2006

Internet Cookies: When is Permission Consent?

Max Oppenheimer
University of Baltimore School of Law, moppenheimer@ubalt.edu

Max Stul Oppenheimer*

Internet Cookies: When is Permission Consent?

TABLE OF CONTENTS

I. INTRODUCTION

Consent is the Philosophers' Stone[1] of the law: it can transmute an unconstitutional search into a lawful one, a criminal act into a legal one, or a tort into a contract. As technology has evolved, so has this fundamental legal concept. New forms of communication call for new ways to obtain and manifest consent. Examples include shrink-wrap licenses,[2] click-to-accept licenses,[3] faxed signatures,[4] e-mails,[5] and e-signatures.[6] Each of these forms, however, requires some affirmative

* Associate Professor, University of Baltimore School of Law; Faculty, The Johns Hopkins University. I would like to thank my research assistants, Lisa Paganini and Lisa Morgan, for their tireless efforts in search of the obscure.

1. "A reputed solid substance or preparation supposed by the alchemists to possess the property of changing other metals into gold or silver, the discovery of which was the supreme object of alchemy." 11 THE OXFORD ENGLISH DICTIONARY 686 (R.W. Burchfield ed., 2d ed. 1989).
2. *See, e.g.*, Bowers v. Baystate Techs., Inc., 320 F.3d 1317 (Fed. Cir. 2003).
3. *See, e.g.*, Home Basket Co. v. Pampered Chef, Ltd., No. 04-1314-WEB, 2005 U.S. Dist. LEXIS 513, at *1 (D. Kan. Jan. 12, 2005).
4. *See, e.g.*, Patterson Frozen Foods, Inc. v. Crown Foods Int'l, Inc., 307 F.3d 666 (7th Cir. 2002).
5. *See, e.g.*, Lamle v. Mattel, Inc., 394 F.3d 1355 (Fed. Cir. 2005).
6. *See, e.g.*, 37 C.F.R. § 2.33(d) (2005); TRADEMARK MANUAL OF EXAMINING PROCEDURE §§ 304.08, 804.05 (3d ed. 2003).

action by the person sought to be bound. An emerging issue is whether permissions granted by a computer program can constitute consent on behalf of the computer's owner, particularly where the permissions are set by default in the distributed form of the program rather than by a conscious decision by the owner to set them.

On November 8, 2005, the *Boston Globe* reported that Computer Associates International had concluded that Sony BMG was distributing music compact discs which contained not only the music that purchasers wanted, but also code which would run on the purchaser's computer, collect information about the purchaser, and report that information back to Sony.[7] On November 18, 2005 (following Microsoft's decision to classify the Sony program as spyware and provide tools to remove it),[8] Sony recalled the CDs and offered to replace those that had already been sold.[9]

On December 29, 2005, the *New York Times* reported that the National Security Agency had used cookies in transactions on its website[10] in violation of agency guidelines which had been in place since at least as early as 1999.[11] On January 6, 2006, CNET reported that

7. Hiawatha Bray, *Security Firm: Sony CDs Secretly Install Spyware*, BOSTON GLOBE, Nov. 8, 2005, at D1.

8. *Id.*

9. *See* Sony BMG Music Entertainment, Important Legal Notice/Software Update Notice, http://cp.sonybmg.com/xcp (last visited Jan. 30, 2006). On December 4, 2005, Sony issued an apology. Sony BMG Music Entertainment, To Our Valued Customers (Dec. 4, 2005), http://cp.sonybmg.com/xcp/customerletter.html.

10. Associated Press, *Spy Agency Removes Illegal Tracking Files*, N.Y. TIMES, Dec. 29, 2005, at A16.

11. Office of Management and Budget, Guidance and Model Language for Federal Web Site Privacy Policies (June 1, 1999), http://www.whitehouse.gov/omb/memoranda/m99-18attach.html.

Later, the Office of Management and Budget (OMB) placed restrictions on at least "persistent" cookies. Agencies were prohibited from using such cookies unless approved by the agency head upon a showing of a "compelling need to gather data" and "clear and conspicuous notice." Letter from John T. Spotilla, Adm'r, Office of Info. & Regulatory Affairs, to Roger Baker, Chief Info. Officer (Sept. 5, 2000), *available at* http://www.whitehouse.gov/omb/inforeg/cookies_letter90500.html. The policy provides the following:

1. *Tracking technology prohibitions:*
   a. agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below;
   b. agency heads may approve, or may authorize the heads of subagencies or senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's [sic] must post clear notice in the agency's privacy policy of:
      - the nature of the information collected;
      - the purpose and use for the information;
      - whether and to whom the information will be disclosed; and
      - the privacy safeguards applied to the information collected.

"[s]ixty-six politicians in the U.S. Senate and House of Representatives are setting permanent Web cookies even though at least 23 of them have promised not to use the online tracking technique."[12] These are clear examples, and probably isolated instances, of violations of computer users' rights. There are, however, widespread uses of similar technology that pose significantly more far-reaching issues.

Cookies are files stored on a user's computer (the client) on instruction from a second computer (the server) when the client's web browser software (browser) communicates with the server's website. These files typically contain encrypted information relating to the transaction between the client and server. By default, current browsers "accept cookies," that is, they allow the server to write these files to the client and to store them for a period of time determined by the server. Since the data in the file is under the control of the server, it can be used to record and monitor the transactions between the client and server. If the server has appropriate decrypting capability, it can also monitor transactions between the client and other servers. The use of cookies without consent of the user raises a number of issues:

- First, does the use of cookies constitute a trespass on the client computer?
- Second, when the server is controlled by a private party, does its use of cookies constitute unauthorized access to a computer in violation of criminal law?
- Third, when the server is controlled by a government agency, does its use of cookies constitute (in addition to the above violation of

---

c. agencies must report the use of persistent tracking technologies as authorized for use by subsection b. above (see section VII).

2. *The following technologies are not prohibited:*
   a. Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
   b. Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see v.1.b above) and where the following is posted in the Agency's Privacy Policy:
      - the purpose of the tracking (i.e., customization of the site);
      - that accepting the customizing feature is voluntary;
      - that declining the feature still permits the individual to use the site; and
      - the privacy safeguards in place for handling the information collected.
   c. Agency use of password access to information that does not involve "persistent cookies" or similar technology.

Memorandum from the Office of Mgmt. & Budget, to the Heads of Executive Dep'ts & Agencies (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda/m03-22.html.

12. Declan McCullagh & Anne Broache, *Congress' Hands Caught in the Cookie Jar*, CNET NEWS.COM, Jan. 6, 2006, *available at* http://news.com.com/Congress+hands+caught+in+the+cookie+jar/2100-1028_3-6020711.html.

rights) an unlawful search in violation of the Fourth Amendment or an unlawful seizure of property in violation of the Fifth Amendment?

- And fourth, if the use of cookies without permission violates criminal law, individual constitutional rights, or other rights, is there potential secondary liability for the providers of the browser software under the principles announced by the Supreme Court in *MGM v. Grokster*?[13]

Technically, a browser will not accept a cookie from a website unless its permissions have been set to do so. Does this technical answer—cookies are used only when permission has been given in a technical sense—equate to "consent" in the legal sense sufficient to authorize the transaction and insulate the setter of the cookie from the above types of liability?

If the answer is "no," then websites which set cookies are at risk for civil and criminal liability, government websites which set cookies further risk violating constitutional rights, and the distributors of web browsers face potential secondary liability for the use of their products.

II. TECHNOLOGICAL BACKGROUND

A cookie[14] is a text file embedded in an HTTP file exchanged between a server and a web browser running on a client, and it is retrievable by the server.[15] When a user browses a webpage, the website sends an image of the webpage as an HTML file using HTTP. If the user's computer is set to allow cookies, the webpage may embed a cookie in the HTML file, and the cookie is then stored on the user's computer. When the user next contacts the website, the user's computer sends a request for an HTML file and the cookie is embedded in the request. In this fashion, a website can track information relating to prior transactions with the user's computer. This process is referred to as "setting" a cookie. The server site sets the cookie, which typically contains client information, on the client computer, from

13. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005).

14. Although they will be referred to herein as "cookies," typical Internet cookies are more precisely "HTTP Cookies," so called because they are text embedded in HTTP files, the principal engine of Internet webpage exchanges.

15. Wikipedia, HTTP cookie, http://en.wikipedia.org/wiki/HTTP_Cookie (last visited Oct. 6, 2006); *see also, e.g.*, 32 C.F.R. § 806b app. (2005) (defining a cookie as "[d]ata created by a Web server that is stored on a user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). It provides a way for the Web site to identify users and keep track of their preferences. It is commonly used to 'maintain the state' of the session. A third-party cookie either originates on or is sent to a Web site different from the one you are currently viewing.").

which the server can retrieve it during a web browsing session.[16] Cookies are useful in streamlining transactions by reducing the need for repeated transfer of redundant information in exchanges between clients and servers over the Internet. Cookies can store data so that a server can be provided with information about the client's settings, past browsing history, authentication, or preferences without the user's needing to reenter the data; cookies can encode information so that only a small coded file needs to be transferred in order to convey larger amounts of information.[17] A common use of cookies is to maintain a shopping basket on a commercial website—the user can provide authenticating information and a credit card number once during a session, sequentially select items for purchase, and then execute a single purchase instruction.[18] The resulting efficiency is especially im-

16. The cookie is embedded in the HTML files which are exchanged between the client and server during a browsing session. The server embeds the cookie in the HTML file sent to the client, and when the client communicates with the server (for example, to request a webpage), it embeds the cookie in the communication.

17. For example, if a client prefers the server to display in yellow twelve-point Times New Roman font on a blue background, this can be encoded as preference "A" and stored in a cookie on the client computer. When the client logs on to the server, the server only needs to retrieve "A," then look up its meaning in the server's own database, rather than transfer "yellow twelve-point Times New Roman font on a blue background." Because internal lookups are significantly faster than equivalent Internet data transfers, this reduces total transaction time. Furthermore, if either party is paying for bandwidth based on the number of bits transferred, this will reduce the cost as well.

