupied "some" of Register.com's system capacity, the court concluded that the searches would support a trespass cause of action under the very low threshold previously established in *Bidder's Edge*.[128]

Just as in *Bidder's Edge*, though, the court in *Register.com* also noted that regardless of any minimum "quantum" of actual damage caused by the robotic searches, the potential of future harm might satisfy the damage requirement of a trespass claim. In assessing the full extent of damages caused by the robotic searches, the court relied in part on testimony that repeated robotic searches could cause such a strain that Register.com's system could "'malfunction or crash'" in the future.[129] In addition to any problem directly associated with Verio's continued searches, the court emphasized Register.com's concerns that if Verio's robotic searches were deemed lawful, "'then every purveyor of Internet-based services would engage in similar conduct.'"[130] In granting the preliminary injunction against Verio, the court concluded "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."[131] Thus, even if unwanted electronic signals have not yet caused any damage, the risk of future damage seems sufficient to sustain a trespass to chattels claim.

In contrast to the rather liberal standards for assessing the existence of damage articulated in *Bidder's Edge* and *Register.com*, another recent

125. *Id*. at 249.
126. *Id*. at 250.
127. *Id*. (citing eBay Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d at 1071 (citing CompuServe v. Cyber Promotions, Inc., 962 F. Supp. 2d 1012, 1022 (S.D. Ohio 1997))).
128. *Id*. (emphasis added).
129. *Id*.
130. *Id*. at 250.
131. *Id*.

federal court ruled that minor interference with a computer system as a result of robotic searching would not satisfy the damage element necessary for a trespass to chattels claim to continue. In *Ticketmaster Corp. v. Tickets.com, Inc.*, a California magistrate judge denied Ticketmaster's request for a preliminary injunction against Tickets.com, a ticket clearinghouse company that uses robotic search technology to collect ticket sale information from a variety of online ticket sellers, including Ticketmaster.[132] The court purported to follow *Bidder's Edge* with respect to the damages required. Rather than adopting the *Bidder's Edge* logic that simply using or occupying "some" portion of another's computer network satisfies the damage element, the *Ticketmaster* court concluded that Tickets.com's use of the Ticketmaster computer network "appears very small and there is no showing that the use interferes to any extent with the regular business of [Ticketmaster]."[133] In addition, while embracing the general notion expressed in *Bidder's Edge* that a threat of future harm might satisfy the damage element, the court noted that there was no "specture [*sic*] of dozens or more parasites joining the fray, the cumulative total of which could affect the operation of [Ticketmaster's] business."[134] Thus, the court implicitly rejected the liberal "use" damage threshold set forth in *Bidder's Edge* and adopted a much higher actual damage requirement. In the end, the court rather equivocally acknowledged that the trespass claim had "some merit" but concluded more substantial actual damages were necessary to support a valid trespass cause of action.[135]

Approximately one year later, however, another California federal court explicitly rejected the approach of *Ticketmaster* and once again returned to the mere "use" damage threshold.[136] In *Oyster Software, Inc. v. Forms Processing, Inc.*, an Internet software company, Oyster Software, brought a trespass to chattels claim against Forms Processing for using robotic searches (performed over the Internet by one of its subsidiaries) to copy a small amount of information from the Oyster Web site.[137] In denying Forms Processing's motion for summary judgment, the court discussed the level of damages necessary to support a trespass to chattels claim in light of both *Bidder's Edge* and *Ticketmaster*.[138]

132. No. 99CV7654, 2000 WL 1887522, at *1 (C.D. Cal. Aug. 10, 2000).
133. *Id.* at *4.
134. *Id.*
135. *Id.*
136. Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382 at *13 (N.D. Cal., Dec. 6, 2001).
137. *Id.* at *1–*3.
138. *Id.* at *12–*13.

At the outset, the court noted that Bidder's Edge previously rejected the requirement of "substantial interference" with personal property. While noting that *Bidder's Edge* had acknowledged some uncertainty regarding the absolute minimum level of interference necessary to sustain a trespass action, the court stated that even a "negligible" interference with the computer network of another was sufficient to prevail on a trespass claim.[139] Interpreting the standard set forth in *Bidder's Edge*, the court explained that

> [w]hile the *eBay* decision could be read to require an interference that was more than negligible (as did the court in *Ticketmaster*), this Court concludes that *eBay*, in fact, imposes no such requirement. Ultimately, the court in that case concluded that the defendant's conduct was sufficient to establish a cause of action for trespass not because the interference was "substantial" but simply because the defendant's conduct amounted to "use" of the Plaintiff's computer.[140]

Because Oyster presented evidence that robotic searches performed by Forms Processing amounted to "use" of Oyster's computer systems, the court denied Form Processing's motion for summary judgment.

So does existing case law lend any insight into the application of a trespass to chattels claim to cookie technology? Although a complete argument for recognizing a trespass to chattels claim in the context of cookie technology will be developed more fully below, the cases addressing the Internet and unauthorized information access seem to provide a solid foundation for building a case in several important respects. First, with respect to the interference element of a trespass claim, simply sending electronic signals or merely using another's computer network seems to suffice. Second, in order to fulfill the damage requirement, no demonstration of presently quantifiable harm is necessary. Instead, the damages element could be satisfied either from the "negligible" harm that necessarily arises from mere "use" of another's computer network or even through the risk of any future harm that might arise. Finally, while making a computer system available for use by another might represent some form of consent, that consent can be easily revoked, either explicitly or implicitly through filing suit to halt the unwanted access.

139. *Id*. at *12.
140. *Id*. at *13.

2. Bulk E-mails or "Spam"

In addition to court decisions addressing unauthorized information access, a small number of cases involving bulk e-mails or "spam" shed further light on the shape a trespass claim might take in the realm of cookie technology. Although bulk e-mail cases have arisen in only a few jurisdictions, the courts have recognized a valid trespass to chattels claim in each instance considered. Perhaps more important, the rulings as a whole reflect a consistently supple approach regarding the application of common law trespass principles to the Internet and to the computer hardware through which we access the Internet itself.

In the earliest and most cited case, *CompuServe, Inc. v. Cyber Promotions, Inc.*, a federal district court in Ohio relied on trespass to chattels grounds to enjoin an Internet advertising firm from sending unsolicited bulk e-mails to any e-mail addresses maintained by CompuServe, a popular Internet service provider.[141] At the outset, the court adopted a flexible view with respect to the basic concept of committing a trespass through intangible electronic signals. Citing *Thrifty-Tel*, the court noted that sending electronic signals alone, even without any "substantial interference" with CompuServe's network, constituted sufficient contact to support a trespass cause of action.[142] With respect to the element of damage, although CompuServe alleged lost customer subscriptions and a diminished server capacity as a result of the "spam" advertising, the court emphasized that actionable damages would result simply if the unwanted contacts impaired in some way the "quality, condition, or value" of CompuServe's network.[143] Because the bulk e-mails sent by Cyber Promotions "demand the disk space and drain the processing power of [CompuServe's] computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment is diminished, even though it is not physically damaged by defendant's conduct."[144] Consistent with the approach adopted in the cases addressing unwanted information access, then, the court in *CompuServe* applied the trespass requirements rather flexibly to cover unwanted bulk e-mails, at least with respect to what constitute interference and damage.

With respect to the issue of consent, however, the *CompuServe* decision articulated a somewhat stringent standard that required giving

141. CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017–18 (S.D. Ohio 1997).
142. *Id*. at 1021.
143. *Id*. at 1022.
144. *Id*.

prior notice regarding any limitations on authorized use. Central to the arguments presented by the parties and to the court's opinion was the special position that CompuServe occupied as an Internet service provider, an essential intermediary through which CompuServe customers accessed the Internet and communicated via e-mails with the public at large. Although Cyber Promotions argued that CompuServe had consented to the bulk e-mails by making its network generally open to public Internet traffic, the court refused to adopt the argument that all Internet users had been implicitly authorized to use CompuServe's system in any manner desired. Instead, the court determined that CompuServe's network was private property and consent to use that private property could be revoked or modified at any time. To assess the question of what authorization others had to use the CompuServe network, the court pointed to an online policy statement published by CompuServe that explicitly prohibited sending unsolicited e-mails using CompuServe computer systems. While noting that the policy statement alone might not have provided sufficient notice of the limitations that CompuServe placed on the use of its network, the court also explained that Cyber Promotions was sent a specific notice indicating that the bulk e-mails were unacceptable.[145] Even though the court rejected Cyber Promotion's argument that the CompuServe network represented a public utility to which access could not be restricted, the court still seemed to couch its discussion of consent in light of the general public expectation that e-mail communication should be unfettered absent explicit limitations. Thus, the court incorporated a notice element into the concept of intent, stating "[t]o prove that a would-be trespasser acted with the intent required to support liability in tort it is crucial that defendant be placed on notice that he is trespassing."[146] Following that approach, the court placed heavy weight on that specific notice sent to Cyber Promotions regarding activity to which CompuServe had not consented and the injunction was granted.

