University of Arkansas at Little Rock Law Review

Volume 24 | Issue 3 Article 4

2002

Arkansas Surfers and Their Privacy, or Lack Thereof: Does the Common Law Invasion of Privacy Tort Prohibit E-Tailers' Use of "Cookies"?

Bryan T. McKinney

Dwayne Whitten

ARKANSAS SURFERS AND THEIR PRIVACY, OR LACK THEREOF: DOES THE COMMON LAW INVASION OF PRIVACY TORT PROHIBIT E-TAILERS' USE OF "COOKIES"?

Bryan T. McKinney[*]
Dwayne Whitten[**]

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.[1]

I. INTRODUCTION

Imagine the anachronism of Samuel Warren and Louis Brandeis, relaxing in the privacy of their Boston law office, surfing the Internet in the late nineteenth century. Perhaps they would log on to a Web site seeking directions to an upcoming vacation destination. Perhaps they would seek information regarding the week's weather forecast. Perhaps they would conduct a few hours of legal research, utilizing the many Web sites designed for this very purpose. If they understood the potential privacy ramifications of their actions, perhaps Warren and Brandeis would not surf the Internet at all. Warren and Brandeis's seminal article was prompted by what they saw as the excesses of a press empowered by increasingly sophisticated technology. Warren and Brandeis argued that the increasing pace of modern life and the technology associated with it tended to decrease individual privacy, but at the same time increase the individual's desire for it:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual, but modern enterprise and invention have, through invasions

* General Counsel and Assistant Professor of Business Law, Ouachita Baptist University. The author would like to thank his current colleagues at Ouachita Baptist University, and his former colleagues at the McMillan, Turner, McCorkle, and Curry Law Firm for their encouragement and support.

** Assistant Professor of Information Systems, Ouachita Baptist University.

1. With these words, Samuel Warren and Louis Brandeis, then law partners, introduced one of the most influential law review articles ever written, wherein they argued that the common law should protect an individual's right to privacy. *See* Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

> upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[2]

The same phenomenon still occurs. A modern example is what some consider the invasion of privacy that occurs when companies engaging in Internet commerce place monitoring information on their customers' computers, without their knowledge or consent. This practice, which involves the use of "cookies," is the subject of this article.

Several plaintiffs have recently filed unsuccessful lawsuits in federal court alleging that the use of cookies violates various federal laws.[3] In both *In re DoubleClick Inc. Privacy Litigation* and *Chance v. Avenue A, Inc.*, the plaintiffs alleged violations of federal law, as well as the common law tort of invasion of privacy. However, in both cases, the courts dismissed the federal claims, and subsequently refused to exercise supplemental jurisdiction over plaintiffs' remaining state common law invasion of privacy claims.[4]

In the context of individual privacy rights, this article will briefly consider the basic functions of the Internet and will then focus on the use of cookies by various Web-enabled companies.[5] Once a "rudimentary grasp" of the "architecture and engineering" of the Internet has been achieved,[6] it should be readily apparent that although the Internet offers society tremendous benefits, the Internet also presents complex questions regarding individual privacy rights.[7]

After a brief consideration of the *In re DoubleClick* and *Chance* cases, this article will consider in some detail whether or not the use of cookies could give rise to a successful lawsuit alleging the Arkansas common law

---

2. *Id.* at 196.

3. *See, e.g.*, Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001); *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

4. *See Chance*, 165 F. Supp. 2d at 1163 (noting that once the federal claims are dismissed, "novel and complex issues of state law predominate"); *In re DoubleClick*, 154 F. Supp. 2d at 526 ("[W]e have dismissed plaintiffs' federal claims which were the sole predicate for federal jurisdiction . . . . We decline to exercise supplemental jurisdiction over plaintiffs' state law claims.").

5. The concept of cookies will be addressed in further detail in Part II, but a brief definition may prove helpful. A cookie is defined as "[a] very small text file placed on your hard drive by a Web Page server." Microsoft Corporation, *Cookies: What They Are, Why You Are In Charge*, *at* http://www.microsoft.com/info/cookies.htm (last updated Nov. 2, 1999). Web browser software can use these cookie files to store specific information such as consumer name, products previously viewed on a site, and user names. Web servers can later access and use this data for a variety of purposes.

6. *In re DoubleClick*, 154 F. Supp. 2d at 500-01. Judge Buchwald noted that "[a]lthough a comprehensive description of the Internet is unnecessary to address the issues . . . , a rudimentary grasp of its architecture and engineering is important." *Id.*

7. *See, e.g.*, Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551 (1999).

tort of invasion of privacy.[8] This is an issue yet to be addressed by Arkansas courts, and as of the date of this writing, the authors of this article have found no published case law addressing the issue of whether the use of cookies violates an Internet user's common law right to privacy. Currently, federal law provides little relief to consumers who feel aggrieved by a Web-based retailer's use of cookies; however, one could argue that the use of cookies violates an Internet user's common-law right to privacy as defined by Arkansas courts.

II. BRIEF SURVEY OF THE INTERNET

In the current business environment, companies are increasingly relying on the collection, processing, and use of information related to consumers. Some of the more promising business uses of this data include targeted marketing, increased convenience of electronic commerce, and customized customer service, support, and Web pages in general.[9] Personal information can be gathered from product warrantees, retail scanners, automobile registration, and Web site visits, among other methods. Of particular importance is the data collected via the Web.[10]

Consumer data collected via the Web can enhance Web-based retailing efforts ("E-tailing"), providing the opportunity to employ a dynamic, real time, micro-marketing approach. As Internet usage continues to grow, E-tailing is becoming an increasingly important electronic business application.[11] A 1998 Internet survey reported that nearly one-half of all respondents reported purchasing products online at least once per month.[12]

The infomediary[13] industry has emerged to assist in the application of the consumer data that is gathered. Gathering customer data is an infomedi-

---

8. For a thorough and thoughtful analysis of Arkansas law regarding the tort of invasion of privacy, see John J. Watkins, *The Privacy Tort: An Arkansas Guide*, 1993 ARK. L. NOTES 91.

9. Stephen F. Ambrose, Jr. & Joseph W. Gelb, *Consumer Privacy Regulation and Litigation*, 56 BUS. LAW. 1157, 1157 (2001).

10. *See* George R. Milne & Andrew J. Rohm, *Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives*, 19 J. PUB. POL'Y & MARKETING 238, 238 (2000).

11. *See* J. Yannis Bakos, *The Emerging Role of Electronic Marketplaces on the Internet*, 41 COMM. ASS'N COMPUTING MACHINERY 35, 35 (1998); *see also* Varun Grover & James Teng, *E-Commerce and the Information Market*, 44 COMM. ASS'N COMPUTING MACHINERY 79, 79 (2001).