18. In *In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 14 (1st Cir. 2003), the court stated: "[C]ookies often store user preferences, login and registration information, or information related to an online 'shopping cart.' Cookies may also contain unique identifiers that allow a website to differentiate among users." However, it is also possible to collect personal information: "The following personal information was found on Pharmatrak servers: names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website." *Id.* at 15. For another example, see U.S. Patent No. 5,960,411 (filed Sept. 12, 1999), where the patent's abstract describes the invention as follows:

> A method and system for placing an order to purchase an item via the Internet. The order is placed by a purchaser at a client system and received by a server system. The server system receives purchaser information including identification of the purchaser, payment information, and shipment information from the client system. The server system then assigns a client identifier to the client system and associates the assigned client identifier with the received purchaser information. The server system sends to the client system the assigned client identifier and an HTML document identifying the item and including an order button. The client system receives and stores the assigned client identifier and receives and displays the HTML document. In response to the selection of the order button, the client system sends to the server system a request to purchase the identified item. The server system receives the request and combines the purchaser information associated with the client identifier of the client system to generate an order to

portant when bandwidth is a limiting factor, as for example when retrieving large files over modem connections. The cookie may be stored in the client's random access memory (RAM) (in which case it disappears when the client computer is turned off, the user's browser is closed, or, at the server's option, when the transaction with the browser ends), or it may (again, at the server's option) be stored on the client's hard drive (in which case the duration of the cookie is determined by the server).[19] A cookie which is stored in RAM or erased from the client's hard drive at the end of the transaction is referred to as a "temporary" or "session" cookie; a cookie which remains on the hard drive after the session is closed is referred to as a "persistent" cookie.[20]

In addition to cookies set and retrieved by the server from which the client has requested a webpage, third-party cookies may be set and retrieved. For example, a server may provide information to an advertising website[21] advising of the client's interests (as evidenced by the webpages the client has requested) so as to enable the advertising website to select targeted advertising to be presented to the client.[22]

Theoretically, the ability of a server to set a cookie is controlled by the user. All common browsers have settings which allow the user to block (at the user's option) some or all cookies. However, the default setting is to allow cookies; browsers do not conspicuously advise users that cookies are being accepted, and the process for changing the default settings requires sufficient sophistication to navigate through

---

purchase the item in accordance with the billing and shipment information whereby the purchaser effects the ordering of the product by selection of the order button.

19. Of course, the same information could be stored on the server, which has implications for analysis of trespass and unauthorized access. *See infra* section IV.A. For such a system to work, the client user would need to log in so that the appropriate data could be matched to the client. There are at least three reasons website operators might prefer to store the information on the client computer: obviously, it uses client resources rather than server resources; the information can be shared with other servers; and, at least with current technology, there is no need to request user cooperation.

20. These definitions can be found in Microsoft's Internet Explorer under "Help"/"Contents and Index"/"cookies"/"types of cookies."

21. *E.g.*, *In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4 (D. Mass. 2002).

22. Third-party advertising may be incorporated in the page requested by the client as a banner, or may be sent as a pop-up or pop-under ad. Third-party cookies present special issues with respect to client consent in connection with trespass and criminal liability. *See infra* section IV.A. They also present special issues of aggregation, similar to those presented by government cookies. *See infra* section IV.C.

several layers of commands.[23] The most ubiquitous browser running under the Windows operating system, Microsoft's Internet Explorer, defaults to allow all cookies and provides user control under the "Tools"/"Internet Options"/"Privacy" menu, where the user can select levels of privacy which restrict the ability of selected servers to set cookies—hardly a straightforward process for many users. The Mozilla-based browsers[24] provide greater user control[25] but still require navigation,[26] and are set to allow all cookies by default.[27]

The server's website may be designed to refuse access to a client if the client's browser is set so that cookies are not allowed. Assuming that the owner of the server is under no obligation to provide access,[28] using this power does not run afoul of the law. If the user's browser is set to reject cookies and the server's website is set to refuse access where cookies are disabled, the user will need to make a conscious decision whether access to the site is worth the price of allowing cook-

23. The index to the Windows XP basic guide does not even list "cookies," although it does list "HTML" and "HTTP." The "Help" file for the current version of Internet Explorer provides the following information under "Cookies"/"About Cookies":

> Understanding cookies
>
> Some Web sites store information in a small text file on your computer. This file is called a cookie.
>
> There are several types of cookies, and you can choose whether to allow some, none, or all of them to be saved on your computer. If you do not allow cookies at all, you may not be able to view some Web sites or take advantage of customization features (such as local news and weather, or stock quotes).

Conspicuously absent in the top-level summary is any suggestion that the "small text file" may contain a user's personal information, or why a user might want to "choose . . . to allow some, none, or all of them." Those details are provided under the "How cookies are used" subindex of "Cookies"/"About Cookies." Some third-party websites provide instructions for controlling cookies on major browsers. *See, e.g.*, Junkbusters, How Web Servers' Cookies Threaten Your Privacy, http://www.junkbusters.com/cookies.html (last visited Oct. 6, 2006) (providing instructions on "[h]ow to disable cookies").

24. Mozilla-based browsers include Mozilla Firefox and Netscape 6, as well as earlier browsers.
25. For example, cookies can be forced to expire when the browser is closed.
26. The commands are located in the "Tools"/"Options"/"Privacy"/"Cookies" subfolder of the Mozilla Firefox browser.
27. See, for example, the Mozilla Firefox browser's "Help" menu under "Managing Cookies"/"Setting Up Cookie Rules."
28. There are circumstances in which the server owner may be under such an obligation. Two examples are paid subscription services and services supported by grants conditioned on public access. Unless the relevant contract allows the owner of the server to condition access on the client's acceptance of cookies, denial of access would be a breach of contract (and, of course, the contract could not be used to demonstrate authorization so as to avoid criminal liability). Government websites present a special case with additional issues. *See infra* section IV.C. At least with respect to criminal statutes, the dual requirements of intent and lack of consent may be sufficient to protect the server owner who reasonably, but mistakenly, relies on the competence of the user.

ies. If a legally competent user makes the decision to accept cookies, there is neither violation of the law nor cause for complaint.[29]

III. THE NATURE OF CONSENT

The definition of consent is contextual. In a general sense, consent is defined as "[a]greement, approval, or permission as to some act or purpose."[30] Express consent is "[c]onsent that is clearly and unmistakably stated,"[31] while implied consent is "[c]onsent inferred from one's conduct rather than from one's direct expression."[32] The existence of consent in a particular case is a question of fact and may be inferred from actions. Mass marketers have faced the problem of obtaining consent in wholesale contexts and have developed techniques for obtaining consent without retail negotiations of consent.[33]

In the tort context,

> [c]onsent means that the person concerned is in fact willing for the conduct of another to occur. Normally this willingness is manifested directly to the other by words or acts that are intended to indicate that it exists. It need not, however, be manifested by words or by affirmative action. It may equally be manifested by silence or inaction, if the circumstances or other evidence indicates that the silence or inaction is intended to give consent. Even without a manifestation, consent may be proved by any competent evidence to exist in fact, and when so proved, it is as effective as if manifested.[34]

The consequence of consent is that "[o]ne who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it."[35]

In the criminal context, a victim cannot consent to a crime since the victim cannot waive the right of the state to prosecute. However, a victim's consent may convert what would otherwise be a criminal act into a legal act. For example, it is ordinarily criminal to attack a person with a knife; even if two people agreed to settle a disagreement with a knife fight, that agreement would not prevent prosecution of both parties for criminal assault and battery. However, a patient may agree to surgery, converting what would otherwise be a criminal act into a lawful one.

In the context of constitutional protection against unreasonable search and seizure, consent means permission granted provided "a

29. The special case of acceptance by users who are not legally competent presents other issues relating to both primary liability, *see infra* notes 192–94 and accompanying text, and secondary liability, *see infra* section IV.D.
30. BLACK'S LAW DICTIONARY 323 (8th ed. 2004).
31. *Id.*
32. *Id.*
33. For example, mass marketers of software have developed solutions for shrink wrap licenses and "click-to-accept" agreements. *See supra* notes 2–3 and accompanying text.
34. RESTATEMENT (SECOND) OF TORTS § 892 cmt. b (1979).
35. *Id.* § 892A.

reasonable person would feel free to decline the . . . requests or otherwise terminate the encounter."[36]

Consent has numerous potential effects with respect to cookies. Consent can insulate against civil liability for trespass, invasion of privacy, or battery;[37] it can insulate against criminal liability for trespass, wiretapping, or unauthorized access to computers; and it can legitimize a governmental search and seizure. There is, however, a possible perceptual disconnect between the parties to a cookie transaction. The party setting the cookie knows that the cookie may not be set unless the recipient's computer gives permission to do so, but the recipient may not know how the computer is configured. Although consent may be implied from actions, there must be a reasonable belief that the action is meant to convey consent.[38] Under the current state of user sophistication, it does not appear that the action of accepting cookies carries the necessary implication of consent in the absence of specific, conspicuous notice.

IV. ABSENCE OF CONSENT: THE RISKS

A. Trespass to Chattel

Placing information on a third party's computer without authorization may constitute a trespass to chattel.[39] A trespass to chattel is "intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another."[40] Even accidental harm suffices to impose liability,[41] and the degree of interfer-

36. Florida v. Bostick, 501 U.S. 429, 436 (1991).

37. Of particular interest in this context is the following:

> *Exceeding privilege.* If the actor exceeds the consent given, the consent does not protect him from liability for the excess. When, as is normally the case, the harm caused by the excess is severable from that resulting from the privileged act, the actor is subject to liability only for the excess. Thus if there is consent to an entry on land for a proper purpose and the actor enters for that purpose and subsequently commits an unpermitted tort upon the premises, he becomes liable for the subsequent tort but not for the original entry.

RESTATEMENT (SECOND) OF TORTS § 892A cmt. h (1979).

38. *Id.* § 892 cmt. b.

39. The cases to date fall into two main categories: those where the unwanted information was transmitted (for example, unsolicited e-mail), *see infra* notes 45, 57 and accompanying text, and those where the information was appropriated (for example, by web crawlers), *see infra* note 52 and accompanying text.

40. RESTATEMENT (SECOND) OF TORTS § 217 (1965). Comment e defines "intermeddling" as "intentionally bringing about a physical contact with the chattel."