Because the court somewhat conflated the concepts of intent and notice, however, it remains unclear whether or not the notice requirement applies generally to all instances of trespass or just to cases where there is some common expectation of use absent an explicit limitation. After all, it would seem rather odd to conclude that a thief who picked the lock on my front door lacked the intent to trespass on my property simply because I failed to provide sufficient notice to the thief that he should not enter the apartment for the purpose of stealing my television. In any event, at least

145. *Id*. at 1024.
146. *Id*.

with respect to the special circumstances described in *CompuServe*, the court concluded no trespass could arise without sufficient warning that the bulk e-mails were unwanted.

In *Hotmail Corp. v. Van$ Money Pie Inc*., a California federal court granted a preliminary injunction preventing various Internet advertisers from sending bulk e-mails using a computer network owned by Hotmail, an Internet service provider that offered free e-mail accounts to the public.[147] The district court initially noted that the "the computers, computer networks and computer services that comprise Hotmail's e-mail system" were the private property of Hotmail; therefore, consent to use the system could be modified or revoked at any time.[148] Although the defendants had obtained implicit consent to set up Hotmail e-mail accounts, that authorization was limited to use of the e-mail system within the parameters set by Hotmail. Because spamming was expressly prohibited by the "Terms of Service" posted on Hotmail's Web site, the court concluded that by sending bulk e-mails, the Internet advertisers exceeded the scope of consent and thereby trespassed on Hotmail's network. Thus, with respect to the issue of consent, the court avoided the *CompuServe* approach that entangled the concepts of intent and notice. Instead, even though the court relied on the notice Hotmail provided regarding the limitations placed on the use of its e-mail network, the court framed its approach based on the revocation of implicit authorization already granted rather than on the advertisers' intent to commit the acts (sending bulk e-mails) that gave rise to the trespass itself.

In terms of damages, while the injuries suffered were not quantified by the court, the harms that the court cited included diminished storage space, a risk of impairment to future service, increased personnel costs necessary to deal with the bulk e-mail problem and harm to Hotmail's business reputation and goodwill.[149] Therefore, not only were the risks of future harms sufficient to satisfy the damages element, an unquantifiable, yet negative impact on business intangibles (such as good will and reputation) surpassed the minimum damage threshold as well.

147. Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *1–*2 (N.D. Cal. 1998).

148. *See id.* at *7.

149. *Id*.

In a trio of cases involving America Online ("AOL"),[150] courts applying Virginia law found that Internet advertisers trespassed on AOL's computer network by sending unauthorized bulk e-mails to AOL subscribers. In the first case, *America Online, Inc. v. IMS*, the district court granted AOL's motion for summary judgment against a firm that allegedly sent over 60 million unsolicited e-mails to AOL customers.[151] Explicitly adopting the approach of *CompuServe*, the court noted in summary fashion that the advertiser "intentionally caused contact with AOL's computer network by sending bulk e-mail messages," that the "contact with AOL's computer network was unauthorized" and that the "contact with AOL's computer network injured AOL's business good will and diminished the value of its possessory interest in its computer network."[152] Although no damages were quantified, the court accepted AOL's undisputed allegations that the unauthorized e-mails "burdened" AOL's equipment, cost "time and money" to process the messages, required devoting "technical resources and staff" to address the spamming problem and diminished "goodwill" among AOL's members. Noting that the spamming continued even after AOL sent a cease and desist letter, the court granted summary judgment concluding there was simply no "factual dispute" that the advertisers were liable on trespass to chattels grounds.

Around the same time, in *America Online, Inc. v. LCGM, Inc.*,[153] another Virginia district court granted AOL's motion for summary judgment against an Internet spam advertiser on trespass to chattels grounds. Citing *CompuServe*, *Hotmail* and *IMS* as support, the court found that simply sending electronic signals to the AOL network constituted sufficient intentional, physical contact and that any impairment whatsoever to the "'condition, quality, or value'" of AOL's computer systems sufficed to support a trespass claim.[154] On the issue of consent, however, the court distanced itself somewhat from the rather stringent notice requirement set forth in *CompuServe*. The court noted that the e-mails were unauthorized solely because the AOL "Terms of Service" prohibited bulk e-mailing. While *CompuServe* placed greater emphasis on the additional notice sent specifically to the advertisers, the court in *LCGM* explained in a footnote that the lack of consent was simply "further

150. *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1277 (N.D. Iowa 2000); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–55 (E.D. Va. 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998).

151. *IMS*, 24 F. Supp. 2d at 549–50.

152. *Id*. at 550 n.2.

153. *LCGM*, 46 F. Supp. 2d at 444.

154. *Id*. at 452 (citing RESTATEMENT (SECOND) OF TORTS § 218(b)).

demonstrated" by the fact that the advertisers had received "cease and desist letters from AOL."[155]

Completing the trio is *America Online, Inc. v. Nat'l Health Care Discount, Inc*.[156] Applying Virginia law, an Iowa district court found that an independent advertising contractor hired by a health care company had trespassed on AOL's personal property by sending unsolicited bulk e-mail messages. Although the court cited *America Online v. IMS* in discussing the nature of a trespass claim generally, the court summarily referred to factual findings in a prior hearing to support the application of trespass principles to cover the bulk e-mails at issue in the present case. In the end, the court actually denied AOL's motion for summary judgment against the health care company because the issue of the e-mail contractor's agency status was a question of fact.[157] Of course, the lack of a full discussion of the trespass claims undermines the usefulness of the decision, at least in terms of understanding how the facts might enhance or restrict the principles discussed in earlier cases. In any event, the court noted that AOL had "established a *prima facie* case of trespass to chattels" against the contractor.[158]

Finally, in yet another California case, *Intel Corp. v. Hamidi*,[159] a state appellate court upheld a summary judgment order against Kenneth Hamidi, an Intel employee who had sent only six bulk e-mails concerning the company's employment practices to over 30,000 employees.[160] Citing *Thrifty-Tel*, *CompuServe* and the trio of cases involving AOL, the court determined that Hamidi had committed an actionable trespass by using Intel's e-mail system against the guidelines published by the company. Although Intel consented to its employees' use of company computers to access the Internet and the firm e-mail network, exceeding the terms of use set forth by the company revoked that consent. Moreover, the court

155. *Id*. at 452 n.4.

156. Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255 (N.D. Iowa 2000).

157. *Id*. at 1280.

158. *Id*. at 1277.

159. Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244 (Ct. App. 2001), *review granted and opinion superceded by* Intel Corp. v. Hamidi, 43 P.3d 587 (2002).

160. In *Intel Corp. v. Hamidi*, the California Supreme Court granted review of the Appellate Court ruling. While the Appellate Court decision was previously published, according to California Court Rule 976, "no opinion superseded by a grant of review, rehearing, or other action shall be published. After granting review, after decision, or after dismissal of review and remand as improvidently granted, the Supreme Court may order the opinion of the Court of Appeal published in whole or in part." CAL. R. CT., R. 976(d) (2002). Therefore, while review is pending in the California Supreme Court, the Appellate Court decision may not be cited as authority in any court except under limited circumstances. CAL. R. CT., R. 977(b) (2002).

rejected Hamidi's claim that Intel suffered no injury, stating instead that the damage threshold had been met by a showing that the e-mails drained disk space, diminished the network's processing power, hampered employee productivity or required expending resources to block the e-mails.[161] But that list of actual damages was not even necessary, because "where a company cannot precisely measure the harm caused by an unwelcome intrusion, the fact the intrusion occurs supports a claim for trespass to chattels."[162] In fact, stretching still further the notion of damages articulated in prior cases, the court noted that "even assuming Intel has not demonstrated sufficient 'harm' to trigger entitlement to nominal damages for past breaches of decorum by Hamidi, it showed he was disrupting its business by using its property and therefore is entitled to injunctive relief based on a theory of trespass to chattels."[163] Thus, according to the court in *Hamidi*, it seems as if almost no amount of damages would be too small to support a trespass cause of action.

In the end, the three America Online cases, in conjunction with *CompuServe*, *Hotmail* and *Hamidi*, demonstrate the effectiveness of trespass to chattels principles to impose liability or at least to survive summary judgment in the specific context of unsolicited bulk e-mails.[164] And more generally, the malleability with which courts have applied those principles suggests the boundaries for framing a trespass claim in the context of cookie technology might be equally flexible.