12. Georgia Tech Research Corp., *Frequency of Purchasing Online*, *at* http://www.gvu.gatech.edu/user_surveys/survey-1998-10/graphs/shopping/q124.htm (Oct. 1998).

13. "Infomediaries" are companies that collect consumer profile data, store the data, and then analyze the data to build customer profiles. These profiles can be used to create custom marketing efforts on Web pages as Web users visit Web sites. The term "infomediary" is derived from the concatenation of information and intermediary, ultimately meaning "a

ary's first function.[14] The data may be gathered in a number of ways. Customer registration on Web sites is the easiest and least expensive method. Companies may provide incentives such as the chance to win a prize, the offer of free software, or the opportunity to play an online game to motivate a potential customer to complete the form. Other sites may require a registration process before accessing the services available on that particular site. The well-known Internet research company Gartner Group uses this tactic, requiring users to complete a registration form before accessing the research published on their site.[15]

In addition to collecting data from their own Web visitors, companies can purchase data from other companies that also use online forms or collect data via cookies.[16] Cookies can be used to store specific information, which a Web server can later retrieve.[17] Specific examples of cookie use include:

- Storing a list of items in a virtual shopping cart until the consumer is ready to complete the transaction. This is more efficient than the Web server storing the data, since thousands of people may be shopping on the site at the same time;
- Storing consumer names so that consumers can be greeted with a customized message when they make a return visit to a particular site;
- Logging the pages that have been visited on a particular Web site;
- Storing the type of information requested from the site;
- Storing the product pages viewed; and
- Storing usernames and passwords.[18]

The privacy issue arises by virtue of the fact that cookies may be created without the consent of or disclosure to the visitor. The data collection methods discussed so far may offer benefits to E-tailers such as providing some personal data and a minimal amount of past online behavior. While this data is useful in predicting future purchasing decisions, a complete consumer knowledge base requires more extensive demographic and lifestyle data. Infomediaries offer supplemental data that is based on consumer profiles from national offline consumer database compiler companies such as Polk Company in Southfield, Michigan, and Naviant in Newtown Square,

---

company that utilizes information in a process involving at least two other entities."

14. *See* Table 1, *infra* p. 755.

15. Gartner, Inc., *Privacy Policy*, *at* http://www3.gartner.com/6_help/18a.html (last visited Feb. 10, 2002).

16. H.M. DEITEL ET AL., E-BUSINESS AND E-COMMERCE FOR MANAGERS 751 (2001); *see supra* note 5 (defining "cookie").

17. Microsoft Corporation, *supra* note 5.

18. *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001).

Pennsylvania. These companies collect and organize data from sources such as credit card companies, censuses, surveys, product registration and warranty cards, and vehicle registrations. The table below provides a more complete listing of demographic and behavioral attributes that are included in the infomediary knowledge bases.

Table 1: Examples of Consumer Data Stored

Basic demographics	• Age • Gender • Income • Marital status
Family demographics	• Number of adults and children in household • Owner/renter • Length at residence • Occupation
Lifestyle dimensions	• Outdoors • Fitness • Domestic • Cultural • Blue chip • Do-it-yourself • Technology
Automotive	• Type of car • Number and age of vehicles owned
High tech	• Computer • Cell phone • Reference and educational software • Pager • Games
Direct mail purchases	• Photo equipment • Home furnishings • TV • Apparel
Source: Cogit.com	

The companies specializing in consumer profiles sell their data to infomediaries such as Cogit.com, DoubleClick, and Engage Technologies. These infomediaries may also collect Web activity information from other companies as well. For example, infomediaries may have agreements with hundreds of companies that allow the infomediary access to the customer data they control.

Even past purchasing patterns on given Web sites are available if requested.[19] For example, the recent alliance between Cogit.com and the Polk

19. Janis Mara, *Cogit.com Service Offers Profiling and Predictions*, ADWEEK-E.

Company has generated data on over 100 million households covering over 1000 demographic attributes.[20] Newer releases of the software are based on consumer demographics, Web activity, purchasing patterns, and customer interests. Thus, they are able to add considerable knowledge to the process of suggesting product offerings and promotions of interest to the individual online.

E-tailers can supplement the knowledge from the infomediary with their own clickstream data, which is the history of the Web pages a Web surfer has visited. This data provides a valuable source of information about the current behavior of site visitors, especially point-of-sale data, which details the products purchased. Another source of information is log files. These files tell where visitors are coming from, what they do while on the site, and where and when they leave. By integrating data from these two sources with the infomediary knowledge, E-tailers have an even more accurate model of predicted visitor behaviors. Companies such as America Online and Columbia House are already combining purchased consumer data with their customer data to build their own customer knowledge bases. Some companies in turn sell this online data to infomediaries or information vendors who may in turn sell to infomediaries. Over time, this process makes the knowledge of an individual consumer's behavior more valuable to all E-tailers using infomediaries.

Data collection is constrained by privacy laws in the European Union (EU), resulting in a reduced scope for data collection by infomediaries.[21] Published reports of information abuses and EU privacy laws have led to an increased concern about online privacy in the United States as well. Although some sites publish their privacy policies and provide E-verification company logos and symbols, privacy remains a critical issue. According to a recent Gallup Poll survey, seventy-eight percent of respondents are concerned about personal privacy when online, and seventy-one percent of individuals are concerned with the use of cookies.[22]

United States companies are limited in the collection of data involving transactions from the EU countries due to the *European Community Directive on Data Protection* 95/46/EC.[23] These standards for EU countries, di-

---

EDITION, Mar. 13, 2000, at 44.

20. *Cogit.com*, *at* http://www.directionsmag.com/pressreleases.asp?PressID=1039 (last visited Mar. 1, 2002).

21. *See generally* Michael Fjetland, *Global Commerce and the Privacy Clash*, INFO. MGMT. J., Jan.-Feb. 2002, at 54.

22. *Online Privacy Concerns Continue to Linger*, COMMUNITY BANKER, Sept. 2001, at 44, 46.

23. Council Directive 95/46/EC, 1995 O.J. (L 281) 31. The Directive went into effect on October 28, 1998. Donna Gillin, *Safe Harbor Principles for the European Privacy Directive Are Finalized*, MARKETING RES., Winter 2000, at 41, 41.

rected at the online privacy of personal data, are more stringent than those in the United States. Personal data on citizens of EU countries cannot be exported to countries that do not have similar privacy protection.[24] In response to this directive, the United States Department of Commerce worked with the EU to develop "safe harbors," a set of common principles designed to provide the minimal level of privacy required for export of data outside of the EU. The EU accepted these principles as adequate protection on July 27, 2000.[25] As a result, companies could once again use the services of infomediaries for EU consumer data, although the infomediaries were limited in the scope of collectable data.