41. While intent is an element of the offense,

> an intention is present 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 a violation of the possessory rights of another.

ence need not be great.[42] While consent is a defense, exceeding the scope of authorization vitiates that consent.[43] The development of trespass theory has followed scientific developments in interpreting what can constitute a physical invasion, and it now encompasses electronic invasion.[44]

In *Compuserve Inc. v. Cyber Promotions, Inc.*,[45] one of the earliest electronic trespass cases, Compuserve sold Internet and e-mail access to subscribers, and Cyber Promotions sent mass, unsolicited e-mail advertising[46] to Compuserve's subscribers. Compuserve produced evidence of subscribers' complaining and threatening to cancel their subscriptions.[47] In response to the complaints, Compuserve established screens to block e-mails from Cyber Promotions' address, but Cyber Promotions circumvented the screens by falsifying the "sender" information in its e-mails.[48] The district court enjoined all Cyber Promotions' e-mails to Compuserve customers as a trespass, finding that the transmission of electronic signals to Compuserve's customers (and, thus, Compuserve's computers) satisfied the physical contact requirement[49] and that the resulting demand for disk space and processing power reduced the availability of resources for Compuserve's subscribers and diminished the value of Compuserve's equipment.[50] The court rejected the argument that, by making its service available to the general public, Compuserve consented to any and all e-mailers, although the court required that there be notice that such mass mailings were not permitted.[51] Because technological advances have outpaced judi-

---

> Thus, it is immaterial that the actor intermeddles with the chattel under a mistake of law or fact which has led him to believe that he is the possessor of it or that the possessor has consented to his dealing with it.

Id. cmt. c.

42. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1065 (N.D. Cal. 2000) (granting a preliminary injunction and finding a trespass where evidence (on summary motions) showed that the unwanted access to eBay's computers represented between 1.11% and 1.53% of the total load on its listing servers, though the evidence failed to show that expenses were incrementally incurred because of the trespass, or that any particular service disruption could be attributed to the activities).
43. *Id.* at 1070.
44. Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Ct. App. 1996).
45. 962 F. Supp. 1015 (S.D. Ohio 1997).
46. This is now called "spam."
47. *Compuserve*, 962 F. Supp. at 1019.
48. *Id.*
49. *Id.* at 1021.
50. *Id.* at 1028.
51. *Id.* at 1024; *accord* Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998) (granting injunctions against unsolicited mass e-mail, upon showing of electronic transmission to plaintiff's computer, resulting in impairment of condition, quality or value).

cial resolution of the issue of the degree of interference required in order to constitute trespass, the question remains unresolved.

In *eBay, Inc. v. Bidder's Edge, Inc.*,[52] Bidder's Edge used an automated process to repeatedly access eBay's auction website to collect data on the status of its auctions.[53] Although the eBay website was open to, and invited, the public, Bidder's Edge accessed the site 100,000 times per day.[54] The court held that this level of access exceeded the authorization granted to the public to access the website and therefore found the lack of consent necessary to constitute a trespass.[55] The court found the necessary element of interference with property in Bidder's Edge's use of eBay's computer system capacity, depriving eBay "of the ability to use that portion of its personal property for its own purposes."[56]

The mere transmission of electronic signals was held insufficient to establish trespass, however, in *Intel Corp. v. Hamidi*.[57] There, Hamidi, a former Intel employee, used Intel's computer system by sending several mass e-mailings critical of management to between 8,000 and 35,000 Intel employees[58] contrary to Intel's guidelines for computer use. Intel testified that some employees found the messages unwelcome, and that its technical staff spent time and effort attempting to block them; the former employee admitted using multiple computers in an effort to circumvent the employer's efforts to block the e-mails.[59] The California Supreme Court reversed the court of appeals' decision to uphold an injunction against continued trespass to chattel, finding that the undisputed facts demonstrated no damage or threat of damage to the computer system, and holding that trespass did not cover electronic communication that "neither damages the recipient computer system nor impairs its functioning."[60] The court distinguished spamming cases, where it perceived that large quantities of e-mail might overburden a computer system, and interpreted the holding in *eBay* as consistent with its view, since the *eBay* court, though commenting that "[e]ven if . . . its searches use only a small amount of eBay's computer system capacity, [Bidder's Edge] has nonetheless deprived eBay of the ability to use that portion of its personal property

52. 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

53. "Programs that recursively query other computers over the Internet in order to obtain a significant amount of information are referred to . . . by various names, including software robots, robots, spiders and web crawlers." *Id.* at 1060 n.2.

54. *Id.* at 1063.

55. *Id.* at 1070.

56. *Id.* at 1071.

57. 71 P.3d 296, 309–10 (Cal. 2003).

58. *Id.* at 323 (Kennard, J., concurring).

59. *Id.* at 301 (majority opinion).

60. *Id.* at 300.

for its own purposes,"[61] nevertheless went on to find "that the defendant's conduct, if widely replicated, *would* likely impair the functioning of the plaintiff's system."[62] In this way, eBay had shown potential injury.[63]

That was not the case in *Ticketmaster Corp. v. Tickets.com, Inc.*,[64] however. Ticketmaster and Tickets.com each sold tickets to events and maintained websites to provide information as to location, date, time, description of the event, and ticket prices. Tickets.com attempted to list all events for which tickets were available. It obtained information about competitors' tickets by using a program called a "spider" or "crawler" to review their websites and extract the information. When Tickets.com did not have tickets available for sale, it linked to a website that did. One of the linked sites was Ticketmaster's. Ticketmaster filed suit alleging breach of contract, copyright infringement, and trespass. Disagreeing with other district court holdings that no harm need be shown in order to establish an electronic trespass, Senior Judge Hupp found that the use of Ticketmaster's resources was "very small" and that there was "no showing that the use interfere[d] to any extent with [Ticketmaster's] regular business."[65] Observing that "scholars and practitioners alike have criticized the extension of the trespass to chattels doctrine to the internet context, noting that this doctrinal expansion threatens basic internet functions (i.e., search engines) and exposes the flaws inherent in applying doctrines based in real and tangible property to cyberspace,"[66] the court held that the mere use of a spider to enter a publicly available website to gather information, without more, was insufficient to fulfill the harm requirement for trespass to chattel[67] and dismissed Tickmaster's trespass claims.

In *Oyster Software, Inc. v. Forms Processing, Inc.*,[68] the plaintiff sued a competitor that had accessed its computer system, asserting a

61. *Id.* at 306 (quoting *eBay*, 100 F. Supp. 2d at 1071).
62. *Id.*
63. *Id.*
64. No. CV-99-7654-HLHVBKX, 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 6, 2003).
65. Ticketmaster Corp. v. Tickets.com, Inc., No. CV-99-7654, 2000 U.S. Dist. LEXIS 12987, at *17 (C.D. Cal. Aug. 10, 2000).
66. *Ticketmaster*, 2003 U.S. Dist. LEXIS 6483, at *11 (citing Laura Quilter, *Cyberlaw: Regulating Conduct on the Internet: The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421 (2002); R. Clifton Merrell, *Trespass to Chattels in the Age of the Internet*, 80 WASH. U. L.Q. 675 (2002); Mary Anne Bendotoff & Elizabeth R. Gosse, *"Stay Off My Cyberproperty!": Trespass to Chattels on the Internet*, INTELL. PROP. L. BULL., Spring 2001, at 12; Edward Lee, *Rules and Standards for Cyberspace*, 77 NOTRE DAME L. REV. 1275, 1283–84 (2002)).
67. *Id.* at *13.
68. No. C-00-0724JCS, 2001 U.S. Dist. LEXIS 22520 (N.D. Cal. Dec. 6, 2001).

variety of federal and state causes of action, including trespass. The court denied the defendant's motion for summary judgment in which the defendant asserted that its access did not constitute trespass, even though the plaintiff had conceded that the access had "placed a 'negligible' load on [the plaintiff's] computer system.[69] The court noted the conflicting approaches of the *eBay* and *Ticketmaster* courts:

> While 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 Plaintiff's computer. . . . [That court relied on language saying that] a plaintiff can sustain an action for trespass to chattels, as opposed to an action for conversion, without showing a substantial interference with its right to possession of that chattel. Therefore, the Court declines to dismiss Oyster's trespass claim on the grounds that Oyster has shcwn only a minimal interference because Oyster has presented evidence of "use" . . . .[70]

In *Register.com, Inc. v. Verio, Inc.*,[71] Register.com sought to enjoin Verio from using an automated process to monitor Register.com's Internet domain name registry in order to compile a customer list, although Register.com had no published policy prohibiting such activity and could not provide proof of quantifiable damage from the activity. The Second Circuit affirmed the district court's decision to grant the injunction as within that court's discretion, relying on the finding that Verio's use of search robots "consumed a significant portion of the capacity of Register's computer systems" and that "[w]hile Verio's robots alone would not incapacitate Register's systems, the [lower] court found that if Verio were permitted to continue," a more significant trespass was "highly probable."[72]

Thus, courts[73] appear to reach conclusions which can be reconciled only by attempting to quantify "impact" on computer resources, an inherently ambiguous concept. An impact which might be imperceptible at one instant could be catastrophic at another. An impact which

69. *Id.* at *39–40.
70. *Id.* at *40–41 (citations and internal quotation marks omitted).
71. 126 F. Supp. 2d 238 (S.D.N.Y. 2000).
72. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404 (2d Cir. 2004).
73. In the interest of completeness, it should also be noted that state trespass claims may be appended to federal claims under statutes such as the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-190, 100 Stat. 1848 (codified as enacted and amended in scattered sections of 18 U.S.C.). Courts are reluctant to retain jurisdiction over such state claims if the federal claim is dismissed. For example, in *In re Pharmatrak, Inc. Privacy Litigation*, 220 F. Supp. 2d 4 (D. Mass. 2002), a state trespass claim was included in an ECPA case. Although reversed on appeal in *In re Pharmatrack, Inc. Privacy Litigation*, 329 F.3d 9 (1st Cir. 2003) (reversing the holding as to violation of the ECPA), the trial court dismissed the federal claims and declined to retain jurisdiction of the state trespass claims. *See also* cases cited *infra* notes 185–86 and accompanying text.

might be imperceptible to a machine with a state-of-the-art processor and a large hard drive connected to a T1 connection might be catastrophic to a machine with a slower processor, a smaller hard drive, and a dial-up connection. The problem for companies communicating through the Internet is that they are not likely to know in advance which configuration is on the receiving end of the communication.