V. *DOUBLECLICK* REVISITED

Having examined the historical foundations of trespass, the basic common law elements of a trespass to chattels claim and existing case law involving trespass claims related to the Internet, we are poised to answer more intelligently the question that began our investigation. Are Internet advertising firms trespassing on our computers? Using the facts discussed

161. *Hamidi*, 114 Cal. Rptr. 2d at 250–52.

162. *Id*. at 249.

163. *Id*.

164. The Eastern District of Virginia also briefly considered another trespass to chattels claim in *America Online, Inc. v. GreatDeals.net*, 49 F. Supp. 2d 851 (E.D. Va. 1999). After citing its prior decisions in *LCGM* and *IMS*, the court summarily stated without elaboration that GreatDeals had committed a trespass in sending unsolicited bulk e-mails over the AOL network. *Id*. at 861, 864–65. More recently, in *Verizon Online Services, Inc. v. Ralksy*, 203 F. Supp. 2d 601 (E.D. Va. 2002), Verizon brought a suit against a variety of defendants for sending millions of bulk e-mails over its Internet service. Although the court acknowledged that "[s]everal courts, including this one, have held that under certain circumstances, the transmission of UBE [unsolicited bulk e-mails] through a computer system constitutes the tort of trespass to chattel," the case was in the early stages of litigation and only procedural issues were before the court. *Id*. at 606.

in *DoubleClick* as a platform for analysis, the answer seems to be "yes." With respect to each of the elements of a trespass claim and even the defense of consent, a strong case exists for concluding that the use of cookie technology renders Internet advertisers liable on common law trespass to chattels grounds.

A. TANGIBLE PROPERTY

Recent cases do not leave much doubt that an individual's computer hard drive and the memory capacity occupied by DoubleClick's cookie files constitute sufficiently tangible property to support a trespass to chattels claim. According to those cases, the concept of chattels includes computer networks, Internet servers, information databases, hardware and software, virtual storage capacities, e-mail programs, telephone codes, communications systems generally and the very electronic signals through which those systems operate.[165] That very broad understanding of what qualifies as a chattel certainly envelopes the hard drive of an individual's computer and with quite a bit of room to spare at that. After all, if e-mail programs, telephone codes and information databases that exist only as digital signals stored on a computer system represent sufficiently tangible property to support a trespass claim, it seems necessary from a conceptual standpoint that the physical hard drive on which that ephemeral electronic data is stored must be sufficiently tangible as well. As a rather simple threshold matter, then, the computer hard drives and memory capacities on which DoubleClick planted its cookie files satisfy the tangibility requirement of a trespass claim.

165. *See generally* Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382 (N.D. Cal. 2001) (involving computer systems and computer capacity); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (discussing electronic databases and Internet server capacity); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255 (N.D. Iowa 2000) (discussing computer networks and e-mail systems); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (addressing information databases, computer systems, virtual storage capacity, computer equipment and Internet server capacity); Ticketmaster Corp. v. Tickets.com, Inc., 2000 WL 1887522 (C.D. Cal. 2000) (concerning computer equipment, computer functions and electronic impulses); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998) (involving computer networks, computer equipment and e-mail systems); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998) (concerning computer networks, computer equipment and e-mail systems); Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389 (N.D. Cal. 1998) (addressing computer networks, computer services and computer space); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (discussing computer equipment, software, disk space, processing power, e-mail programs and service); Intel Corp. v. Hamidi, 114 Cal. Rptr.2d 244 (Ct. App. 2001) (addressing e-mail systems, computer equipment, disk space and processing power); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Ct. App. 1996) (concerning electronic signals, computer networks and telephone codes).

B. DISPOSSESSION OR INTERFERENCE

The element of interference does not provide a terribly difficult hurdle to surmount in the context of DoubleClick's practices. By depositing, accessing and altering cookie files, DoubleClick rather clearly interfered with the possessory interest individuals maintain in their computers. As described in *Thrifty-Tel* and embraced by several later courts, simply sending electronic signals to another's computer provides sufficient physical contact to support a trespass claim.[166] Even if DoubleClick were to claim that cookie files do not significantly affect the ability of the computer to operate, no substantial interference is required. Instead, mere "use" of the computer system or occupying some small portion of memory capacity suffices to establish the requisite level of interference.[167] The cookie files that DoubleClick deposited on the computers of Internet users undeniably occupied some portion of the memory capacity. Moreover, each time DoubleClick accessed or altered the information contained in the cookie files, DoubleClick used an individual's computer system or data in much the same way that robotic search programs scour data contained on an Internet server or that an individual sends e-mail. Given the rather low threshold set by existing case law, DoubleClick almost certainly interfered with private property by depositing, accessing and altering cookie files on the computers of Internet users.

C. INTENT

Once again, satisfying the element of intent does not provide much difficulty in the context of DoubleClick. As set forth in the Restatement, the intent required need not involve any wrongful motive. To the contrary, as long as the acts which constitute the interference or dispossession were voluntary, the requisite intent exists.[168] Perhaps because the intent required remains so minimal, most cases discussing trespass claims in the context of computers and Internet technology just assumed the necessary intent was present, especially in light of the clear commercial motivation driving most

166. *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473 nn.6–7. *See also CompuServe*, 962 F. Supp. at 1015; *IMS*, 24 F. Supp. 2d at 548; *LCGM*, 46 F. Supp. 2d at 444; *Nat'l Health Care Disc.*, 121 F. Supp. 2d at 1255.

167. *Oyster Software*, 2001 U.S. Dist. LEXIS 22520 at *13; *Bidder's Edge*, 100 F. Supp. 2d at 1070–71; *Register.com*, 126 F. Supp. 2d at 250; *CompuServe*, 962 F. Supp. at 1015; *Intel*, 114 Cal. Rptr. 2d at 244.

168. *See supra* notes 100–02 and accompanying text.

instances of computer trespass.[169] With respect to DoubleClick, claiming that the cookies were deposited and maintained as a result of some accident or mistake seems quite unlikely. Instead, cookie technology played and continues to play an important role in DoubleClick's basic business operations. Therefore, it seems readily apparent that DoubleClick purposefully and intentionally placed cookie files on the computer hard drives of Internet users.

Although DoubleClick might contend that it lacked the specific intent to trespass due to the absence of any explicit notice from Internet users regarding their aversion to unwanted cookie files, specific intent is not required by the Restatement or well supported in the relevant case law. Still, the court in *CompuServe* explicitly stated that in order to satisfy the intent element, "it is crucial that defendant be placed on notice that he is trespassing."[170] But as already explained, that assessment seemed to conflate the concepts of intent and notice.[171] The court relied heavily on the unique nature of CompuServe as an Internet service provider and attempted to address what it described as "at least a tacit invitation for anyone on the Internet to utilize [CompuServe's] computer equipment to send e-mail to its subscribers."[172] Considering that the court found some "tacit invitation" was given to the public at large, the notice that the court required related more sensibly to a revocation of some implied authorization to use CompuServe's property rather than to the intent of Cyber Promotions to send the bulk e-mails. In any event, even if DoubleClick were to rely on a simple reading of *CompuServe* regarding the relationship between notice and intent, the Restatement expressly rejects the requirement of specific intent in the context of trespass to chattels and no other court has followed *CompuServe* in requiring some motive of wrongdoing to sustain a trespass claim.[173] In the end, DoubleClick could certainly attempt an argument that it lacked the specific intent to commit a trespass, but that position misconstrues the nature of the intent required and the opinions of the vast majority of cases addressing trespass to chattels.

169. *See, e.g.*, *Oyster Software*, 2001 WL 173682 at *11, *12; *Bidder's Edge*, 100 F. Supp. 2d at 1069–70; *Register.com*, 126 F. Supp. 2d at 249–50; *IMS*, 24 F. Supp. 2d at 550; *LCGM*, 46 F. Supp. 2d at 452; *Hotmail Corp*, 1998 WL 388389, at *1, *7.

170. *CompuServe*, 962 F. Supp. at 1024.

171. *See supra* notes 145–46 and accompanying text.

172. *CompuServe*, 962 F. Supp. at 1023–24.

173. According to the Restatement, sufficient intent exists

> when an act is done for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a substantial certainty, result from the act. It is not necessary that the actor should know or have reason to know that such intermeddling is in violation of the possessory rights of another.

RESTATEMENT (SECOND) OF TORTS § 217, at cmt. C. *See also* DOBBS, *supra* note 87, at 123.