The process of analyzing a consumer's behavior in comparison with other consumers who have shown similar purchasing patterns is called collaborative filtering.[26] Based on this analysis, infomediaries not only share consumer data and composite profiles, but also share predictions about an individual consumer's behavior. This knowledge is the basis of customization. A list of products that should be of interest to the visitor may be displayed on the Web page in a convenient and obvious location.

When a potential customer visits the site, a personally identifiable attribute is sent to the infomediary. This data is checked against the infomediary knowledge base to determine whether a match exists. Assuming a match is made, the infomediary submits the consumer's personal data for processing in the decision model. This subset of data is then stripped of any personal identification in efforts to protect individual privacy. Next, the infomediary processes the data to determine the best fit of the individual to the market segment. Then, based on past behaviors of consumers in that group, recommendations[27] are made by the infomediary to the E-tailer on content for the visitor.[28]

The process described above relies exclusively on the assimilation and gathering of data that many consumers deem private. A gap exists between the current federal legislation and the perception of many Internet users

24. Gillin, *supra* note 23, at 41.

25. *Id.*

26. See Gordon A. Wyner, *Life (on the Internet) Imitates Research*, MARKETING RES., Summer 2000, at 38, for a discussion of collaborative filtering.

27. For example, if a particular user's profile consisted of a young male, living in Texas, owner of a four-wheel drive truck, and his previous Web site visits include Remington Arms Company, Texas Parks and Wildlife, and Cabela's Outfitter, then a likely banner ad to be presented on the Web page being visited could be for a hunting retail store. *See* Remington Arms Co., Inc., *Remington Home Page*, *at* http://www.remington.com/default (last visited Feb. 10, 2002); Texas Parks & Wildlife, *Texas Parks & Wildlife Home Page*, http://www.tpwd.state.tx.us/ (last modified Feb. 9, 2002); Cabela's Inc., *Cabela's Online Store—Quality Hunting, Fishing, Camping, and Outdoor Gear*, *at* http://www.cabelas.com/ (last visited Feb. 10, 2002).

28. *Cogit.com*, *supra* note 20.

regarding what is and is not private domain. In response to this division between the perception of privacy and the law's protection of privacy, a number of bills have been introduced in the 107th Congress.[29] While each may attempt to protect privacy in different ways, collectively they may be thought to combat an Orwellian prophecy whereby an individual's every move is tracked by businesses for profit concerns.

III. *DOUBLECLICK* AND *CHANCE*: PROOF THAT FEDERAL LAWS PROVIDE LITTLE PROTECTION

Two recent federal cases, *In re DoubleClick* and *Chance v. Avenue A Inc.*, illustrate the futility of consumers' reliance upon existing federal laws to prohibit individual privacy invasions through the use of cookies. This section examines these two cases, focusing first on the leading case, *In re DoubleClick.*

A. *In re DoubleClick Inc. Privacy Litigation*

The plaintiffs brought a class action against DoubleClick, seeking injunctive and monetary relief for injuries allegedly suffered due to DoubleClick's purported illegal conduct. Members of the class were defined as "[a]ll persons who, since 1/1/96, have had information about them gathered by DoubleClick as a result of viewing any DoubleClick products or services on the Internet or who have had DoubleClick 'cookies' . . . placed upon their computers."[30] The plaintiffs brought three claims arising under federal law,[31] alleging that DoubleClick's actions violated the Stored Communications Act,[32] the Computer Fraud and Abuse Act (CFAA),[33] and the Federal

29. *E.g.*, Consumer Internet Privacy Enhancement Act of 2001, H.R. 237, 107th Cong. (2001); *see also* Electronic Privacy Protection Act of 2001, H.R. 112, 107th Cong. (2001); Online Privacy Protection Act of 2001, H.R. 89, 107th Cong. (2001); *infra* note 65. While these proposed bills seek to protect consumers' on-line privacy interests, governmental response to the tragic events of September 11, 2001 will create unique and challenging privacy considerations. For example, on October 24, 2001, the government enacted the USA Patriot Act with the following purposes in mind: "to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes." USA Patriot Act of 2001, Publ. L. No. 107-56, 115 Stat. 272 (2001). While many will find these goals admirable and even necessary, the realization of these goals is not without privacy ramifications. For example, the Patriot Act significantly expands the federal government's ability to conduct electronic surveillance. While a thorough analysis of this act is beyond the scope of this article, the USA Patriot Act does present novel questions for privacy advocates.

30. *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 500 n.1 (S.D.N.Y. 2001) (quoting plaintiffs' May 26 amended complaint).

31. *Id.*

32. 18 U.S.C. §§ 2701-2711 (2000). Title II of the Electronic Communications Privacy

Wiretap Act.[34] The plaintiffs also brought four state law claims alleging the common law tort of invasion of privacy, common law unjust enrichment, common law trespass to property, and violation of two state statutes.[35] The dispositive motion before the court was defendant's motion to dismiss the plaintiffs' claims pursuant to Federal Rule of Civil Procedure 12(b)(6).[36]

Writing for the court, Judge Buchwald first provided a thoughtful explanation of the Internet and the services offered by DoubleClick, focusing on targeted banner advertisements and cookie information collection.[37] In its discussion, the court first considered the Stored Communications Act and determined that its goal was to prevent hackers from obtaining, altering, or destroying certain stored electronic communications.[38] The Act defines the prohibited conduct as follows:

> Except as provided in subsection (c) of this section whoever (1) intentionally accesses without authorization a facility through which an electronic information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such system shall be punished . . . .[39]

The Stored Communications Act also provides an important exception: "Subsection (a) of this section does not apply with respect to conduct au-

---

Act is referred to as the "Stored Communications Act."

33. 18 U.S.C. § 1030 (2000), *amended by* Pub. L. No. 107-56, 115 Stat. 272 (2001).

34. 18 U.S.C. §§ 2510-2522 (2000).

35. *In re DoubleClick*, 154 F. Supp. 2d at 500. Specifically, the plaintiffs alleged violations of sections 349(a) and 350 of article 22A of the New York General Business Laws. *See* N.Y. GEN. BUS. LAW §§ 349(a), 350 (McKinney 1988) (providing protection from deceptive acts and practices).

36. *In re DoubleClick*, 154 F. Supp. 2d at 500; *see* FED. R. CIV. P. 12(b)(6).