B. Criminal Liability for Unauthorized Access

The typical American website does not provide conspicuous notice that it sets cookies. Generally, notice is only provided if cookies have been turned off and the site needs them in order to function, i.e., in situations in which the user already has actual knowledge of cookies and has made the decision not to allow them. In contrast, the European Union requires websites to advise users if the sites use cookies and permit users to reject them.[74]

Federal criminal statutes in the United States also prohibit certain types of activities with respect to computers. The Computer Fraud and Abuse Act[75] prohibits "exceeding authorized access"[76] to a computer, which means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."[77] The Electronic Communications Privacy Act[78] prohibits intentional interception of wire, oral, or electronic communications.[79] It also prohibits intentional unauthorized access to a facility through which an electronic information service is provided, or "intentionally exceed[ing] an authorization to access that facility" and obtaining access to an electronic communication "while it is in electronic storage."[80] The CFAA and the ECPA both create private causes of action.[81]

74. Council Directive 2002/58/EC, Recital 25 & art. 5(3), Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37, 39, 44 (EC).

75. 18 U.S.C. § 1030 (2000). Jurisdictionally, the plaintiff must show at least $5,000 in damages. *Id.* § 1030(e)(8).

76. *Id.* § 1030(a)(1). Similarly, § 1030(a), subsections (2) and (4), prohibit activity that "exceeds authorized access."

77. *Id.* § 1030(e)(6).

78. Pub. L. No. 99-190, 100 Stat. 1848 (1986) (codified as enacted and amended in scattered sections of 18 U.S.C.)

79. 18 U.S.C. § 2511 (2000 & Supp. IV 2004).

80. *Id.* § 2701(a). Although apparently redundant, subsection (c) provides an exception for conduct authorized by the person to whom the communication was directed.

81. *See id.* §§ 2520, 2707.

Most states also have statutes which prohibit unauthorized access to computers.[82] The term "unauthorized access" presents an issue of interpretation. Access without authorization is clearly covered. It is less clear whether the term covers the situation where there is authority for initial access for certain purposes but not for subsequent use of that access beyond the originally intended purposes, or where there is arguably implied consent to access but no specific grant of access. Both issues are directly relevant to the analysis of the use of cookies.

Arizona,[83] Georgia,[84] Hawaii,[85] Maryland,[86] Michigan,[87] New Mexico,[88] North Dakota,[89] Ohio,[90] and South Carolina[91] explicitly

82. Alabama: ALA. CODE § 13A-8-102 (Supp. 2004); Arizona: ARIZ. REV. STAT. ANN. § 13-2316(A) (2001); Arkansas: ARK. CODE ANN § 5-41-104 (1997); *id.* §§ 5-41-202(a)(1), 5-41-203(b)(1) (Supp. 2005); Colorado: COLO. REV. STAT. § 18-5.5-102 (2005); Connecticut: CONN. GEN. STAT. § 53a-251 (2001); Delaware: DEL. CODE ANN. tit. 11, § 932 (2001); Florida: FLA. STAT ANN. § 815.06 (West 2006); Georgia: GA. CODE ANN. § 16-9-153 (Supp. 2005); Hawaii: HAW. REV. STAT. §§ 708-890, 708-895.5(1) (Supp. 2005); Idaho: IDAHO CODE ANN. § 18-2202 (2004); Illinois: 720 ILL. COMP. STAT. ANN. 5/16D-3 (West 2003); Iowa: IOWA CODE ANN. §§ 714.1(8), 716.6B (West Supp. 2006); Kansas: KAN. STAT. ANN. § 21-3755(d) (Supp. 2005); Maryland: MD. CODE ANN., CRIM. LAW § 7-302 (LexisNexis 2005); Massachusetts: MASS. GEN. LAWS ANN. ch. 266, § 120F (West 2000); Michigan: MICH. COMP. LAWS ANN. § 752.795 (West 2004); Minnesota: MINN. STAT. ANN. § 609.89 (West 2003 & Supp. 2006); Missouri: MO. ANN. STAT. § 569.099 (West 1999 & Supp. 2006); Nebraska: NEB. REV. STAT. § 28-1347 (Reissue 1995); Nevada: NEV. REV. STAT. § 205.4765 (2003); New Hampshire: N.H. REV. STAT. ANN. § 638:17 (LexisNexis 1996 & Supp. 2005); New Jersey: N.J. STAT. ANN. § 2C:20-25 (West Supp. 2005); New Mexico: N.M. STAT. § 30-45-5 (2004); New York: N.Y. PENAL LAW §§ 156.05, 156.10 (2006); North Carolina: N.C. GEN. STAT. § 14-454 (2003); North Dakota: N.D. CENT. CODE § 12.1-06.1-08(2) (Supp. 2005); Ohio: OHIO REV. CODE ANN. §§ 2913.04(B), 2913.421(D)(1) (LexisNexis Supp. 2005); Oklahoma: OKLA. STAT. ANN. tit. 21, § 1953(A)(4) (West 2002); Oregon: OR. REV. STAT. § 164.377(4) (2003); Pennsylvania: 18 PA. CONS. STAT. ANN. §§ 7611, 7613 (West Supp. 2005); Rhode Island: R.I. GEN. LAWS § 11-52-3 (2002); South Carolina: S.C. CODE ANN. §§ 16-16-10, 16-16-20(1) (Supp. 2004); Tennessee: TENN. CODE ANN. § 39-14-602(b) (2003); Utah: UTAH CODE ANN. § 76-6-703 (2003 & Supp. 2005); Washington: WASH. REV. CODE ANN. § 9A.52.120 (West 2000); West Virginia: W. VA. CODE ANN. § 61-3C-5 (West 2005) (computer services); *id.* § 61-3C-11 (obtaining confidential public information); *id.* § 61-3C-12 (computer invasion of privacy); Wisconsin: WIS. STAT. ANN. § 943.70(2) (West 2005); and Wyoming: WYO. STAT. ANN. § 6-3-504 (2005). It does not appear that the District of Columbia, Alaska, California, Indiana, Kentucky, Louisiana, Maine, Mississippi, Montana, Texas, Vermont or Virginia have specific statutes prohibiting unauthorized access to computers.

83. ARIZ. REV. STAT. ANN. § 13–2316(A) (2001).

84. GA. CODE ANN. §§ 16-9-92, 16-9-93(b)(3) (Supp. 2005).

85. HAW. REV. STATS. §§ 708-890, 708-895.5 to -895.7 (Supp. 2005).

86. MD. CODE ANN., CRIM. LAW § 7-302 (LexisNexis 2005).

87. MICH. COMP. LAWS ANN. § 752.795 (West 2004).

88. N.M. STAT. § 30-45-5 (2004).

89. N.D. CENT. CODE § 12.1-06.1-08(2) (Supp. 2005).

90. OHIO REV. CODE ANN. §§ 2913.04(B), 2913.421(D)(1) (LexisNexis Supp. 2005).

91. S.C. CODE ANN. §§ 16-16-10, 16-16-20(1) (Supp. 2004) (subject to damages).

prohibit access to a computer exceeding that authorized by the client computer's owner. Oklahoma[92] and Kansas[93] prohibit access exceeding that authorized by the owner when coupled with resulting damage.

Maryland's statute[94] is typical of those prohibiting exceeding authorized access, and its history illustrates the definitional problem. It currently defines "access" to a computer as follows: "'Access' means to instruct, communicate with, store data in, retrieve or intercept data from, or otherwise use the resources of a computer program, computer system, or computer network."[95] The statute prohibits intentional unauthorized access: "A person may not intentionally, willfully and without authorization access . . . or exceed the person's authorized access to all or part of a computer network . . . [or] computer. . . ."[96]

In any web transaction, there is no question that the server accesses the client computer—that is the point of the web transaction.[97] The more difficult question is whether the access is unauthorized. Again, there seems little room to argue that the superficial transaction between the client and server—the transfer from the server to the client of the information actually requested by the user—is unauthorized. The superficial transaction is knowingly initiated by the user.[98] If the user is given notice and understands that part of the transaction will involve the collection and storage of information about the transaction on the user's computer, it would be difficult to argue that the use of cookies constitutes unauthorized access. However, as noted above, current browsers default to allow cookies and therefore do not provide notice that they will be stored on the user's computer. Nevertheless, under standard contract principles, formal notice would be

92. OKLA. STAT. ANN. tit. 21, § 1953(3) (West 2002).

93. KAN. STAT. ANN. § 21-3755(b)(3), (d) (2005).

94. MD. CODE ANN., CRIM. LAW § 7-302(a) (LexisNexis 2005) (originally enacted as MD. ANN. CODE art. 27, § 146(a) (1984)).

95. *Id.* § 7-302 (a)(2) (derived from former MD. ANN. CODE art. 27, § 146(a)(9), which was substantially the same, providing: "'Access' means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including, but not limited to, computers and other data processing equipment or resources connected therewith.").

96. *Id.* § 7-302(c).

97. Although the transaction is initiated by the client with a request for information (such as an HTML page) from the server, the server must also retrieve information from the client in order to fulfill the request.

98. Certain transactions are arguably not "knowingly" initiated by the user (i.e., so-called pop-up or pop-under ads). These are triggered by actions which the user has taken, but are not specifically requested by the user. For an example, see "What are Popups?" in Mozilla Firefox under "Help"/"Help Contents"/"Controlling Popups." Current versions of browsers provide user control over pop-up and pop-under ads, although they require the same type of navigation as the controls of cookies. The special problems of pop-up and pop-under ads are beyond the scope of this Article.

unnecessary if the user were aware of the use of cookies and accepted a benefit with such knowledge.[99] At this point, the available data does not support such a position.

In 2000, *Business Week* conducted a survey on Internet privacy,[100] asking, "If you use a computer, have you ever heard of an online technology known as 'cookies'?" Sixty percent of the respondents answered "no." Of those respondents who had heard of cookies, seventy-five percent correctly identified their function. In other words, only thirty percent of respondents knew what a cookie does. When advised that some websites track user movements online, thirty-five percent of those who claimed to use the Internet responded that they would be "not at all comfortable," and twenty-eight percent would be "not very comfortable" with such websites even if the site did not tie their online activity to their name or real-world identity. The numbers went to sixty-eight and twenty-one percent, respectively, when the question included linking browsing habits into a profile linked to the user's real name and identity, and to eighty-two and thirteen percent, respectively, when additional personal information such as income, driver's license, credit data, and medical status was added to the profile. Even without the link to identifying information or additional personal information, sixty-seven percent of respondents were "not at all comfortable" with sharing information that would allow tracking on multiple websites, while twenty-four percent were "not very comfortable." The message would appear to be that there is not sufficient awareness to find implied consent to the use of cookies simply by virtue of use of the web. A large majority of users would in fact object to the use of cookies if made aware of them.