D. DAMAGES

Because courts have set such a low level of damages needed for a trespass to chattels claim to survive, the damages resulting from DoubleClick's use of cookies would most likely surpass the required minimum. While actual damages are required to sustain a trespass to chattels claim, demonstrating presently quantifiable damages is wholly unnecessary. Instead, as existing cases make clear, sufficient damages may result from depriving another's "use" of some part of the computer,[174] occupying merely a "small" or "negligible" amount of disk space or memory capacity,[175] "slowing" processing capability,[176] creating a "risk" of future harm to computer capacity or system functions,[177] diminishing the "condition, quality or value" of the computer system,[178] causing effort and resources to be expended to block or correct the unwanted contacts,[179] diminishing "productivity,"[180] adversely affecting "reputation or goodwill"[181] or otherwise causing "mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels."[182] Thus, while the cases do not reject the need for actual damages, courts have adopted a very flexible notion of what constitute actual damages in the realm of computer technology.

In light of that broad approach to damages, the cookie files deposited by DoubleClick seem to cause ample damage, at least for a trespass claim to survive. At the outset, even if the cookie files occupy only a few kilobytes of disk space, occupying even a "negligible" amount of storage capacity creates sufficient damage. Moreover, by pirating that memory capacity, DoubleClick deprives the computer owners of the "use" of that virtual space. DoubleClick could counter that the files could be deleted and the memory capacity restored, but causing users to block or correct the

174. *Oyster Software*, 2001 WL 1736382, at *12; *Bidder's Edge*, 100 F. Supp. 2d at 1070.

175. *Id.* at 1071; Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 250 (S.D.N.Y. 2000); Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *7 (N.D. Cal. 1998); *CompuServe*, 962 F. Supp. at 1022; Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 250 (Ct. App. 2001).

176. *Register.com*, 126 F. Supp. 2d at 250; *CompuServe*, 962 F. Supp. at 1022.

177. *Register.com*, 126 F. Supp. 2d at 250; *Hotmail Corp*, 1998 WL 388389, at *7.

178. *Bidder's Edge*, 100 F. Supp. 2d at 1071; *Register.com*, 126 F. Supp. 2d at 250; Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 452 (E.D. Va. 1998); *CompuServe*, 962 F. Supp. at 1022.

179. *Intel*, 114 Cal. Rptr. 2d at 246.

180. *Id*. at 250.

181. *IMS*, 24 F. Supp. 2d at 550; *LCGM*, 46 F. Supp. 2d at 452; *Hotmail Corp.*, 1998 WL 388389, at *7.

182. *Register.com* , 126 F. Supp. 2d at 250.

unwanted cookie contacts presents cognizable damage as well. With respect to future harm, to the extent the profiles collected through the cookie technology were sold or not adequately protected, the cookies might expose individuals to snail-mail solicitations, telephone marketing campaigns or perhaps even theft of credit card numbers or other valuable personal data. Finally, if the "rental value" of the detailed consumer information that DoubleClick obtains were used as a measure (that is, the amount another company would pay for the right to place and maintain cookies on our computers), the money damages from the unauthorized use of cookies might be impressively substantial.[183] In fact, some firms have offered in-kind payments, worth $1,000, to purchase from individuals the right to collect and process their online consumer preferences.[184] But regardless of the actual amount of damages suffered, DoubleClick's cookies seem to cause damages well in excess of the minimum quantum necessary to support a trespass to chattels claim.

E. CONSENT AND AUTHORIZATION

While establishing a prima facie case against DoubleClick with respect to each of the basic elements of trespass might not pose much difficulty, assessing the defense of consent poses a bit more of a challenge. In addition to examining the approach taken in *DoubleClick*, *Intuit*, *Avenue A* and *Pharmatrak*, evaluating the merits of the defense requires a deeper look into the kinds of consent or authorization that DoubleClick might generally claim. Although DoubleClick could present a somewhat stronger set of arguments regarding consent than on any of the basic elements of a trespass claim, the notion that the millions of us who use the Internet knowingly authorized DoubleClick to create and maintain personal data files on our computers seems weak at best.

While Internet advertisers obtained favorable outcomes in *DoubleClick*, *Intuit*, *Avenue A* and *Pharmatrak*, those four cases do not provide a particularly sound argument for DoubleClick to claim that Internet users consented to the placement of cookies under a trespass to chattels theory. Recall that the issue of authorization in each of those cases was discussed in light of the precise language and legislative history

183. *See* DOBBS, *supra* note 87, at 124.

184. Karen Kaplan, *In Giveaway of 10,000 PCs, The Price is Users' Privacy Marketing: Recipients Must Agree to Let Pasadena Firm Monitor Where They Go on Internet and What They Buy*, L.A. TIMES, Feb. 8, 1999, at A1. *See also* Lawrence Jenab, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 U. KAN. L. REV. 641, 648 (2001).

surrounding three federal statutes, namely the ECPA, the CFAA and the Wiretap Act. Although consent provided a defense to liability under each of those statutes, the kind of consent required was either different in nature than the consent relevant to a trespass to chattels claim or, in the case of the CFAA, the courts simply did not reach the issue of authorization because the statutory claim failed on other grounds. And even within that peculiar statutory discussion of consent, the court in *Intuit* actually accepted the class of Internet users' allegation that DoubleClick lacked sufficient consent to use cookies as part of its targeted advertising scheme.

In *DoubleClick*, for instance, the court first addressed the issue of consent within the context of the ECPA. But as interpreted by the court, the precise language of the statute did not require consideration of consent from individual Internet users. Instead, the court limited its assessment of consent to any authorization provided by a "facility" or an entity through which electronic communication was provided. As interpreted by the court, the term "facility" was construed to cover Web sites or servers but not the individual computers of Internet users. Based on that statutory construction, the court determined that no liability under the ECPA arose because the Web sites (or "facilities" under the statute) with which DoubleClick contracted had authorized DoubleClick to receive the cookie files.[185] Regarding the Wiretap Act, the statute exculpated a party for intentionally intercepting an electronic communication to the extent that one of the parties to the communication consented to the interception. Again, the court ignored the question of whether or not Internet users had offered their consent and focused instead on the consent given by the Web sites that were contractually affiliated with DoubleClick. Since the DoubleClick affiliated Web sites clearly consented to DoubleClick's interceptions of the cookie data files, the Wiretap Act did not impose liability.[186] Finally, with respect to the CFAA, the consent issue was simply not reached. Because the court found that the damages for any particular instance of accessing cookie data fell far below the $5,000 statutory minimum, the CFAA claim was dismissed as well.[187] Within the context of the specific provisions addressed by the court, the issue of whether or not Internet users consented to DoubleClick's placement of cookie files was never considered. Thus, the *DoubleClick* decision could not serve as effective authority for establishing in the context of a trespass to chattels claim that DoubleClick had some prior consent to deposit,

185. *See supra* notes 26–29 and accompanying text.
186. *See supra* notes 30–34 and accompanying text.
187. *See supra* notes 35–37 and accompanying text.

access and alter the cookie files on the computers of individual Internet users.

Due to limitations on the notion of consent imposed by the statutory context, the decision in *Avenue A* is similarly inapposite as well. In *Avenue A*, the court closely followed the approach articulated in *DoubleClick* with respect to each of the federal claims. While Avenue A was an intermediary with which DoubleClick had contracted to place banner ads on its behalf, that slight factual wrinkle did not affect the applicability of the reasoning expressed in *DoubleClick*. Wholeheartedly embracing the *DoubleClick* ruling, the court dismissed the ECPA claim based solely on the consent given by DoubleClick's affiliated Web sites to access the cookie files deposited on the computers of Internet users. Under the terms of the statute, consideration of consent from the perspective of the Internet users was again simply irrelevant.[188] With respect to the Wiretap Act, the court found no liability, because the DoubleClick affiliated Web sites had consented to the interception of the cookie data by Avenue A on behalf of DoubleClick.[189] And once again, the court found the CFAA unavailing because the minimum damage level could not be met for any particular instance of accessing the data contained in the cookie files.[190] Just as in *DoubleClick*, Avenue A certainly obtained a favorable result with respect to the federal claims at issue in the case. But also just as in *DoubleClick*, the peculiar statutory context within which the court construed the question of consent makes it inappropriate to use the case as authority for establishing that Internet advertisers enjoy some overarching consent to deposit and access cookie files.