37. *In re DoubleClick*, 154 F. Supp. 2d at 500-05. Generally, the court explained that DoubleClick's process of targeting banner advertisements involves three participants (the user, the DoubleClick-affiliated Web site, and the DoubleClick server). *Id.* at 503. This process involves four steps, which the court outlined as follows: (1) the user seeks access to a Web site affiliated with DoubleClick, at which time the user's browser requests that site's homepage; (2) the site processes the request, sends a copy of the page (minus any banner advertisements), and sends an Internet Provider (IP) link to the DoubleClick server that instructs the user's computer to automatically send a communication to DoubleClick; (3) the user's computer sends a communication to DoubleClick containing such information as a cookie identification number, the Web site that the user accessed, and the type of browser that the user has; and (4) DoubleClick uses this information to identify the user's profile and to determine what advertisements it will send to the user, then sends a communication to the user's computer containing the banner advertisements. *Id.* at 503-04. Another thorough description of the Internet may be found in *Reno v. ACLU*, 521 U.S. 844 (1997).

38. *See In re DoubleClick*, 154 F. Supp. 2d at 507.

39. 18 U.S.C. § 2701(a) (2000).

thorized . . . by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user . . . ."[40]

After a thorough analysis of the Stored Communications Act,[41] the court concluded that the "plaintiffs' GET, POST and GIF submissions are excepted from § 2701(c)(2) because they are 'intended for' [only those] DoubleClick-affiliated Web sites who have authorized DoubleClick's access."[42] The court determined that the cookie identification numbers sent to DoubleClick from the plaintiffs' computers "fall outside of Title II's protection because they are not in 'electronic storage.'"[43] Had this information been in electronic storage, DoubleClick would have been authorized to access "its own communications."[44]

Having discarded the Title II Stored Communications Act claim, the court moved on to consider the Wiretap Act.[45] Consistent with the Stored Communications Act, the Wiretap Act also provides a relevant prohibition and an exception.[46] The Wiretap Act provides for a private right of action against

> any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire,

---

40. *Id.* § 2701(c).

41. *See In re DoubleClick*, 154 F. Supp. 2d at 507-13. For a concise, helpful discussion of the Stored Communications Act, see Holly K. Towle & Aimee Arost, *Online Liability: Digital Boundaries*, at 177, *in* SEVENTH ANNUAL INSTITUTE FOR INTELLECTUAL PROPERTY LAW (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, PLI Order No. G0-00PS/2, 2001).

42. *In re DoubleClick*, 154 F. Supp. 2d at 513. The court explained what GET, POST, and GIF submissions are:

> GET information is submitted as part of a Web site's address or "URL," in what is known as a "query string." For example, a request for a hypothetical online record store's selection of Bon Jovi albums might read: *http://recordstore.hypothetical.com/search?terms=bonjovi.* The URL query string begins with the "?" character meaning the cookie would record that the user requested information about Bon Jovi.
>
> Users submit POST information when they fill in multiple blank fields on a Webpage. For example, if a user signed up for an online discussion group, he might have to fill in fields with his name, address, email address, phone number and discussion group alias. The cookie would capture this submitted POST information.
>
> Finally, DoubleClick places GIF tags on its affiliated Web sites. GIF tags are the size of a single pixel and are invisible to users. Unseen, they record the users' movements throughout the affiliated Web site, enabling DoubleClick to learn what information the user sought and viewed.

Id. at 504.

43. *Id.* at 513.

44. *Id.* at 513-14.

45. *See id.* at 514.

46. DoubleClick conceded that its actions, as pleaded, violated this prohibition. *Id.*

> oral, or electronic communication . . . . [However] . . . [i]t shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception *unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or any State.*[47]

The court determined that DoubleClick was entitled to take advantage of the exception in 18 U.S.C. § 2511(2)(d) because DoubleClick and its affiliated Web sites are "parties to the communication[s]" as defined in the exception.[48] The only remaining issue in the Wiretap Act claim was whether or not DoubleClick's actions were conducted for the purpose of committing any criminal or tortious act. Looking to the legislative history and case law interpreting this section,[49] the court found as a matter of law that the plaintiffs failed to show that DoubleClick acted with a tortious purpose.[50]

The court then turned its attention to the CFAA.[51] Section 1030(g) stated the following:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief . . . . Damages for violations involving damage as defined in section (e)(8)(A) are limited to economic damages . . . .[52]

---

47. 18 U.S.C § 2511 (2000) (emphasis added).

48. *In re DoubleClick*, 154 F. Supp. 2d at 514.

49. The court explained that "[s]ection 2511(2)(d)'s legislative history and caselaw make clear that the 'criminal' or 'tortious' purpose requirement is to be construed narrowly, covering only acts accompanied by a specific contemporary intention to commit a crime or tort." *Id.* at 515. Quoting *Sussman v. ABC*, 186 F.3d 1200, 1202 (9th Cir. 1999), the court stated that under this section

> the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for interception—its intended use—was criminal or tortious . . . . Although ABC's taping may well have been a tortious invasion under state law, plaintiffs have produced no probative evidence that ABC had an illegal or tortious purpose when it made the tape.

In re DoubleClick, 154 F. Supp. 2d at 516. For examples of other cases addressing tortious purpose, see *Deteresa v. ABC*, 121 F.3d 460 (9th Cir. 1997); *J.H. Desnick v. ABC*, 44 F.3d 1345 (7th Cir. 1995); *Boddie v. ABC*, 881 F.2d 267 (6th Cir. 1989).

50. *See In re DoubleClick*, 154 F. Supp. 2d at 519.

51. *See id.* at 519-20.

52. 18 U.S.C. § 1030(g) (2000), *amended by* Pub. L. No. 107-56, § 814(e), 115 Stat. 272, 384 (2001). Section 1030(g), which has been amended since *In re DoubleClick*, now reads:

Section 1030(e)(8) defined "damage" as

> any impairment to the integrity or availability of data, a program, a system, or information that—(A) causes loss aggregating at least $5000 in value during any 1-year period to one or more individuals; (B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals; (C) causes physical injury to any person; (D) threatens public health or safety.[53]

The plaintiffs argued that the $5000 minimum should be calculated in the aggregate, not individually, but the court disagreed with the proposed aggregation.[54] The court later concluded that the plaintiffs failed to prove the losses and damages caused by DoubleClick's access to a single computer over one year's time could meet § 1030(e)(8)(A)'s $5000 requirement.[55] As previously mentioned, upon the disposal of the federal law claims, the court refused to exercise supplemental jurisdiction over the state law claims.[56]

B. *Chance v. Avenue A, Inc.*

The *Chance* case is quite similar to the *In re DoubleClick* case.[57] The plaintiffs (again, in a class action) alleged that the defendant's unauthorized placement of cookies on plaintiffs' computers enabled the defendant "to monitor [their] electronic communications without plaintiffs' knowledge,

---

> A civil action for a violation of this section may be brought only if the conduct involved 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.

§ 814(e), 115 Stat. at 384.

53. 18 U.S.C. § 1030(e)(8), *amended by* Pub. L. No. 107-56. § 814(d)(3), 115 Stat. 272, 384 (2001). Section 1030(e)(8) now simply defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." § 814(d)(3), 115 Stat. at 384. Subsection (a)(5)(B)(i) of § 1030 now sets out the circumstances under which economic damages are recoverable:

> Whoever . . . by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) . . . loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value.