The argument still might be made that by initiating a transaction with a website, the user has implicitly authorized whatever might facilitate that (or a similar future) transaction. That argument, however, would need to overcome the principle that consent given under a mistaken understanding of the transaction is ineffective.[101] Furthermore, the development of modern criminal statutes regarding unau-

99. *See* RESTATEMENT (SECOND) OF CONTRACTS § 69(1) (1981) ("Where an offeree fails to reply to an offer, his silence and inaction operate as an acceptance in the following cases only: (a) Where an offeree takes the benefit of offered services with reasonable opportunity to reject them and reason to know that they were offered with the expectation of compensation. . . ."). A similar argument could be made to support government use of cookies, since widespread knowledge of the use of cookies would defeat an expectation of privacy with respect to information stored in cookies.

100. Harris Interactive, *Business Week/Harris Poll: A Growing Threat*, BUS. WK., Mar. 20, 2000, http://www.businessweek.com/2000/00_12/b3673010.htm. The data was collected by a telephone survey of 1,014 adults between March 2 and March 6, 2000, by Harris Interactive. The raw data collected from the survey (concerning cookies) is found *infra* in the appendix.

101. *See* RESTATEMENT (SECOND) OF TORTS § 892B (1979). The provision provides:

thorized access suggests a trend toward prohibition not only of unauthorized access, but also of access exceeding initial authority.

The evolution of the Maryland statute is instructive on this critical question of authorized access, and particularly on the question of whether a user's grant of access for one purpose is sufficient authorization to cover all subsequent activities. As originally enacted, the statute provided that

> (2) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, . . . [or] computer system, . . . to: . . . (ii) Alter, damage, or destroy data or a computer program stored, maintained, or produced by . . . any part of these systems. . . .[102]

In *Briggs v. State*,[103] a criminal defendant, Terry Briggs, was a computer programmer, hired as the system administrator of the Scarborough Group's network. His duties included management of the entire system. Thus, his access to the computers clearly was authorized. Following a dispute, however, Briggs resigned. Scarborough then discovered that some of its files had been password protected,[104] and that

---

> (1) Except as stated in Subsection (2), consent to conduct of another is effective for all consequences of the conduct and for the invasion of any interests resulting from it. (2) If the person consenting to the conduct of another is induced to consent by a substantial mistake concerning the nature of the invasion of his interests or the extent of the harm to be expected from it and the mistake is known to the other or is induced by the other's misrepresentation, the consent is not effective for the unexpected invasion or harm.

102. MD. ANN. CODE art. 27, § 146(c) (1996 & Supp. 1997). The full text of the statute provided as follows:

> (c) *Illegal access.*—(1) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services.
>
> (2) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services to:
>
> (i) Cause the malfunction or interrupt the operation of a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services; or
>
> (ii) Alter, damage, or destroy data or a computer program stored, maintained, or produced by a computer, computer network, computer system, computer services, computer database, or any part of these systems or services.
>
> (3) A person may not intentionally, willfully, and without authorization:
>
> (i) Identify or attempt to identify any valid access codes; or
>
> (ii) Distribute or publicize any valid access codes to any unauthorized person.

103. 704 A.2d. 904 (Md. 1998).

104. Briggs admitted having placed the passwords. *Id.* at 906.

only Briggs had the password, which Briggs had "difficulty remembering."[105] Briggs was charged with, among other things, unauthorized access to a computer under article 27, section 146.[106] The State's theory was that "although Briggs was authorized to access the computer system, he was not authorized to access the system in such a way as to interrupt the operation of . . . the system."[107] The trial court denied a motion for judgment of acquittal and a jury convicted on the charges of unauthorized access.[108] On appeal,[109] Briggs argued that he had been granted access to Scarborough's computer system and that the statute did not cover "conduct that can be characterized as only exceeding authorized access."[110] The purpose of the statute, Briggs argued, "was to deter unauthorized users from breaking into computer systems."[111]

While it was disputed whether Briggs had been authorized to place passwords on files, the court found it unnecessary to resolve that dispute, holding it sufficient for reversal of the conviction that Briggs' "access to the computer was not 'without authorization' within the [plain] meaning of the statute."[112] "Authorization" was not defined in the statute, but, applying dictionary definitions, the court concluded that the initial grant of access ended the inquiry: employees who had permission "to 'instruct,' 'communicate with,' 'store data in,' or 'retrieve data from'" a computer system were authorized within the meaning of the statute and subject to no implied limits on their authority.[113] The court noted that

> [t]he legislative history supports our reading of the statute. In 1984, in an apparent response to the inadequacies of current criminal law to address disruptive or voyeuristic acts involving computer information systems, House Bill 121, approved by both houses, and enacted as Chapter 588, 1984 Laws of Maryland, criminalized "illegal access to computers." A representative of the Department of Budget and Fiscal Planning testified in support of the bill: Generally speaking, the threat [of computer crime] may be viewed as being divided into two reasonably identifiable types: 1) those associated with criminal intent or activity, and 2) those associated with the so called "hacker" type

105. *Id.*
106. The full text of the statute under which Briggs was charged is set forth *supra* note 102. Briggs was also charged with theft, but acquitted of those charges. *Briggs*, 704 A.2d at 906 n.3.
107. *Briggs*, 704 A.2d at 906.
108. *Id.* The court sentenced Briggs to one year of incarceration, with all but two days suspended, two years supervised probation, 150 hours of community service, and a fine of $500. The court also ordered him to cooperate with Scarborough and required him to release any remaining password information and client files. *Id.*
109. The verdict was appealed to the Maryland Court of Special Appeals, but the Maryland Court of Appeals granted certiorari on its own motion before consideration by the Court of Special Appeals. *Id.*
110. *Id.* at 907.
111. *Id.*
112. *Id.* at 908.
113. *Id.* at 910.

> of activity, where just the challenge of penetrating the system, or some sort of "electronic vandalism" or other mischief is the objective. While outright criminal activity involving information systems is covered by current statute, the Department feels this bill provides a needed addition by directly addressing *the second type of threat* by prohibiting all unauthorized access, for whatever purpose, and by providing penalties for its occurrence.[114]

Therefore, the court concluded,

> The legislative history thus suggests that House Bill 121 was drafted in reaction to the concern about the recent "hacker" activity. The Senate Judicial Proceedings Committee Report for House Bill 121, reported favorably by Chairman (now President of the Senate) Thomas V. Mike Miller, underscores our conclusion that the statute should apply to those who break into computers: . . . "This legislation is intended to make it a misdemeanor for a person intentionally and without authorization to access, attempt to access or cause access to a computer system. *The purpose of the bill is to deter individuals from breaking into computer systems.*"[115]

The court then invited the legislature to broaden the statute if it intended the law to apply to cases such as *Briggs*.[116] In 2002 the legislature accepted the court's invitation, amending the statute[117] to provide that "(1) A person may not intentionally, willfully, and without authorization access, attempt to access, cause to be accessed, *or exceed the person's authorized access* to all or part of a computer network, computer control language, computer, computer software, computer system, computer services, or computer database."[118]

The Maryland statute defines "computer" as "an electronic, magnetic, optical, organic, or other data processing device or system that performs logical, arithmetic, memory, or storage functions."[119] It defines a "computer network" as "the interconnection of one or more

---

114. *Id.* (citation omitted).

115. *Id.* at 910–11 (citation omitted).

116. *See id.* at 911 ("If the law is to be broadened to include Briggs's conduct, it should be modified by the Legislature, not by this Court.").

117. This amendment is now found at MD. CODE ANN., CRIM. LAW § 7-302 (LexisNexis 2005).

118. *Id.* § 7-302(c)(1) (emphasis added). The complete text of the current section 7-302(c) provides as follows:

> (1) A person may not intentionally, willfully, and without authorization access, attempt to access, cause to be accessed, or exceed the person's authorized access to all or part of a computer network, computer control language, computer, computer software, computer system, computer services, or computer database.
> (2) A person may not commit an act prohibited by paragraph (1) of this subsection with the intent to:
> (i) cause the malfunction or interrupt the operation of all or any part of a computer, computer network, computer control language, computer software, computer system, computer services, or computer data; or
> (ii) alter, damage, or destroy all or any part of data or a computer program stored, maintained, or produced by a computer, computer network, computer software, computer system, computer services, or computer database.

119. *Id.* § 7-302 (a)(4)(i).

computers through: (i) the use of a satellite, microwave, line, or other communication medium; and (ii) terminals or a complex consisting of two or more interconnected computers regardless of whether the interconnection is continuously maintained."[120] It defines a "computer system" as "one or more connected or unconnected computers, peripheral devices, computer software, data, or computer programs."[121]

Thus, the definitions of computer, computer system, and computer network are broad enough to encompass the client-server configuration typically involved in web browsing, with the statute apparently specifically directed to Internet-type connections.[122]

Given the history of the current statute, it would be difficult to argue that merely overstepping one's authority was not prohibited. Maryland's statutory revision was clearly a response to the Maryland Court of Appeals' decision in *Briggs*, and clearly intended to clarify the point that exceeding authority violates the statute.

Therefore, under such statutes, the fact that a transaction giving rise to a cookie is initiated by the user will not protect the server's owner from liability if the user does not authorize the cookie itself. Setting the unauthorized cookie is a clear case of exceeding the scope of initially authorized access.

The geographic reach of the Maryland statute is defined in subsection (f): "Venue.—A court of competent jurisdiction may try a person prosecuted under this section in any county in this State where: (1) the defendant performed the act; or (2) the accessed computer is located."[123]

Thus, it is not necessary for the server to be located in Maryland; access by a Maryland user would be sufficient to confer jurisdiction. Since the nature of the Internet prevents a server from determining (or verifying) the physical location of the client computer, the owner of any server which sets cookies is at risk. The factor determining liability is not the location of the server, but the location of the client.