The recent opinion in *Pharmatrak* similarly provides wholly inadequate grounds upon which to construct a consent defense in the context of a trespass to chattels claim. While *Pharmatrak* involved a Web monitoring firm rather than an Internet advertiser, the court parroted much of the opinions in *DoubleClick* and *Avenue A*. With respect to the ECPA, the court again focused on the term "facility" to limit the ambit of the statute. Adopting the statutory construction articulated in *DoubleClick*, the court simply stated that a personal computer was not a facility within the meaning of the legislation. Relying on that specific statutory construction, the court limited its analysis of consent to whether or not the drug companies that operated the Web sites had authorized Pharmatrak to access

188. *See supra* notes 52–55 and accompanying text.
189. *See supra* notes 56–59 and accompanying text.
190. *See supra* notes 60–62 and accompanying text.

the cookie files.[191] Because Pharmatrak had contracted with the drug companies to monitor the use of their Web sites, the court handily concluded sufficient consent existed. Likewise with respect to the Wiretap Act, the court focused only on the consent given by the drug companies. Since Pharmatrak was retained to track activity on the drug company sites, the court determined that Pharmatrak was authorized to intercept any communications between the drug companies and individual Internet users.[192] And following both *DoubleClick* and *Avenue A*, the court simply did not reach the issue of consent under the CFAA, because the statutorily prescribed minimum damage level could not be satisfied for any single instance of accessing the cookie files. Because the specific statutory provisions at issue in *Pharmatrak* caused the court to ignore entirely the issue of consent from the perspective of individual Internet users, the case does not provide adequate grounds for establishing that DoubleClick possessed authorization sufficient to combat a common law trespass claim.

Even if DoubleClick insisted the concept of consent discussed in some specific statutory context should control, the decision in *Intuit* actually undermines the claim that DoubleClick possessed adequate consent. With respect to the CFAA and Wiretap Act claims, however, the court in *Intuit* dismissed the claims using the same reasoning expressed in both *DoubleClick* and *Avenue A*.[193] But with respect to the ECPA, the court adopted a different tact. Construing the term "facility" as used in the ECPA to cover the computers of Internet users and not just Web sites or Internet servers, the focus of the consent consideration shifted to include Internet users as well. Because Internet users had alleged they did not authorize the placement of any cookie files by Intuit, the court refused to dismiss the ECPA claim. So even within the limited statutory context of the ECPA, then, the basic structure of Internet communication does not necessarily grant Web sites or advertisers some implied authorization to plant cookies on our computers.

Thus, the decisions in *DoubleClick*, *Avenue A*, *Intuit* and *Pharmatrak* do not provide a convincing platform from which DoubleClick could argue that it possessed sufficient consent to deposit cookie files on the individual computers of Internet users. Because the meaning of consent was controlled by the precise language of the statutes considered, those cases remain inapposite to the issue of consent within the context of a trespass to chattels claim. And as the decision in *Intuit* demonstrates, even within the

191. *See supra* notes 66–71 and accompanying text.
192. *See supra* notes 72–75 and accompanying text.
193. *See supra* notes 39–49 and accompanying text.

confines of some limited and arguably irrelevant statutory framework, the basic mechanics of Internet technology do not mandate the conclusion that Internet users automatically consent to the use of cookies.

But within the common law context of trespass to chattels, what kind of consent argument might DoubleClick advance? To establish consent, DoubleClick would have to argue that Internet users gave either actual or apparent authority to place cookies on their individual hard drives. A cursory analysis of the facts underlying DoubleClick's position reveals it is unlikely that DoubleClick (or DoubleClick affiliated Web sites) possessed either actual or apparent consent to place and manipulate cookie files on the computers of individual Internet users.

Establishing actual consent would present a particularly difficult challenge for DoubleClick. Actual consent represents the express willingness for an action to occur.[194] Whether the expression takes the form of words or actions, the ultimate question is whether or not the defendant reasonably believed that the words or actions reflected genuine consent.[195]

In the context of Internet advertising, establishing actual consent seems quite a stretch. Upon visiting a Web site, few (if any) sites immediately display a pop-up window containing a warning that states, "By viewing this site, you agree to the placement of a cookie file on your computer that will monitor your online preferences and potentially collect any information you submit over the Internet. Click 'OK' to continue." Perhaps DoubleClick might counter that even without such an explicit admonition, embedded within the policy statements of each affiliated Web site lies a statement to the precise effect of that warning. But would it really be reasonable for DoubleClick to assume that a typical Internet user has investigated the cookie policy statement contained on every affiliated Web site? Even if a Web site visitor in fact stumbled across such a cookie policy, would it be sensible for DoubleClick to assume that the individual understood what cookies are and the commercial purposes for which the detailed personal data might be dedicated? In light of some estimates that only forty percent of Internet users even know that cookie technology exists,[196] it seems rather unlikely that by accessing a site, individuals knowingly convey a "genuine consent" to the placement of cookie files.

194. *See* RESTATEMENT (SECOND) OF TORTS § 892; DOBBS, *supra* note 87, at 218.

195. DOBBS, *supra* note 87, at 218.

196. *See* Jenab, *supra* note 184, at 647 (reporting that a March, 2000 Business Week/Harris poll "indicate[d] that sixty percent of Internet users have never heard of cookies"); Rachel K. Zimmerman, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century*, 4

While some important precedent suggests that online postings can affect authorization, that case law undermines rather than supports DoubleClick's claim that its postings could garner actual consent to plant cookie files. Perhaps the strongest case upon which DoubleClick might rely is *America Online, Inc. v. LCGM, Inc.*, where the court concluded that posting use limitations within the "Terms of Service" section of AOL's Web site provided sufficient notice regarding its prohibition on bulk e-mails.[197] DoubleClick might contend that its online postings should suffice to define consent in the same manner that the AOL postings controlled the consent granted in *LCGM*. *LCGM*, however, can be distinguished on the simple grounds that AOL was limiting the authority it was granting to others regarding use of its own e-mail system rather than restricting the use of property over which it had no ownership interest. Moreover, there was a generally perceived authorization granted by AOL to its customers with respect to sending and receiving e-mails over the AOL network—one of the basic services provided by AOL. Thus, the posting by AOL represented an express modification of the general consent already provided to AOL customers regarding the use of AOL's network and the policy statements contained in the AOL Terms of Service had no effect on what AOL customers consented to with respect to their own property.

The circumstances surrounding any DoubleClick affiliated site postings, however, make LCGM's favorable posture regarding the effectiveness of online notices unavailable to DoubleClick. After all, because DoubleClick affiliated Web sites have no ownership interest in the hard drives of Internet users, *LCGM* does not simply create some right to place conditions on the use of another person's property. Furthermore, where the AOL posting responded to a general expectation that AOL had consented to the use of its e-mail system (based on AOL's existence as an Internet service provider), no such general expectation of consent to receive cookie files applies to typical visitors to a random Internet site. Therefore, contrary to supporting DoubleClick's position, *LCGM* more likely suggests that if an Internet user posted a notice on her computer indicating "I don't want cookies," that notice would be sufficient to modify any generally perceived consent regarding her amenability to cookies. Still, it seems the

N.Y.U. J. LEGIS. & PUB. POL'Y 439, 456 (2001) (arguing that "[f]urthermore, of the sites that do have [cookie] policies, many are accessible only if the user notices tiny print hidden at the bottom of the Web page . . . most users do not notice or read the privacy policies of the majority of the sites they visit"); Dick Kelsey, *Almost No One Rejects Cookies — Study*, NEWSBYTES NEWS NETWORK, Apr. 3, 2001, *available at* 2001 WL 2817264 (stating that "most surfers know little or nothing about [cookies]" and that only .68% of individuals disable them). *See also infra* note 199 and accompanying text.

197. Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 452 n.4 (E.D. Va. 1998).

notice would not even be necessary absent some reasonable expectation on the part of Web sites that Internet users had generally consented to the placement of cookie files in the first place. In any event, existing case law suggests that simply accessing an Internet site does not reflect the genuine willingness necessary to support a claim of actual consent to the placement of cookie files on an individual's computer.

Turning to apparent consent, no strong argument supports the notion that DoubleClick possessed apparent authority to deposit cookie files. In general, apparent authority is consent manifested through custom, prior dealings between parties or some other existing relationship regarding use.[198] For example, in many communities where purchasing Girl Scout cookies is a welcome and predictable ritual, an enterprising Scout could walk up to your front door without risking liability for trespass, unless you provided some notice to the contrary. To establish some apparent consent, then, DoubleClick would have to argue that Internet users shared some general understanding with DoubleClick (or its affiliated Web sites) regarding the use of cookies or had some standing relationship where the use of cookies was knowingly embraced.