Id. § 814(a)(4), 115 Stat. at 383.

54. *See In re DoubleClick*, 154 F. Supp. 2d at 519-26.

55. *Id.* at 526.

56. *Id.*; *see also supra* note 4.

57. *Compare* Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001), *with In re DoubleClick*, 154 F. Supp. 2d 497.

authorization, or consent."[58] In *Chance*, the plaintiffs also alleged the defendant violated the Wiretap Act, the Stored Communications Act, and the Computer Fraud and Abuse Act, in addition to various state law claims.[59] At issue before the court were the defendant's motion for summary judgment and the plaintiffs' motion to strike portions of declarations and motion for summary judgment.[60] Relying heavily on the *In re DoubleClick* case, the court granted defendant's motion for summary judgment.[61]

Given the courts' recent interpretation of federal law, it appears that plaintiffs will struggle to assert valid claims against companies such as DoubleClick based on the Stored Communications Act,[62] the CFAA,[63] and the Federal Wiretap Act.[64] Until Congress adopts a more stringent federal law safeguarding consumer privacy on the Internet,[65] consumers may, however, attempt to hold these companies liable for the common law tort of invasion of privacy. The following section considers whether Arkansas courts might entertain such a cause of action.

IV. APPLICATION OF THE ARKANSAS TORT OF INVASION OF PRIVACY

There is certainly no excess of case law regarding the invasion of privacy tort in Arkansas. The first Arkansas case to formally recognize this

---

58. *Chance*, 165 F. Supp. 2d at 1155.

59. *Id.*

60. *Id.*

61. *Id.* at 1163. The court stated, "Plaintiffs' attorneys have brought nearly identical claims against other leading digital advertising and media companies such as DoubleClick and MatchLogic. In a very thorough opinion, the District Court for the Southern District of New York recently dismissed with prejudice a virtually identical claim against DoubleClick under Rule 12(b)(6)." *Id.* at 1155. *Cf. In re DoubleClick*, 154 F. Supp. 2d at 497. Because of the similarity between the two opinions, further discussion regarding *Chance* is not merited.

62. 18 U.S.C. §§ 2701-2712 (2000); *see supra* notes 38-44 and accompanying text.

63. 18 U.S.C. § 1030 (2000), *amended by* Pub. L. No. 107-56, 115 Stat. 272 (2001); *see supra* notes 51-55 and accompanying text.

64. 18 U.S.C. §§ 2510-2522 (2000); *see supra* notes 45-50 and accompanying text.

65. *See, e.g.*, Consumer Internet Privacy Act of 2001, H.R. 237, 107th Cong. (2001). This bill would render illegal the practice of commercial Web site operators collecting personally identifiable information online from users of that Web site unless the operator provides (1) notice to the user of the Web site and (2) an opportunity to that user to limit the use of marketing purposes, or disclosure to third parties of personally identifiable information collected. *Id.*; *see also* Online Privacy Protection Act of 2001, H.R. 89, 107th Cong. (2001). Developed to protect those individuals not covered by the Children's Online Privacy Protection Act of 1998, this Act would make it unlawful for a Web site operator or online service to collect, use, or disclose various personal information without appropriate notice and other safeguards. Online Privacy Protection Act of 2001, H.R. 89, 107th Cong. (2001); *see* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, § 1301 (codified at 15 U.S.C. §§ 6501-6506 (2000)).

privacy tort is *Olan Mills, Inc. v. Dodd*,[66] decided in 1962. In his opinion, Justice McFaddin acknowledged, "[w]hile there is a dearth of case law in Arkansas on the point, there are cases, textbook writings, and law review articles elsewhere."[67]

In the forty years since Justice McFaddin's opinion, Arkansas courts have had relatively few opportunities to address invasion of privacy claims.[68] Nonetheless, Arkansas courts have provided adequate guidance to practitioners by indicating the courts' acceptance of the four categories of invasion of privacy as adopted by the *Restatement (Second) of Torts*.[69] These four categories are: intrusion upon seclusion; appropriation of name or likeness; publicity given to private life; and publicity that places a person in false light.[70] Thus, an analysis of existing Arkansas case law, as well as an analysis of case law originating in other jurisdictions that have also adopted the *Restatement*, should provide an adequate framework with which to consider the privacy issues raised by an E-tailer's use of cookies.

A. Intrusion upon Seclusion

The *Restatement* explains the tort of intrusion upon seclusion as follows: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[71] The Arkansas Supreme Court first considered an intrusion upon seclusion claim in *CBM v. Bemel*.[72] In *Bemel*, a defendant collection agency repeatedly harassed the plaintiff with letters (over fifty) and telephone calls (approximately seventy) seeking to collect a hospital bill representing charges incurred by the plaintiff's child. Relying on the tort of invasion of privacy, the court affirmed the jury's verdict of $1000 for compensatory damages, and $4000 for punitive damages.[73]

66. 234 Ark. 495, 353 S.W.2d 22 (1962).

67. *Id.* at 497, 353 S.W.2d at 23.

68. *See, e.g.*, Dunlap v. McCarty, 284 Ark. 5, 678 S.W.2d 361 (1984); CBM v. Bemel, 274 Ark. 223, 623 S.W.2d 518 (1981); Dodrill v. Ark. Democrat Co., 265 Ark. 628, 590 S.W.2d 840 (1979).

69. *See, e.g.*, *Dunlap*, 284 Ark. 5, 678 S.W.2d 361; *Dodrill*, 265 Ark. 628, 590 S.W.2d 840.

70. RESTATEMENT (SECOND) OF TORTS § 652A (1977) [hereinafter RESTATEMENT].

71. *Id.* § 652B.

72. 274 Ark. 223, 623 S.W.2d 518 (1981).

73. *Id.* at 224, 623 S.W.2d 519. In addition to the letters and telephone calls, the plaintiff claimed an employee of the defendant represented that he worked for the prosecuting attorney's office. Perhaps this representation played a role in the punitive damage award. *See id.*, 623 S.W.2d 519.