C. Government Cookies: Searches and Takings?

Government websites set cookies. There are specific guidelines for determining when it is appropriate for federal agencies to do so.[124]

120. *Id.* § 7-302 (a)(7).
121. *Id.* § 7-302 (a)(11).
122. *See id.* § 7-302(a)(7).
123. *Id.* § 7-302(f).
124. *See, e.g.*, U.S. GEN. ACCOUNTING OFFICE, REPORT TO THE CHAIRMAN OF THE U.S. SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS, INTERNET PRIVACY: IMPLEMENTATION OF FEDERAL GUIDANCE FOR AGENCY USE OF "COOKIES" (2001). While the reported uses of cookies on government websites have, to date, involved federal websites, the same issues would be posed by the use of cookies by state or local governments or agencies.

The information placed by government cookies can be used to track what information is being requested by particular users. The Office of Management and Budget, in its June 1, 1999 *Guidance*[125] noted that persistent cookies[126] raised "serious concerns" because they made it "technically easy" for the agency to learn the complete history of users' web activity.[127] Following the same logic as developed in Part III, authorization to engage in a web-based transaction is not equivalent to authorization to set a cookie, or to read one that has previously been set. Particularly since the government can aggregate all of the information contained in cookies set by any government website, it has the ability to produce a composite image of an individual.

Arguably, as in the corporate context, what takes place is an exchange of access in return for user information. The government, however, is a special type of provider of information and in a special situation with respect to obtaining information from its citizens.

The extent to which the government may require surrender of a right other than through eminent domain has been analyzed by the Supreme Court in a series of cases starting with the *Ruckelshaus v. Monsanto Co.* trade secret case.[128] A trade secret is information that derives independent economic value from not being generally known or readily ascertainable by proper means, where its owner takes reasonable steps under the circumstances to maintain its secrecy.[129] Trade secrets are violated by misappropriation: unauthorized access to, use of, or disclosure of trade secrets obtained by improper means.[130] Trade secret law protects the information; the medium of storage is irrelevant, and courts have specifically found data stored in computers to qualify for trade secret protection.[131]

If the information stored in cookies is viewed as a trade secret of the computer owner, three consequences follow. First, unauthorized access to, use of, or disclosure of such information is a misappropriation of the trade secret.[132] Second, unauthorized use or disclosure of such information by a government is a taking.[133] And finally, unauthorized access to such information by a government may constitute an unlawful search and seizure under the Fifth and Fourteenth Amendments.

---

125. Office of Management and Budget, *supra* note 11.
126. These are cookies which were stored on a user's computer beyond the web browsing session in which they were set. *See* discussion *supra* note 20 and accompanying text.
127. Office of Management and Budget, *supra* note 11.
128. 467 U.S. 986 (1984).
129. UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 537 (2005).
130. *Id.*
131. *See Monsanto*, 467 U.S. 986.
132. UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 537 (2005).
133. *See* discussion *infra* note 134 and accompanying text.

It is clear that the superficial transaction—the request for information and receipt of the response—is authorized. The deeper issue is whether the government can require authorization of cookies in order to obtain access to the requested information.

In *Monsanto*, the Supreme Court specifically addressed whether the government's use of trade secret information constituted a taking under the Fifth Amendment.[134] Monsanto had submitted proprietary data to the Environmental Protection Agency (EPA) in order to obtain permission to market a compound regulated by the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA).[135] Under EPA regulations, the agency was permitted to use Monsanto's proprietary data in evaluating submissions for similar compounds submitted by Monsanto's competitors. While the EPA might have compelled Monsanto to make the data available to competitors through eminent domain, the Fifth Amendment would require payment of "just compensation,"[136] and instead the agency chose to rely on the argument that the data had been voluntarily submitted and could be used for any authorized regulatory purpose. The Court held that trade secrets were property[137] subject to the protection of the Fifth Amendment, and that their use by the government triggered the right to just compensation. Although the Court found an adequate remedy that allowed avoiding enjoining the use,[138] it did deal with the question whether Monsanto's voluntary submission of the data in order to obtain the required EPA license constituted a waiver of the constitutional protection.[139] While noting that there was "no set formula" and that courts must look to the particular circumstances of each case,[140] the Court held that since Monsanto was "aware of the conditions under which the data are submitted, and the conditions are rationally related to a legitimate Government interest, a voluntary submission of data by an applicant in exchange for the economic advantages of a registration can hardly be called a taking."[141] The valuable benefit

134. *See Monsanto*, 467 U.S. at 1004.

135. 7 U.S.C. § 136 (2000).

136. "No person shall . . . be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." U.S. CONST. amend. V.

137. The information qualified as a trade secret under the relevant state law (Missouri). *Monsanto*, 467 U.S. at 1003. Thus, not only does *Monsanto* bear on the "access in exchange for information" question, but also on the question whether information as to a user's browsing route is a protectable property right.

138. *See* Tucker Act, 28 U.S.C. § 1491 (2000); *Monsanto*, 467 U.S. at 1016.

139. There was also an issue as to information submitted under old regulations which did not explicitly state that the EPA would use the data in evaluating competitors' applications. As to these, the Court held that there was a taking. *See Monsanto*, 467 U.S. at 1009.

140. *Id.* at 1005 (quoting Kaiser Aetna v. United States, 444 U.S. 164, 175 (1979)).

141. *Id.* at 1007.

which Monsanto received in return for the use of its proprietary data included a term of exclusive license to use its compound and the right to compensation from competitors who wished to rely on Monsanto's data.[142]

At the other end of the spectrum, in *Nollan v. California Coastal Commission*,[143] a state refused to grant a permit to improve existing beachfront property unless the owner dedicated a public easement.[144] While the dissent would have considered the grant of a permit a benefit akin to that in *Monsanto*,[145] the majority disagreed, stating that "the announcement that the application for (or granting of) the permit w[ould] entail the yielding of a property interest cannot be regarded as establishing the voluntary 'exchange' that we found to have occurred in *Monsanto*."[146] The *Nollan* Court explained that the ability to improve one's own property, though subject to some regulation, is not comparable to the type of government benefit proffered in exchange for use and disclosure of trade secret information in *Monsanto*.[147] Thus, *Nollan* recognizes that the mere granting of permission to engage in routine activities, incident to existing rights, does not constitute compensation sufficient to support a *Monsanto*-type exchange.

Likewise, in *Philip Morris Inc. v. Reilly*,[148] Massachusetts had required tobacco companies to submit proprietary information in order to continue doing business in the Commonwealth. The court found no exchange which compensated Philip Morris: allowing a company to continue to do business did not provide the required benefit under *Monsanto*.[149]

It is therefore unlikely that a government could avoid the taking requirements simply by arguing that a user of its website had voluntarily surrendered its rights (even if the government provides notice that cookies are being used). As in *Philip Morris*, the user is only accessing data it already has the right to access. Unlike *Monsanto*, no special benefit is conferred on a specific user in exchange for access to the information.

D. Accessory/Secondary Liability

Cases analyzing secondary liability for third-party actions in civil contexts provide insight into whether providers of software which fa-

142. *See id.*; Philip Morris Inc. v. Reilly, 65 U.S.P.Q.2d 1065, 1081–82 (1st Cir. 2002) (discussing *Monsanto*).
143. 483 U.S. 825 (1987).
144. *See id.* at 828.
145. *See id.* at 860 n.10 (Brennan, J., dissenting).
146. *Id.* at 833 n.2 (majority opinion) (quoting *Monsanto*, 467 U.S. at 1007).
147. *Id.*
148. 65 U.S.P.Q.2d 1065, 1082 (1st Cir. 2002).
149. *See id.*

cilitates setting cookies without authorization should face secondary liability. Two Supreme Court cases have focused on liability[150] of providers of enabling technology: *Sony Corp. of America v. Universal City Studios, Inc.*[151] and *MGM v. Grokster*.[152]

Under *Sony*, it would be difficult to impose secondary liability on the producers of web browsers predicated on the use of those browsers to violate the rights of others. The *Sony* decision exonerated Sony from liability for the manufacture of videorecorders, even though the videorecorders could be used (and were shown to have been widely used) to violate the rights of copyright holders,[153] because the videorecorders were also capable of substantial uses which did not violate the rights of copyright holders.[154]

Analyzing the theory of liability for actions of others (in *Sony*, liability for contributory copyright infringement committed by third-party users of Sony's videorecorders), the Supreme Court held that the sale of videotape recorders,

> like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses. The question is thus whether the Betamax is capable of commercially significant noninfringing uses. In order to resolve that question, we need not explore *all* the different potential uses of the machine and determine whether or not they would constitute infringement. Rather, we need only consider whether on the basis of the facts as found by the District Court a significant number of them would be noninfringing.[155]

At the time that the *Sony* case reached the Supreme Court, no statute imposed secondary liability for facilitating violation of a copyright owner's rights.[156] However, the *Sony* court noted

> the absence of such express language in the copyright statute does not preclude the imposition of liability . . . on certain parties who have not themselves

150. Both cases were civil cases based on secondary liability for alleged violations of copyright. The copyright statute also has provisions imposing criminal liability. *See, e.g.*, 17 U.S.C. § 506 (2000).

151. 464 U.S. 417 (1984).

152. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005).

153. *See Sony*, 464 U.S. at 455 n.40.

154. *Id.*

155. *Sony*, 464 U.S. at 442. Betamax was Sony's brand of videotape recorder at the time; it used a proprietary recording format (Beta), which Sony no longer produces.

156. "The Copyright Act does not expressly render anyone liable for infringement committed by another. In contrast, the Patent Act expressly brands anyone who 'actively induces infringement of a patent' as an infringer, 35 U.S.C. § 271(b), and further imposes liability on . . . 'contributory' infringers, § 271(c)." *Sony*, 464 U.S. at 434–35. The Copyright Statute now does impose secondary liability in one particular circumstance: 17 U.S.C. § 905(3) prohibits inducing or knowingly causing infringement of semiconductor designs and raises questions as to whether the judicially created concept of secondary liability in the copyright act was implicitly narrowed by passage of this specific statutory statement of secondary liability.

> engaged in the infringing activity. For *vicarious liability is imposed in virtually all areas of the law*, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another.[157]

Traditionally, secondary liability for copyright infringement has been divided into two categories: contributory infringement and vicarious infringement.[158] Contributory infringement liability is imposed upon "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[159] Vicarious liability for copyright infringement is imposed upon a party who, while not directly committing infringement, facilitates infringement by another whom the vicariously liable party has "the right and ability to supervise [which] coalesce[s] with an obvious and direct financial interest in the exploitation of copyrighted materials."[160]

Since *Sony*-type vicarious liability requires either control over the primary infringer or financial benefit from the infringement, a defen-

---

157. *Sony*, 464 U.S. at 435 (emphasis added) (footnote omitted).