But no such understanding or relationship that would support apparent consent seems to exist. While DoubleClick's placement of cookie files arguably might be habitual, the practice does not represent a shared custom accepted by the parties involved if the Internet users do not even know what cookies are or the uses to which DoubleClick might put those files.[199] Knowledge that a custom actually exists represents an essential prerequisite to offering consent through customary practice.[200] Moreover, even if Internet users enjoyed some purported benefits of cookies (for example, automatically recalled passwords, personalized Web pages, the presentation of local information, etc.), mere satisfaction with those benefits would say precious little about the users' knowledge of the underlying means to produce them. With respect to apparent authority, then, the basic rule

198. DOBBS, *supra* note 87, at 219–20. *See* SPEISER ET AL., *supra* note 88, at 687. *See, e.g.*, Smith v. VonCannon, 197 S.E.2d 524, 529 (N.C. 1973); Rawls & Assoc. v. Hurst, 550 S.E.2d 219, 224 (N.C. Ct. App. 2001); Colmus v. Sergeeva, 27 P.3d 166, 168 (Or. Ct. App. 2001).

199. *See* Jenab, *supra* note 184, at 647 ("When entities collect data through the use of surreptitious technological methods such as cookies and web bugs, individual users with an average level of sophistication are almost certainly unaware of the nonconsensual monitoring transaction(s) underlying the consensual surface transaction (i.e., viewing the website)"); Kelsey, *supra* note 196 (noting that "'[t]he obvious absurdity of this situation is that the average user is unaware of the cookies and the tracking'") (quoting Jason Catlett, privacy advocate and president of Junkbusters.com). *See also supra* note 196 and accompanying text.

200. *See* DOBBS, *supra* note 87, at 220.

remains that in order to offer consent through customary practice, a person must have prior knowledge that the custom in fact exists.[201] To the extent Internet users do not know about cookie technology, any failure of users to take affirmative steps to block cookies does not imply apparent consent to the cookies themselves.

Furthermore, if DoubleClick were able to establish that Internet users had given their actual or apparent consent to the placement of cookie files for some purposes, any use exceeding the scope of that consent would still subject DoubleClick to trespass liability.[202] Assuming for the moment that Internet users actually consented to the use of cookies in order to facilitate personalized greetings, screen preferences or other beneficial purposes, that limited consent would not allow cookies to be used to build detailed consumer profiles for targeted banner advertising. Instead, a trespass action could be avoided only if the cookie files deposited on individuals' hard drives were used solely for the purposes actually authorized.

DoubleClick might counter stating that Internet users who knowingly accepted cookies for some beneficial purposes revealed their apparent consent to the use of cookie technology generally. But that leap seems utterly unsupported by logic or law. If Internet users do not know that DoubleClick and its affiliated Web sites utilize cookie files for other potentially harmful applications in addition to the beneficial purposes about which the users know, it seems rather odd to discern that those Internet users have consented to those unknown and potentially harmful applications. After all, just because I invite someone into my home for one purpose does not imply that I consent to any action that person might take. For example, if I invite the cable repairman into my house to fix the reception on my television, it seems unlikely that invitation would serve as consent for the repairman to place a monitoring device in my television that records my viewing habits. Whether actual or apparent, the scope of consent is limited by the purposes for which the authority was originally granted.[203] Although some argument might exist that Internet users have authorized the use of cookies for some purposes, utilizing cookies to create detailed personal profiles for commercial advertising purposes would most likely exceed the scope of any consent granted.

201. *Id*.

202. *See id.* at 243. *See also* Fletcher v. Conoco Pipe Line Co., 129 F. Supp. 2d 1255, 1262 (W.D. Mo. 2001); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 249 (S.D.N.Y. 2000); City of Amsterdam v. Goldreyer, Ltd., 882 F. Supp. 1273, 1281 (E.D.N.Y. 1995) (citing RESTATEMENT (SECOND) OF TORTS §§ 256, 892A (1965)).

203. 75 AM. JUR. 2d Trespass § 88 (1991); DOBBS, *supra* note 87, at 243–44. *See also* Matanuska Elec. Assoc. v. Weisler, 723 P.2d 600, 605 (Alaska 1986).

Finally, because consent may be modified or revoked at any time, even if Internet users had granted some form of consent to the use of cookie technology, the act of filing suit against DoubleClick arguably serves to rescind any prior authority to deposit and access cookie files. Recall that in *Register.com*, the court found that the online policies published by Register.com did not clearly prohibit the use of Internet search robots. Still, the court inferred that the act of filing suit revoked any implicit authorization to use robotic search technology, stating "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."[204] To the extent Register.com serves as a guide, even if DoubleClick were able to make some tenable claim that it used cookies only with the actual or apparent consent of Internet users, the filing of the class action suits against DoubleClick (and its affiliated Web sites) may have revoked any consent previously granted. Thus, with respect to each of the elements of a trespass claim and the basic defense of consent, a rather tidy argument exists that DoubleClick and other Internet advertisers expose themselves to liability on trespass to chattels grounds by using cookie technology. In contrast to the rigid requirements of various statutory claims that prevented Internet users from gaining any redress against DoubleClick, the flexibility of the common law seems to provide a much more hospitable foundation upon which to base a successful claim.

VI. COOKIES, CLASS ACTIONS AND THE COMMON LAW

While common law trespass to chattels provides a rather accommodating theory within which to construct a claim against Internet advertisers, some practical or strategic considerations might affect the ultimate usefulness of the common law as the basis for a class action suit. After all, framing a class action suit within the context of the common law arguably creates a number of risks that could potentially undermine the feasibility of a class action suit at the outset. On the other hand, using the common law as a basis for liability creates distinct advantages as well. In the end, a proper assessment of the practical and strategic considerations surrounding a common law class action claim would inevitably turn on the precise circumstances of the case involved and the evaluation could vary as the common law itself evolves. Nonetheless, at least for the time being, the potential benefits of basing a class action claim on common law trespass to chattels grounds seem to outweigh the drawbacks that might exist.

204. *Register.com*, 126 F. Supp. 2d at 249.

A. POTENTIAL RISKS

Several significant problems may affect the very viability of a common law class action claim that attempts to impose liability on Internet advertisers for using cookie technology. Statutory laws may preempt a common law remedy, common law principles may vary from one jurisdiction to the next, some states may refuse to recognize a trespass to chattels cause of action at all and the prospect of low damages might render the project too risky for plaintiffs' firms to undertake.

1. Statutory Preemption

Because state or federal statutes may preempt common law principles, a class action based on trespass to chattels grounds might not be possible at the outset. As a basic principle of jurisprudence, Congress may modify or abolish any common law cause of action to the extent that its actions do not violate the Constitution. Similarly, a state may pass legislation superseding or abrogating a common law right as long as that legislation does not violate either the state or federal constitution.[205] While statutes may directly derogate the common law, if a statute provides a similar remedy to that afforded under a common law right, courts will generally consider the statutory remedy as providing an additional cause of action. Therefore, only if the intention to supersede or repeal a common law right is clear will courts deem the statute to have abrogated the common law. Without that clear intention, courts generally attempt to interpret statutes in a manner consistent with existing common law principles.[206]

With respect to the application of common law trespass to chattels principles to cookie technology, statutory preemption does not present a current problem. Although all fifty states and the federal government have passed a variety of laws addressing computer crimes or Internet communication generally,[207] none of those statutes explicitly repeals a

205. MARTIN WEINSTEIN, SUMMARY OF AMERICAN LAW 102 (1988). *See also* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1026 (S.D. Ohio 1997) ("Indeed, if there were some applicable statutory scheme in place this Court would not be required to apply paradigms of common law to the case at hand.").

206. *See* Intel v. Hamidi, 114 Cal. Rptr. 2d 244, 252 (Ct. App. 2001); WEINSTEIN, *supra* note 205, at 102; Steven E. Bennett, *Canning Spam:* CompuServe, Inv. v. Cyber Promotions, Inc., 32 U. RICH. L. REV. 545, 560 (1998).

207. *See* Raymond T. Nimmer, THE LAW OF COMPUTER TECHNOLOGY § 12.4 (3rd ed. 1997). "By the end of the 1980s, forty-eight states had adopted criminal statutes tailored to interests in computer systems, information, and related materials." *Id*. §§ 10:11, 12:4, 12:17, 12:18, 12:28 (discussing various civil and criminal statutes under state and federal law). *See also* VT. STAT. ANN. tit. 13, § 2021 (2002) (setting forth certain computer crimes under Vermont law); Briggs v. State, 704 A.2d 904, 910

common law claim of trespass to chattels in the context of computer technology. Moreover, no court has yet interpreted any state or federal statute to abrogate common law trespass principles in that particular context. To the contrary, the very cases that rejected the federal statutory claims that Internet users brought against DoubleClick and other Internet advertisers implicitly recognized the potential viability of a trespass to chattels claim in the context of the Internet.[208] While still a potential problem in the future, statutory preemption does not create any current impediment to bringing a common law class action claim based on trespass to chattels.