Shortly after the *Bemel* decision, the Arkansas Supreme Court had another opportunity, in *Dunlap v. McCarty*,[74] to consider a case wherein the plaintiff alleged the privacy tort of intrusion upon seclusion.[75] Though the court concluded the plaintiff's claim was barred by the statute of limitations, the case helped further develop the Arkansas privacy tort. In *Dunlap*, the court acknowledged that

> the Restatement . . . gives five examples of invasion of privacy by intrusion, which are briefly: a reporter takes plaintiff's picture in a hospital room against plaintiff's wishes; a detective looks into plaintiff's windows; a detective wiretaps plaintiff's phones; the defendant examines the plaintiff's bank records for evidence in a civil action; and the defendant, a professional photographer, telephones the plaintiff repeatedly to have her picture made.[76]

Comment b is perhaps more helpful than the illustrations when analyzing the unauthorized placement of cookies on one's computer. Comment b states that:

> The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself . . . over the plaintiff's objection . . . . It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs . . . . It may be by some other form of investigation or examination into his private concerns . . . . The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the . . . information collected.[77]

An argument could be made that the unauthorized placement of cookies onto one's computer is generally the type of behavior prohibited by Comment b of the *Restatement*. The placement of the cookie is a physical invasion into a place a reasonable person could presume to be secluded.[78] Whether or not Internet users are aware that cookies have been placed on their computers, evidence indicates that most Internet users consider their actions on the Internet to be private.[79]

---

74. 284 Ark. 5, 678 S.W.2d 361 (1984).

75. *See id.* at 9, 678 S.W.2d at 364 (relying on RESTATEMENT § 652B, illus. 1-5).

76. RESTATEMENT, *supra* note 70, § 652B cmt. b, illus. 1-5.

77. *Id.* § 652B cmt. b.

78. *See supra* note 22 and accompanying text.

79. Various studies have considered Internet users' privacy expectations. A common theme discovered through these efforts is that Internet users want a guarantee of some degree of privacy when they utilize the Internet. In addition, most Internet users favor opt-in standards for the collection of personal information, rather than the opt-out standards that are currently endorsed by the Federal Trade Commission. *See, e.g.*, SUSANNAH FOX ET AL., PEW INTERNET & AM. LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO

Fletcher v. Price Chopper Foods of Trumann, Inc.[80] is a recent case from the United States Court of Appeals for the Eighth Circuit applying Arkansas law regarding the privacy tort of intrusion upon seclusion. In *Fletcher*, the court clarified that this tort consists "[o]f three parts: (1) an intrusion (2) that is highly offensive (3) into some matter in which a person has a legitimate expectation of privacy."[81]

Regarding the intrusion element, the court stated that an intrusion occurs when an actor "believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act."[82] The placement of a cookie on one's hard drive requires a physical intrusion. The question then remains whether or not companies such as DoubleClick lack the legal or personal permission to commit this act. The distinction between legal and personal permission is significant.[83] Even if existing federal legislation does not prohibit intrusive acts, these acts should not occur absent the personal permission of the Internet user.

The second element of this tort requires an act that is highly offensive. While the collection of names, addresses, and other public information may not be highly offensive,[84] the collection of certain information regarding consumers could be highly offensive to a reasonable person. For example, an Internet user may access a medical Web site seeking information regarding an illness she has contracted. Assuming the Internet user does not wish to disclose the facts of her illness, the disclosure of the fact that she visited the medical Web site could be highly offensive.

REWRITE THE RULES 2 (Aug. 20, 2000), *available at* http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.

80. 220 F.3d 871 (8th Cir. 2000).

81. *Id.* at 875-76.

82. *Id.* at 876 (quoting O'Donnell v. United States, 891 F.2d 1079, 1083 (3d Cir. 1989)).

83. If an E-tailer lacks *either* legal *or* personal permission to collect personal information imbedded within a cookie, then the E-tailer has arguably satisfied the intrusion element. A report issued by the Pew Internet and American Life Project determined that eighty-six percent of Internet users support an opt-in provision. FOX ET AL., *supra* note 79, at 2. Thus, the vast majority of users do not give E-tailers personal permission to collect personal information simply by virtue of the fact that a Web site has been visited. *See id.* Opt-in provisions serve as appropriate mechanisms by which Internet users may notify E-tailers that personal permission to collect specified personal information has been granted. The Pew report echoes the argument of Warren and Brandeis:

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others . . . . [I]f he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them.

Warren & Brandeis, *supra* note 1, at 198.

84. The *Restatement* echoes this theme: "Thus there is no liability for the examination of a public record concerning the plaintiff . . . ." RESTATEMENT, *supra* note 70, § 652B cmt. c.

The third element of the intrusion upon seclusion tort requires the consumer to have a legitimate expectation of privacy. As the *Fletcher* court stated, "A legitimate expectation of privacy is the touchstone of the tort of intrusion upon seclusion."[85] In order to have a legitimate expectation of privacy, Internet users must conduct themselves in a manner consistent with an actual expectation of privacy. According to the *Fletcher* court, "a person's behavior may give rise to an inference that he no longer expects to maintain privacy in some aspect of his affairs."[86]

Comment b of the *Restatement* affirms this principle that a person's behavior serves as evidence of whether or not that person has an expectation of privacy. Comment b clarifies that the invasion must be "over the plaintiff's objection."[87] Companies such as DoubleClick who offer "opt-out" provisions would argue that the placement of cookies was not over the plaintiff's objection. If plaintiffs object, they may simply opt out. For example, the DoubleClick Web site educates interested consumers, and explains to them how they may opt out.[88] However, while many consumers are concerned about their privacy with regard to their use of the Internet, some consumers are simply unaware that their privacy is at risk and are unaware that they may opt out.

The fact that a consumer could prevent any invasion by utilizing an opt-out mechanism, but fails to do so, should not bar recovery. For example, the second illustration in Comment b of *Restatement* section 652B states: "A, a private detective seeking evidence for use in a lawsuit, rents a room in a house adjoining B's residence, and for two weeks looks into the windows of B's upstairs bedroom through a telescope taking intimate pictures with a telescopic lens. A has invaded B's privacy."[89] In this illustration, B could certainly prevent A from invading B's privacy. B could install and close blinds, blocking the view through B's window. Or, B could simply avoid rooms with windows. The fact that B has not done so should not imply that B has no legitimate expectation of privacy. Likewise, if a computer user perceives the placement of cookies to be an invasion of privacy, and fails to utilize an opt-out provision, this should not bar recovery.

Many privacy advocates, as well as several proposed federal laws, argue that companies such as DoubleClick must provide "opt-in" rather than "opt-out" opportunities. The distinction is significant. By requiring an opt-in

85. *Fletcher*, 220 F.3d at 877.

86. *Id.* (quoting Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994)).

87. RESTATEMENT, *supra* note 70, § 652B cmt. b.

88. DoubleClick, ***Ad Cookie Opt-Out***, *at* http://www.doubleclick.com/us/corporate/privacy/privacy/ad-cookie/default.asp?asp_object_1=d (last visited Feb. 10, 2002); *see also* DoubleClick, *Privacy Policy: Brief Overview*, *at* http://www.doubleclick.com/us/corporate/privacy/privacy/default.asp?asp_object_1=& (last updated Nov. 19, 2001).