158. It is arguable that the *Sony* decision does not observe the traditional definitions in its use of the terms "contributory liability" and "vicarious liability." "[T]he [*Sony*] Court [treated] vicarious and contributory infringement interchangeably." *In re* Aimster Copyright Litig., 334 F.3d 643, 654 (7th Cir. 2003) (interpreting *Sony*, 464 U.S. at 435 & n.17).

159. Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (footnote omitted). Columbia Artists Management (CAMI) promoted a local community concert association that in turn sponsored a concert in which copyrighted musical compositions were performed without permission. The district court granted summary judgment against CAMI, stating that by "organizing, supervising, and controlling" the local association, and by "knowingly participat[ing]" in the association's infringing activity, CAMI caused the infringement. Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 312 F. Supp. 581, 583 (S.D.N.Y. 1970). The Second Circuit affirmed:

> With knowledge that its artists included copyrighted compositions in their performances, CAMI created the . . . audience as a market for those artists. CAMI's pervasive participation in the formation and direction of this association and its programming of compositions presented amply support the district court's finding that it "caused th[e] copyright infringement."

Gershwin, 443 F.2d at 1162–63 (quoting *Gershwin*, 312 F. Supp. at 583).

160. Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963) (holding a department store vicariously liable for copyright infringement by its record sales concessionaire). *See also* Dreamland Ball Room, Inc. v. Shapiro, Bernstein & Co., 36 F.2d 354 (7th Cir. 1929) (holding dance hall vicariously liable for copyright infringement committed by the orchestra it had hired); KECA Music, Inc. v. Dingus McGee's Co., 432 F. Supp. 72 (W.D. Mo. 1977) (holding cocktail lounge vicariously liable for infringement by musicians who played background music); *cf.* Artists Music Inc. v. Reed Publ'g Inc., 31 U.S.P.Q.2d 1623 (S.D.N.Y. 1994) (holding that landlord who received the same rent regardless of the profits earned by its tenant and who could not control the infringing activity on the premises was not vicariously liable for infringement by its tenant).

dant may escape liability by showing the lack of either. In addition, under *Sony*, a defense (imported from patent law) is available to secondary copyright defendants.[161] The exact nature of the defense is susceptible to at least four readings of the standard:

> [T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement *if the product is widely used for legitimate, unobjectionable purposes.* Indeed, it need merely be *capable of substantial noninfringing uses.* The question is thus whether the Betamax is *capable of commercially significant noninfringing uses.* In order to resolve that question, we need not explore *all* the different potential uses of the machine and determine whether or not they would constitute infringement. Rather, we need only consider whether on the basis of the facts as found by the District Court a *significant number of them would be noninfringing.*[162]

As technology advanced, subsequent cases considered the argument that providing software that facilitates widespread violations of rights could impose secondary liability on the provider of the software, with a split in the circuits over the correct reading of the *Sony* standard. For example, the Seventh Circuit found secondary infringement for facilitating peer-to-peer file sharing,[163] while the Ninth Circuit found such activities insufficient to impose secondary liability.[164]

Manufacturers of web browsers could not face secondary liability under any reading of the *Sony* standard, because web browser software clearly has significant uses which do not infringe user's rights. However, in 2005, the Supreme Court granted certiorari in *Grokster*[165] to resolve the conflict between the Seventh and Ninth Circuits' interpretations of *Sony*. MGM complained that software distributed by Grokster facilitated peer-to-peer transfer of files over the

---

161. *Sony*, 464 U.S. at 442. The Court stated,

> The staple article of commerce doctrine must strike a balance between a copyright holder's legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce. Accordingly, the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.

Id.

162. *Id.* (emphasis added to identify the possible ways to read the standard). For a suggested interpretation that harmonizes the four possible readings, see Max Stul Oppenheimer, *Yours for Keeps:* MGM v. Grokster, J. MARSHALL J. COMPUTER & INFO. L. 209 n.96 (2005).

163. *In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 540 U.S. 1107 (2004). Aimster was not a primary infringer; "because copies of the songs reside on the computers of the users and not on Aimster's own server, Aimster is not a direct infringer of the copyrights on those songs. Its function is similar to that of a stock exchange, which is a facility for matching offers rather than a repository of the things being exchanged . . . ." *Id.* at 646–47.

164. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004), *vacated*, 125 S. Ct. 2764 (2005).

165. 543 U.S. 1032 (2004).

Internet in violation of its copyrights.[166] MGM did not allege that Grokster had committed direct copyright infringement, but instead argued that Grokster was secondarily liable for enabling massive copyright infringement.[167]

The Court was unable to reach a majority decision on the *Sony* issue[168] and instead turned to a different basis for secondary liability: inducement.[169] The *Grokster* Court held that the basis of Grokster's liability was not limited to interpretations of *Sony*; the *Sony* decision "did not displace other theories of secondary liability,"[170] and secondary liability based on inducement could be established by showing "intent to bring about infringement and distribution of a device suitable for infringing use" plus "evidence of actual infringement by recipients of the device."[171] The Court found it significant that the defendants had not attempted to design their product so as to minimize the risk that it would be used to infringe others' rights.[172]

Browsers are set to accept cookies by default. This facilitates the widespread violation of users' rights. Unlike *Sony*, under *Grokster*, there can be secondary liability if a product facilitates a violation and the producer has not attempted to design it so as to minimize the risk of that violation. This may well be enough to run afoul of the *Grokster* standard. It would be a simple matter to set the defaults on browser software to reject cookies. Why, then, have the producers of browser software chosen to set the defaults to accept cookies? It would be difficult to construct an argument that would provide an alternative to the

166. The plaintiffs alleged that they "own the copyrights in most of the material infringed on Grokster and StreamCast, and they are the only copyright owners with sufficient resources and incentives to litigate effectively against respondents." Petition for Writ of Certiorari at 29, *Grokster*, 125 S. Ct. 2764 (No. 04-480).

167. MGM, in its petition for writ of certiori, alleged that "[m]ore than 2.6 billion infringing music files are downloaded each month," and that "between 400,000 and 600,000 copies of motion pictures are unlawfully downloaded each day." *Id.* at 8.

168. *Compare* concurring opinion of Justices Ginsburg, Rehnquist, and Kennedy, *Grokster*, 125 S. Ct. at 2783 (Ginsburg, J., concurring; with Rehnquist, C.J., Kennedy, J.), *with id.* at 2787 (Breyer, J., concurring; with Stevens and O'Connor, J.J.).

169. The "inducement" standard adopted by the Court was not argued by any of the parties, but was suggested in an amicus brief filed by Senators Leahy and Hatch. Brief Amici Curiae of United States Senator Patrick Leahy & United States Senator Orrin G. Hatch in Support of Neither Party at 13, *Grokster*, 125 S. Ct. 2764 (No. 04-480) (stating that *Sony* "explicitly and deliberately left aside liability based on inducement" (citing *Sony*, 464 U.S. at 439 n.19)).

170. *Grokster*, 125 S. Ct. at 2778 (plurality opinion).

171. *Id.* at 2782.

172. *Id.* at 2781 ("[The] evidence of unlawful objective is given added significance by MGM's showing that neither [defendant] attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software. . . . [W]e think this evidence underscores Grokster's and StreamCast's intentional facilitation of their users' infringement.")

obvious conclusion that business considerations drove the decision and that the manufacturers intended to bring about the result that servers could set cookies without clients' knowing authorization.

V. WHOSE LAW? WHOSE COURTS?

It is convenient to think of Internet transactions as taking place in "cyberspace." To date, however, cyberspace does not have a court system, so it is necessary to decide which of the existing courts can assert personal jurisdiction over parties who engage in transactions not tied to a specific physical location. Conceptually, there are arguable distinctions between transactions which a defendant has chosen to initiate[173] and those which the defendant has chosen to accommodate, but which the plaintiff initiated.[174]

While the analysis of these two types of transactions might differ, the constitutional framework is the same. Jurisdiction must be based on statutory authority and constitutional due process.[175] The statutory authority is typically provided by a long-arm statute, conferring jurisdiction over parties transacting business or causing injury in the forum state.

The fundamental constitutional test for jurisdiction is whether the defendant has "minimum contacts" with the forum jurisdiction "such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[176] Factors which have entered into the determination include:

1. Whether the defendant "purposefully avail[ed] itself of the privilege of conducting activities within the forum state."[177] Jurisdiction lies when a defendant has "'purposefully directed' his activities at residents of the forum."[178] In particular, jurisdiction is proper in the state where the injury occurs if the defendant placed the injurious products in "the stream of commerce with the

173. An example would be an e-mail sent by the defendant to the plaintiff. A further distinction could be drawn between transactions which the defendant chose to initiate with the specific plaintiff, and those which the defendant initiated with multiple parties (of whom the defendant was one) but without a specific intent to contact the specific defendant (e.g., spam).

174. An example would be a website, owned by the defendant, which set cookies without explicit permission of the plaintiff. Technically, the transaction would be initiated by the plaintiff's decision to visit the defendant's website. Conceptually, the plaintiff's website might be viewed as an attractive nuisance.

175. U.S. CONST. amend. XIV, § 1.

176. Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).

177. Hanson v. Denckla, 357 U.S. 235, 253 (1958).

178. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 472 (1985) (quoting Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 774 (1984)).

expectation that they will be purchased by consumers in the forum State;"[179]

2. Whether the claim arose out of the defendant's activity in the forum state;[180]
3. Whether the defendant "should reasonably anticipate being haled into court" in the forum state;[181] and
4. The state's interest and "fairness" to the parties.[182]

State courts have disagreed on whether sending an e-mail is sufficient to establish jurisdiction in the recipient's state. An Arkansas court has held it sufficient,[183] while a Utah court has held it insufficient.[184]

Maintaining an Internet site does not require the same specific decision to contact the forum state as does sending an e-mail. Although it might well fall within the reasoning of *World-Wide Volkswagen* that its contents are being placed in commerce with the knowledge that they might enter the forum state and cause injury, cases have held that merely maintaining a website which is accessed by a user in another jurisdiction is insufficient contact with the user's state to establish jurisdiction.[185] It is easy to see the practical reason why the two categories should lead to different results—otherwise, every website owner would be subject to jurisdiction in every state.