2. Inconsistent Law

Because common law principles may vary depending on the jurisdiction, it may not be possible to bring a single class action suit that covers all Internet users in the United States. Although the basic elements of a trespass to chattels claim seem rather constant, some slight variations may still arise that would make the substance of trespass claims different, perhaps, for residents of Virginia compared to residents of California. Of course, no such jurisdictional variation exists for class actions based on federal statutes.

Still, as the common law currently stands with respect to trespass claims, sufficient similarity may exist to join plaintiffs from one jurisdiction to the next.[209] And even if a class were limited to residents of a single state, it seems likely that there would be plenty of Internet users within that jurisdiction to support a statewide class action claim. After all, current estimates peg the number of overall Internet users in the United States between 143 and 175 million.[210] So, even if damages were rather

n.7 (Md. 1998) (citing federal statutes and legislation addressing computer crimes in every state except Vermont).

208. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 523 (S.D.N.Y. 2001) (discussing a prior valid trespass claim against AOL); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001) (refusing to address "novel and complex issues of state law" after declining jurisdiction over common law trespass claim). *In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 15 (D. Mass. 2002) (avoiding discussion of the merits of common law trespass claim after declining jurisdiction over other state law matters).

209. *See, e.g.*, Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (stating "the trespass law of Virginia is so close to that of Ohio, we will rely on the reasoning of CompuServe [decided under Ohio law]").

210. *See* U.S. DEP'T OF COMMERCE, A NATION ONLINE, HOW AMERICANS ARE EXPANDING THEIR USE OF THE INTERNET 7 (Feb. 2002); GLOBAL REACH, GLOBAL INTERNET STATISTICS: SOURCES & REFERENCES, *at* http://global-reach.biz/globstats/refs.php3#us (last modified Mar. 31, 2003) (indicating that there are 173.1 million Americans currently online).

minimal per Internet user, a suit on behalf of one million users in a typical state might still generate the legal fees (assuming a one-third contingency) to make the class action worthwhile for a plaintiffs' firm to pursue. Thus, while inconsistent laws could diminish the number of plaintiffs and the amount of expected damages in any single class action, the fact that some states interpret common law principles differently would not render a class action claim wholly unattractive in any particular jurisdiction.

3. Trespass to Chattels Not Recognized

To the extent courts in any particular jurisdiction expressly refuse to recognize a trespass to chattels claim or perhaps explicitly reject extending trespass theory to cover computer technology, a common law class action within that jurisdiction would certainly fail. To date, however, no jurisdiction has explicitly refused to recognize trespass to chattels as a valid common law tort claim. And with respect to those jurisdictions that already have considered common law trespass claims in the context of computer technology, courts have without exception interpreted trespass to chattels principles to embrace various electronic contracts involving computers, including communication that occurs over the Internet.[211] Thus, while the inchoate nature of the common law with respect to trespass to chattels and computers presents some risk, the current state of the common law seems quite favorable to a class action trespass claim.

4. Low Damages

Although low damages are not a formal impediment to bringing a trespass to chattels claim, the availability of only some minimal financial award could undermine the feasibility of any class action suit. In practical terms, the availability of robust legal fees drives class action litigation. Without a sizeable contingency fee to split among plaintiffs' counsel, the costs of pursuing any class action litigation would likely outweigh the expected benefits. In contrast to many statutory class action claims where the compensatory or punitive damages for each offensive act are specified in the legislation, no such certainty exists for common law trespass to

211. *See, e.g.*, Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382 at *11–*13 (N.D. Cal. 2001); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–71 (N.D. Cal. 2000); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248–51 (S.D.N.Y. 2000); *IMS*, 24 F. Supp. 2d at 550–51; Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998); Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *7–*8 (N.D. Cal. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020–24 (S.D. Ohio 1997); *Intel*, 114 Cal. Rptr. 2d at 247–52; Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 472–73 (Ct. App. 1996).

chattels claims. In fact, few courts have even yet attempted to value the precise amount of damages that might arise in the context of a computer trespass action. Although one court rejected the claim to include "lost profits" in a damages calculation,[212] most courts have simply acknowledged that the damages were difficult to quantify but still sufficient to sustain a trespass to chattels cause of action.[213] Perhaps until courts and juries begin assessing more fully the level of damages awarded in the context of trespass claims involving the Internet, the fear of low damages might not prevent plucky lawyers from attempting a class action suit. But if courts start rejecting favorable damage theories and minimal awards begin trickling out from juries, the incentive for bringing a class action suit based on common law trespass could evaporate.

B. ADVANTAGES

Despite the potential hurdles that could undermine the feasibility of a common law class action claim, significant benefits make a class action suit based on trespass to chattels theory especially attractive nonetheless. At least until those potential impediments become a bit more definite, the advantages to pursuing a class action common law claim seem to outweigh the expected risks.

1. Likelihood of Success

A strong likelihood of success on the merits provides perhaps the strongest and simplest argument in favor of pursuing a common law class action. Pursuing a class action based on federal law might avoid some of the potential risks of common law class action litigation described above. But as demonstrated by *DoubleClick*, *Intuit*, *Avenue A* and *Pharmatrak*, the rigidity of an existing statutory framework does not seem sufficiently accommodating of cookie technology. With respect to each of the three federal statutes considered in those cases, the courts in *DoubleClick*, *Avenue A* and *Pharmatrak* rejected the claims of Internet users based on a very technical interpretation of the statutory language and legislative history surrounding each law. Although the court in *Intuit* accepted the possibility that a claim might exist with respect to one of the statutory claims, the court commented only on the sufficiency of the pleadings and not the underlying merits of the claim. The aim here is not to quarrel with the method of statutory construction employed by the courts in

212. *Oyster Software*, 2001 WL 1736382 at *13.
213. *See, e.g.*, *Bidder's Edge*, 100 F. Supp. 2d at 1071; *Register.com*, 126 F. Supp. 2d at 249–50.

DoubleClick, *Intuit*, *Avenue A* or *Pharmatrak*. Instead the basic point is that statutes originally crafted to cure a specific problem might not be particularly amenable to solving problems or addressing technologies that did not exist at the time the statutes were adopted. Therefore, attempting to force an old statute to apply in a new context might not meet with much success if the language of the statute and the legislative history do not support that plasticity.

In contrast to the lack of success encountered within the statutory framework, a very strong case exists that Internet advertisers trespass on our computers by depositing, accessing and altering cookie files. To be fair, no courts have yet applied trespass to chattels principles within the precise context of cookie technology. But while statutory remedies may be appropriately limited to the precise intentions of the legislature, the common law "adapts to human endeavor" and provides much more flexibility in addressing new circumstances that arise in evolving society.[214] In any event, based on current case law addressing computer technology and trespass, extending trespass to chattels principles to cover cookie technology does not seem like a terribly difficult leap to make. As already detailed at length, with respect to each element of a trespass to chattels claim, a strong prima facie case supports imposing liability on Internet advertisers. While success is certainly not guaranteed using the common law theory, the case supporting a common law trespass to chattels claim at the very least seems much stronger than arguments that already failed within the framework of three federal statutes.

2. Immunity to Dispositive Motions

Related to the likelihood of success on the merits is a finer point of litigation strategy that addresses the longevity of a common law trespass claim irrespective of an ultimately successful outcome. Even if the common law class action claim were not successful in the end, a class action based on trespass to chattels principles seems likely to survive adverse dispositive motions.

With respect to a motion to dismiss, stating a claim that would satisfy the elements of a trespass to chattels claim seems rather undemanding. As the cases surrounding trespass to chattels in the context of bulk e-mails and

214. *Intel*, 114 Cal. Rptr. 2d at 247. *See* RICHARD B. CAPPALLI, THE AMERICAN COMMON LAW METHOD 91–92 (1997); Bruce P. Keller, *Condemned to Repeat the Past: The Reemergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property*, 11 HARV. J.L. & TECH. 401, 403–06, 423–26 (1998).

unauthorized information access demonstrate, computer hardware and software represent sufficiently tangible property interests, simply sending electronic signals suffices to establish interference, no specific intent to commit a wrong act is required and the mere use of another's computer capacity establishes the requisite level of damages to support a valid trespass claim.[215] Thus, only the most minimal allegations would be needed to proceed to the discovery stage of a class action suit.

Similarly, with respect to a motion for summary judgment, the evidentiary hurdles seem rather easy to surmount as well. In fact, merely establishing that cookie technology was used should be sufficient to survive an adverse summary judgment motion. Why? The very existence of cookie files on the computers of Internet users presumes certain facts to exist. Therefore, no issue at all would exist regarding the basic technological fact that in using cookie technology, Internet advertisers (or their affiliated Web sites) actually sent electronic signals that occupied some memory capacity on the computer hard drives of Internet users. Those facts alone satisfy three of the four elements of a trespass claim. Perhaps the only factual issue might arise with the element of damages. But unlike the prior class action suits based on federal statutes, the actual damages requirement of common law trespass to chattels does not require surpassing some minimum threshold of monetary damages. Instead, as the cases involving Internet "spam" and search robots establish, "mere use" of the computer capacity or data satisfies the damages threshold for a trespass claim to survive. At a bare minimum, since no factual debate would exist about Internet advertisers (or their affiliated Web sites) using the cookie data stored on the computer hard drives of Internet users, sufficient facts would inevitably exist to defeat any summary judgment motion.