89. RESTATEMENT, *supra* note 70, § 652B cmt. b, illus. 2.

provision, only those consumers who acquiesce to the use of cookies will participate. If the law merely requires an opportunity to opt out, the privacy of many unassuming Web surfers will be compromised.

B. Appropriation of Name or Likeness

Olan Mills Inc. v. Dodd,[90] the first Arkansas case to recognize the invasion of privacy tort in Arkansas, was based upon an appropriation theory.[91] In *Olan Mills*, the plaintiff sought the services of Olan Mills Photography, wanting to give a photograph of herself to her daughter. Once the photograph was taken, the plaintiff assumed "the transaction was closed."[92] However, the transaction was far from closed. Olan Mills affixed the plaintiff's photograph to 150,000 advertising post cards that were published and distributed throughout Arkansas and surrounding states without the plaintiff's prior knowledge or consent.[93] In addition to the postcards, Olan Mills's door-to-door salespersons carried enlargements of the plaintiff's photograph to solicit orders.[94] The Arkansas Supreme Court affirmed the jury's unanimous verdict of $2500.[95] The Court refused to further develop the appropriation tort in this case, limiting the opinion to the particular facts of the case.[96]

Since *Olan Mills*, the Arkansas courts have had little opportunity to consider the appropriation tort. One of the few appropriation cases applying Arkansas law is *Stanley v. General Media Communications, Inc.*[97] The *Stanley* case is factually unique, to say the least. The plaintiffs were two female high school juniors who voluntarily participated in a contest in a pavilion on the beach in Panama City.[98] Defendant General Media later published a photograph of the fully clothed plaintiffs, taken during the contest, in *Penthouse* magazine.[99]

---

90. 234 Ark. 495, 353 S.W.2d 22 (1962).

91. *See id.*, 353 S.W.2d at 22.

92. *Id.* at 496, 353 S.W.2d at 23.

93. *Id.*, 353 S.W.2d at 23.

94. *Id.*, 353 S.W.2d at 23.

95. *Id.* at 499, 353 S.W.2d at 24.

96. *Olan Mills*, 234 Ark. at 498, 353 S.W.2d at 24 ("It is unnecessary to develop in greater detail the nature of the cause of action; because our opinion herein is limited to the particular facts of this case and the extent of the damages here awarded.").

97. 149 F. Supp. 2d 701 (W.D. Ark. 2001).

98. *Id.* at 704. According to the court, "The contest rules required each participant to place a blindfold over her eyes, unwrap a condom, and place the condom on a 'demonstrator' . . . . The winner of the contest was the participant who finished the task in the shortest amount of time." *Id.*

99. *Id.*

The plaintiffs filed suit, alleging libel, intentional infliction of emotional distress, and the invasion of privacy torts of appropriation and false light.[100] The plaintiffs' invasion of privacy claims were dismissed on summary judgment.[101] The court began its analysis of the appropriation claim by quoting from *Restatement* section 652C, which "provides that '[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.'"[102]

Claiming that appropriation requires the commercial use of a person's name or likeness,[103] the court relied heavily on the fact that *Penthouse* apparently did not capitalize on the plaintiffs' likeness to sell copies of its magazine.[104] The court noted that the photo depicted plaintiffs as either fully clothed or wearing a swimsuit, sitting behind a table, and laughing or smiling. Without so claiming, but perhaps taking judicial notice, the court explained, "Given the content of the publication as a whole, the Court is confident that no reasonable jury could conclude that *Penthouse* magazine intended or expected that patrons would buy the magazine on the basis of the photo at issue."[105] *Penthouse*'s use of the photograph can clearly be distinguished from the use made of personal information collected by companies such as DoubleClick. DoubleClick and its competitors *do* capitalize on Internet users' personal information in order to gain commercial advantage.[106]

Comment b to § 652C of the *Restatement* addresses the question of how one's name or likeness may be appropriated.[107] The comment states, "The common form of invasion of privacy under the rule here stated is the

---

100. *Id.*

101. *Id.* at 708.

102. *Id.* at 706 (quoting RESTATEMENT § 652C).

103. *Stanley*, 149 F. Supp. 2d at 706. Curiously, the *Restatement*, which has been adopted and cited with approval many times by Arkansas courts, does not limit the tort of appropriation to *commercial* appropriation cases:

> Apart from statute, however, the rule stated is not limited to commercial appropriation. It applies also when the defendant makes use of the plaintiff's name or likeness for his own purposes and benefit, even though the use is not a commercial one, and even though the benefit sought to be obtained is not a pecuniary one.

RESTATEMENT, *supra* note 70, § 652C cmt. b.

104. *Stanley*, 149 F. Supp. 2d at 706 ("More importantly, there is no evidence that *Penthouse* capitalized on the Plaintiffs' likeness to sell copies of its 25th Anniversary Edition.").

105. *Id.*

106. *See, e.g.*, Jessica J. Thrill, *The Cookie Monster: From Sesame Street to Your Hard Drive*, 52 S.C. L. REV. 921, 945 (2001) ("Websites gather information using cookies in order to create an individual's profile. Once the profile is complete, the Web site utilizes the user's identity to its advantage—it is either used to create individualized advertising or sold to other companies for profit.").

107. RESTATEMENT, *supra* note 70, § 652C cmt. b.

appropriation and use of the plaintiff's name or likeness to advertise the defendant's business or product, or for some similar commercial purpose."[108] The *Stanley* court expressly concluded that the defendant, General Media Communications Inc. (the publisher of *Penthouse*), did not use the photograph for the purposes of advertising the defendant's product.[109]

DoubleClick's use of personal information is another matter. The very purpose of DoubleClick seemingly involves the appropriation and use of personal information regarding consumers. DoubleClick specializes in collecting, compiling, and analyzing information about Internet users through proprietary technologies and techniques.[110] DoubleClick creates value for its customers by building detailed profiles of Internet users.[111]

Businesses such as DoubleClick claim that the nonconsensual dissemination of personal information does not amount to appropriation. At first glance, three cases seem to support this position. *Shibley v. Time, Inc*,[112] *Dwyer v. American Express Co.*,[113] and *U.S. News & World Report v. Avrahami*[114] involve the defendants' nonconsensual dissemination of the plaintiffs' personal information. In each case the plaintiffs were denied recovery under an appropriation theory.

A brief consideration of *Dwyer* may prove helpful.[115] In *Dwyer*, the plaintiff sued American Express alleging that the company's policy of compiling and selling lists of card members' names and addresses amounted to the tort of appropriation.[116] At first glance, the activities of American Express and DoubleClick appear quite similar. Both companies compile and sell personal information regarding consumers, often without consumers' consent. Because of the similarity of these actions, one might expect similar treatment of their activities under the law.