---

179. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297–98 (1980).

180. Perkins v. Benguet Consol. Mining Co., 342 U.S. 437, 445 (1952) (exercise of personal jurisdiction over the defendant requires contacts with the forum state that are "continuous and systematic"); *see also* McGee v. Int'l Life Ins. Co. 355 U.S. 220 (1957) (the least contact with the forum state that the Supreme Court has allowed is one contact).

181. *World-Wide Volkswagen*, 444 U.S. at 297.

182. Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102 (1987).

183. Kirwan v. State, 96 S.W.3d 724 (Ark. 2003) (relying on ARK. CODE ANN. § 5-27-304(a) (1997), which made it illegal to ship child pornography into the state).

184. Fenn v. MLeads Enter., Inc., 137 P.3d 706 (Utah 2006). The *Fenn* court found specific personal jurisdiction improper as violative of the due process clause where plaintiff, a Utah resident, received one unsolicited advertising e-mail without "ADV:" in the subject line as required by the Utah Unsolicited Commercial and Sexually Explicit Email Act, where defendant did not know specifically that its agent would send an e-mail to plaintiff or to any Utah resident and where plaintiff did not allege any economic, physical, emotional, or dignitary damages. The intermediate appellate court had noted, "[T]his issue is a matter of first impression in Utah and, as far as our research has revealed, in all of the United States." Fenn v. MLeads Enter., Inc., 103 P.3d 156, 159 (Utah Ct. App. 2004). There had already been other cases involving jurisdiction in the case of e-mail, but they involved massive e-mailings and the question of whether jurisdiction was proper where the ISP maintained the computer which handled the e-mails. Verizon Online Servs., Inc. v. Ralsky, 203 F. Supp. 2d 601 (E.D. Va. 2002); Internet Doorway, Inc. v. Parks, 138 F. Supp. 2d 773 (S.D. Miss. 2001); Washington v. Heckel, 93 P.3d 189 (Wash. Ct. App. 2004). Of course, the fact that the e-mails were sent by an agent would be no defense under traditional principles of *respondeat superior*.

185. Soma Med. Int'l v. Standard Chartered Bank, 196 F.3d 1292 (10th Cir. 1999).

Plaintiffs seeking to bring federal class actions have typically advanced multiple theories, including federal statutory, state statutory, and common law claims, but federal courts have been reluctant to retain jurisdiction when the federal claims have been dismissed. *Chance v. Avenue A, Inc.*[186] presents a typical complaint. There, the plaintiffs alleged that they had used the Internet, visited websites, and had an Avenue A "cookie" placed on their computers, thus permitting Avenue A to monitor their electronic communications without their knowledge, authorization, or consent. They moved for class certification to include tens of millions of Internet users, alleging violations of the federal Wiretap Act,[187] the Stored Communications Act,[188] the Computer Fraud and Abuse Act,[189] common law (invasion of privacy, trespass, and unjust enrichment), and Washington statutes prohibiting wiretapping and deceptive and unfair business practices. The court dismissed the federal statutory claims on definitional grounds[190] and, as a matter of discretion, declined to maintain supplemental jurisdiction over the remaining state causes of action, which it characterized as "novel and complex."[191]

VI. SOLUTIONS

The problems described above arise when there is a confluence of four conditions: (1) browsers are set to accept cookies by default; (2) server owners choose to set cookies; (3) some users are unaware of the fact that cookies are being set; and (4) a statute (which defines unlawful access sufficiently broadly to encompass setting cookies) prohibits unauthorized access to a computer. Removing any one of these conditions would insulate against criminal liability.

If browsers were set to deny cookies by default, then cookies could only be set if the user took a conscious step to enable them. This would constitute authorization under any of the statutes currently in force. If the cookie has been knowingly authorized, the issue of exceeding access authority disappears.[192]

186. 165 F. Supp. 2d 1153 (W.D. Wash. 2001).
187. Wire and Electronic Communications Interception and Interception of Oral Communications Act, 18 U.S.C. §§ 2510–2522 (2000 & Supp. IV 2004).
188. *Id.* § 2701(a).
189. *Id.* § 1030.
190. The plaintiffs failed to meet the CFAA requirement of $5,000 damages from a single act or event. *Chance*, 165 F. Supp. 2d at 1158–59. The court found sufficient authorization to avoid liability under the ECPA, and that the Wiretap Act did not apply because one party to the transaction had consented.
191. *Id.* at 1163.
192. The default would need to be set on a user-by-user basis or the authorization argument would fail. The problem of a user who is computer literate but legally incompetent—a relatively common situation—would remain. However, most statutes explicitly require knowingly unauthorized access as an element of the

Owners of websites can avoid liability by acquiring authorization broad enough to cover setting cookies.[193] There are a number of ways to accomplish this, such as providing conspicuous notice that the website is using cookies and a description of the information being stored. If users were to proceed with such knowledge,[194] the access to their computers would be authorized. Elementary contract law provides that authorization can be manifested by action and that formalities are not required.[195] This could be accomplished through a formal contract, entered into as part of the relationship (for example, where the user is a subscriber to a service). Authorization could also be obtained, however, by less formal means.[196]

A conspicuous notice on the home webpage stating that cookies are used and identifying what information is stored for how long should be sufficient, especially if coupled with the requirement of some action by the user indicating an understanding of the site's cookie policy. Again, this establishes authority (and follows the European Union's directive approach). In the future, if knowledge of the use of cookies were to become so widespread as to presume authorization, notice on a specific website might no longer be necessary.

Finally, the statutes could be changed. Given the range of state statutory standards and the reach of state statutes (governing transactions which involve a computer within their borders, regardless of the location of the website server), website owners and hosts would

---

offense, and those which are not explicit would likely be interpreted to require intent. *See supra* section IV.B.

193. There is, of course, another way to avoid liability: avoid the use of cookies.

194. This assumes the users are competent. The special problems of dealing with parties who are not competent is beyond the scope of this Article.

195. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 403 (2d Cir. 2004) ("We recognize that contract offers on the Internet often require the offeree to click on an 'I agree' icon. And no doubt, in many circumstances, such a statement of agreement by the offeree is essential to the formation of a contract. But not in all circumstances. While new commerce on the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract. It is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree." (citing RESTATEMENT (SECOND) OF CONTRACTS § 69 (1)(a) (1981)). *But see* Ticketmaster Corp. v. Tickets.com., Inc., CV99-7654-HLH(VBKx), 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 6, 2003) (apparently turning on the lack of an "I agree" button to signify assent).

196. Such means would, of course, need to meet the ordinary contract law requirements of offer and knowing acceptance. For example, in *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002), the court declined to enforce arbitration terms relating to Netscape's software because it was not clear that users downloading the software had necessarily seen the terms. The terms were posted on the website from which the user downloaded Netscape's software, but would not be seen unless the user scrolled down beyond the point where they could download the software.

benefit from a unified set of rules. While the owners of websites may initially be tempted to opt for the quick fix of a federal statute "immunizing" the use of cookies from liability, passage of such a statute would require overcoming clear public opposition.[197] Such a crude approach, however, is not needed. What is needed is a unified approach to jurisdiction, to eliminate the uncertainty of multiple state laws applying to the same transaction, plus such simple steps as notification in order to comply with the mainstream definition of consent. Internet transactions are clearly interstate commerce and Congress has repeatedly used its Commerce Clause power to regulate the Internet.[198] It could use that power to establish a unified national standard for obtaining permission to set cookies. This is not an area where the federalist principle of allowing state experimentation is appropriate, nor is it an area in which varying community standards might justify different rules in different communities. It is an area in which broad education and unified standards would benefit both users and website owners.

197. In the 2000 *Business Week* poll, *see* Harris Interactive, *supra* note 100, fifty-seven percent of the respondents felt that "the government should pass laws now for how personal information can be collected and used on the Internet." It is clear from the balance of the poll results, *see supra* note 100 and accompanying text; *see also infra* appendix, that the laws they have in mind are not ones that would foster growth of cookie use without consent.

198. While Congress struggles to find a constitutional way of regulating speech on the Internet, its early attempts—the Communications Decency Act of 1996, Pub. L. No. 104-104 § 502, 110 Stat. 133 (1994) (codified as amended at 47 U.S.C. § 223 (2002)), and the Child Online Protection Act (COPA), 47 U.S.C. § 231 (2000)—failed not for lack of congressional authority over the Internet, but for impact on free speech. The problem is one of drafting, not power.

APPENDIX

The following raw data was collected by a telephone survey of 1,014 adults between March 2 and March 6, 2000, by Harris Interactive:[199]

If you use a computer, have you ever heard of an online technology known as "cookies"?

Yes	40
No	60

If you have heard of cookies, which of the following best describes your understanding of what they are?

Files downloaded onto your computer that track your online habits	75
A hacker who breaks the security of private computer systems	5
The telephone number used to dial into an online service	4
The place where e-mail is stored indefinitely	3
Don't know	12

If you have heard of cookies, how often do you set your computer to reject them?

Always	21
Sometimes	21
Rarely	10
Never	43
Don't know	5

Some Web sites track personal information to match users with products and services that meet their needs. Other Web sites profit by sharing or selling user information to other organizations. If you use the Internet, how comfortable would you be if a Web site did the following?

Very Comfortable	Somewhat Comfortable	Not Very Comfortable	Not At All Comfortable	Not Sure
Tracked your movements when you browsed the site, but didn't tie that information to your name or real-world identity				
9	28	28	35	*
Merged your browsing habits and shopping patterns into a profile that was linked to your real name and identity				
3	7	21	68	1
Created a profile of you that included your real name and identity as well as additional personal information such as your income, driver's license, credit data, and medical status				
3	2	13	82	0

How comfortable would you be if a Web site did the following?

Very Comfortable	Somewhat Comfortable	Not Very Comfortable	Not At All Comfortable	Not Sure
Tracked your movements when you browsed the site, but didn't tie that information to your name or real-world identity				
9	28	28	35	*
Shared your information with other organizations				
1	6	25	67	*
Sold your information to other organizations				
1	5	19	74	*
Shared information so you could be tracked on multiple Web sites				
1	7	24	67	0–

199. Harris Interactive, *supra* note 100.