Even if demonstrating lack of consent were considered an element of a prima facie case of trespass to chattels rather than an affirmative defense, a motion for summary judgment (or a motion to dismiss) would be simple to survive. Of course, the standard view is that consent represents an affirmative defense with the burden of proof lying with the defendant.[216] If demonstrating lack of authorization were necessary to support a basic trespass claim, however, a plaintiff's simple statement that no authorization was provided seems enough to get beyond the summary judgment stage. As courts construe trespass and other torts, once lack of authorization is alleged, the existence of consent becomes a question of fact for the jury to

215. *See supra* notes 174–84 and accompanying text.

216. Ward v. N.E. Tex. Farmers Co-Op Elevator, 909 S.W.2d 143, 150 (Tex. App. 1995); 75 AM. JUR. 2d *Trespass* § 216 (1991); 87 C.J.S. *Trespass* § 99 (2000).

resolve.[217] And recall that in a least one case, a court found that simply filing a lawsuit evinced a lack of consent sufficient to grant an injunction against the trespassing party.[218] Even if consent were considered a basic element of a trespass claim, then, avoiding summary judgment should not provide a difficult task for Internet users.

But beyond merely defeating an adverse motion, courts may actually be willing to grant summary judgment in favor of liability on trespass grounds. Recall that in many trespass cases involving robotic searches and bulk e-mails, courts actually granted summary judgment to the parties alleging a trespass had occurred.[219] While those cases did not involve cookie technology, the technological facts associated with depositing cookie files on the hard drives of Internet users are arguably even more definite than the technological facts involved in sending e-mails or conducting robotic searches. To the extent the essential facts of cookie technology fit the elements of a trespass claim even more neatly than bulk e-mails or robotic searches, then, the main focus in a common law class action cookie claim should not be avoiding dismissal on summary judgment but rather winning summary judgment on liability.

3. Sensitive Discovery

Turning to another point of litigation strategy, pursuing a trespass to chattels class action would likely expose Internet advertisers to broad discovery obligations related to issues of consent and damages. While discovery accompanies any litigation, to the extent discovery targets particularly sensitive areas, the incentives for settlement increase. Because discovery in the areas of consent and damages seem particularly sensitive, a class action based on trespass to chattels grounds might secure more easily a favorable settlement even if the case were not ultimately brought to trial.

With respect to discovery on the issue of consent, any act outside the scope of consent constitutes a trespass.[220] Therefore, if advertisers would claim they had actual or apparent consent to use cookie technology,

217. CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023–24 (S.D. Ohio 1997); Special Force Ministries, v. WCCO Television, 584 N.W.2d 789, 792 (Minn. Ct. App. 1998); 87 C.J.S. *Trespass* § 126 (2000).

218. *Register.com*, 126 F. Supp. 2d at 249.

219. *See, e.g.*, Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382, at *13–*14 (N.D. Cal. 2001); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 551 (E.D. Va. 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 453 (E.D. Va. 1998); *Intel*, 144 Cal. Rptr. 2d at 252.

220. *See supra* notes 201–02 and accompanying text.

Internet users would certainly counter that the advertisers exceeded any consent that may have been provided. In order to prove that the use of cookies exceeded the scope of authorization, Internet users would likely be entitled to discovery related to any and all uses to which advertisers put the cookie data, including all personal data profiles, mailing lists and combinations of cookie data with other consumer information (such as the information DoubleClick may have acquired through its acquisition of Abacus Direct).[221]

Moreover, on the issue of damages, because there is obviously no statutory amount of damages per offense associated with a common law trespass claim, establishing damages would require Internet users to craft a level of damages related to the use of computer capacity and the cookie data itself. While some have offered as much as $1,000 for the right to monitor individual online preferences,[222] perhaps the premiums Internet advertisers charge for the ability to target adds to specific consumers represents a better measure of any rental value associated with the cookie files. Discovery on that score would require disclosure of a wide range of sensitive pricing and revenue data. Furthermore, obtaining an accurate assessment of damages for any particular group of users might require breaking down that revenue data further by various demographic, geographic or other criteria. In the end, the damages discovery could require revealing a good deal of sensitive information relating to the advertisers' strategies, marketing efforts and operations. Because of the peculiar nature of the harm involved in a trespass to chattels claim that results from mere use of potentially valuable data, the assessment of damages arguably requires access to the valuation that advertisers place on that information itself.

The wide scope of discovery that courts would likely grant on the issues of consent and damages, then, would make framing a class action on trespass to chattels grounds seem especially attractive from a litigation strategy standpoint. Although every class action involves discovery, to the extent the discovery sweepingly targets sensitive information, the chances for settlement might increase regardless of any expectations for ultimate success on the merits.

221. *See supra* notes 22–23 and accompanying text.

222. *See supra* note 184 and accompanying text.

4. Multiple and Significant Remedies

The availability of both injunctive and monetary relief provides a clear advantage for a trespass to chattels class action. With respect to monetary relief, a good deal of uncertainty exists with respect to the theory of damage calculation that courts might embrace. While courts or juries might not find that the use of cookie technology creates much significant harm, the potential for extraordinary damages exists as well. Were a court or jury to accept the $1,000 rental value as a measure of damages per Internet user, a successful class action on behalf of the 175 million Internet users in the U.S. would yield $175 billion in damages.[223] But even if the monetary relief granted were pennies for each Internet user, a class action on behalf of all Internet users in the U.S. would still garner tens of millions of dollars. While the inchoate nature of trespass to chattels claims in the context of cookie technology makes a risk of low damages quite real, the prospect of incredibly high damage awards makes a common law class action suit especially attractive as well.

In addition to monetary damages, a trespass to chattels suit involves the possibility of injunctive relief. In several of the cases involving trespass to chattels claims and unauthorized bulk e-mail, courts granted permanent or preliminary injunctions preventing any further trespasses to occur.[224] According to those cases, if the actual damages are "impossible to compute"[225] or the harm suffered is "not easily quantified and not adequately compensated with money damages,"[226] an injunction is appropriate to prevent further unwanted intrusions. Again from a purely strategic litigation perspective, the threat of injunction as a remedy would serve as a rather valuable chip in any settlement negotiation. To the extent much of the business of DoubleClick and other Internet advertisers depends on cookie technology, an order enjoining the use of that essential tool could significantly injure if not cripple the company. So even if Internet users desired monetary damages more than an injunction, then, the threat of injunctive relief might help spur a favorable monetary settlement. In that sense, the dual remedies of monetary damages and injunctive relief work in tandem to promote more attractive relief for the class.

223. *See supra* notes 184, 210 and accompanying text.

224. *See LCGM*, 46 F. Supp. 2d at 453; Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, at *8 (N.D. Cal. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1028 (S.D. Ohio 1997); *Intel*, 114 Cal. Rptr. 2d at 255.

225. *CompuServe*, 962 F. Supp. at 1027–28.

226. *Hotmail*, 1998 WL 388389, at *7–*8.

VII. CONCLUDING THOUGHTS

In the end, a very strong case exists that Internet advertisers trespass on our computers by using cookie technology. Moreover, framing a claim in terms of trespass to chattels principles would most likely provide distinct advantages over current statutory causes of action. Not only would a common law class action claim afford a greater likelihood of success compared to the federal claims pursued (and already rejected) in *DoubleClick*, but a variety of strategic litigation benefits might flow from adopting a common law approach as well.

The comparative benefits of using a common law approach to address the issue of cookies, however, should not seem all that shocking. The federal statutes upon which Internet users relied in *DoubleClick* were adopted years before the Internet began to occupy its increasingly dominant position in commerce and culture. While statutes may effectively address existing problems, crafting laws to address what does not yet exist represents quite a difficult challenge. And even if legislators were to act quickly on the problems of the day, it may simply be too difficult for legislators to keep pace with the celerity of technological innovation associated with the Internet age. In contrast, the malleable nature of the common law seems especially well suited to accommodating technological advances, no matter how swift. Still, it does seem a bit peculiar to apply to Cyberspace the same legal principles that centuries ago helped give peasant farmers relief for injuries sustained to their livestock. But in the case of the common law and the Internet, it seems one old adage may turn out to be true. Everything old is new again.