However, the activities are quite distinct. In *Dwyer,* following the reasoning in *Shibley*, the court claimed there is little to no value in one name, expressly stating, "a single, random cardholder's name has little or no in-

108. *Id.*
109. *See supra* note 104 and accompanying text.
110. *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
111. *Id.*
112. 341 N.E.2d 337 (Ohio Ct. App. 1975).
113. 652 N.E.2d 1351 (Ill. App. Ct. 1995).
114. No. 96-203, 1996 WL 1065557 (Va. Cir. Ct. June 13, 1996).
115. *See* 652 N.E.2d 1351.
116. *Id.* at 1353. The court explained the process as follows:

> In order to characterize its cardholders, defendants analyze where they shop and how much they spend, and also consider behavioral characteristics and spending histories. Defendants then offer to create a list of cardholders who would most likely shop in a particular store and rent that list to the merchant. Defendants also offer to create lists which target cardholders who purchase specific types of items, such as fine jewelry.

Id.

trinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names."[117] DoubleClick, on the other hand, creates tremendous value for itself and for other merchants using a single name.[118] DoubleClick collects information regarding individuals that is valuable to DoubleClick and its clients regardless of whether or not that individual has been categorized or aggregated as part of any list.

C. Publicity Given to Private Life

According to the *Restatement*, "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized . . . (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[119] Arkansas courts have simply not had the occasion to develop this tort.[120]

Nonetheless, an analysis of the *Restatement* sheds light on how Arkansas courts might resolve complaints alleging a public disclosure of private facts. Four questions must be asked in order to determine whether or not this tort has been committed. Was the matter publicized?[121] If so, did the matter publicized involve the private life of another?[122] If so, was the publication highly offensive to the ordinary reasonable person?[123] If so, was the

---

117. *Id.* at 1356.

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

119. RESTATEMENT, *supra* note 70, § 652D.

120. *See* Milam v. Bank of Cabot, 327 Ark. 256, 937 S.W.2d 653 (1997). In *Milam*, the plaintiffs' complaint alleged, among other things, invasion of privacy. *Id.* at 259, 937 S.W.2d at 654-55. While the facts of the case could have given rise to an allegation based on public disclosure of private facts, the Milams's failure to plead with specificity was fatal. Thus, the court affirmed summary judgment, and refused to address the public disclosure tort, stating that:

> the Milams do not state which theory of privacy invasion applies to their case. It is also difficult to ascertain both from the complaint and from the Milams' argument whether the invasion was caused by the alleged acquisition of the financial information from the bank by Thompson or Thompson's alleged communication of it to the railroad policemen. In addition, the Milams do not cite any authority to support violation of their privacy rights, and we decline to research this point for them . . . . In sum, we will not develop this claim for the Milams. That was their responsibility. A conclusory allegation by the Milams is not sufficient to ward off summary judgment.

Id. at 264, 937 S.W.2d at 657 (internal citations omitted).

121. RESTATEMENT, *supra* note 70, § 652D cmt. a.

122. *Id.* at cmt. b.

123. *Id.* at cmt. c.

matter of legitimate public concern?[124] If the answers to the first three questions are yes, and the answer to the fourth question is no, then a plaintiff has a cause of action for publication of private facts. An argument could be made that the dissemination to third parties of information collected by DoubleClick in the form of cookies amounts to the public disclosure of private facts.

If an Internet user were to sue DoubleClick, publicity would likely be the most challenging element to prove. The *Restatement* clearly distinguishes the "publicity" element of a public disclosure claim from the "publication" element of a defamation claim.[125] For purposes of defamation, publication includes any communication by the defendant to a third person.[126] However, publicity, as an element of the public disclosure tort, requires:

> that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge . . . . On the other hand, any publication . . . in a handbill distributed to a large number of persons . . . is sufficient to give publicity within the meaning of the term as it is used in this Section. The distinction, in other words, is one between private and public communication.[127]

Assuming the Web company declines to disclose the information collected to an outside source, the publicity element is likely to fail. However, if the Web company gives, loans, or sells this information to a third party advertiser, the publicity element may be satisfied.

Assuming the matter was publicized, did the matter involve the private life of another? Generally, if a Web site only collects information that is of public record, no cause of action will lie for public disclosure of private facts.[128] However, the disclosure of non-public information is not authorized by the *Restatement*, and should remain private.[129]

Was the publication highly offensive to the ordinary reasonable person? The *Restatement* observes, "The protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place,

---

124. *Id.* at cmt. d.

125. *Id.* at cmt. a.

126. *Id.* Thus, the disclosure of a defamatory statement from DoubleClick to a client of DoubleClick would satisfy the publication element for a defamation claim.

127. RESTATEMENT, *supra* note 70, § 652D cmt. a.

128. *Id.* The Restatement explains that "[t]here is no liability for giving publicity to facts about the plaintiff's life that are matters of public record, such as the date of his birth, the fact of his marriage." *Id.* at cmt. b.

129. *See* Thrill, *supra* note 106, at 939 ("[U]nless the data collected by cookies is a matter of accessible public record, information not voluntarily disclosed by an individual should remain private and secret.").

to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens."[130] The *Restatement* appears to support the argument that what is today highly offensive may not be so tomorrow. If today's Internet users have a legitimate expectation of privacy during their use of the Internet, then perhaps the publication would be highly offensive. Clearly, the publication of certain information (such as one's access to a medical Web site) is more offensive than the publication of other information (such as one's name).

Finally, the plaintiff must prove that the information publicized was not of a legitimate public concern.[131] Addressing this issue indirectly, the United States Supreme Court has held that the First Amendment prohibits the recovery for disclosure of and publicity to facts that are of public record.[132] The Court has indicated that an invasion of privacy claim cannot be maintained where the subject matter of the publicity involves a matter of "legitimate concern to the public."[133] Obviously the public benefits from the free flow of information. Nonetheless, this appreciation for information should not unduly jeopardize an individual's right to privacy. An individual's mouse clicks are simply not a matter of legitimate public concern.

D. Publicity Placing a Person in False Light

According to the *Restatement*, publicizing information that sheds "false light" on another creates liability to the one so injured for invasion of his privacy, if a reasonable person would find the "false light" "highly offen-

130. RESTATEMENT, *supra* note 70, § 652D cmt. c.

131. *Id.* at cmt. d.

132. Cox Broadcasting Co. v. Cohn, 420 U.S. 469 (1975); *see also* RESTATEMENT, *supra* note 70, § 652D cmts. c–d.

133. *Cox*, 420 U.S. at 492. In *Lewis v. Harrison School Dist. No. 1*, a federal case arising out of Arkansas, the court addressed the issue of what is and is not a legitimate concern to the public. 621 F. Supp. 1480 (W.D. Ark. 1985). The plaintiff, a principal in the Harrison School district, filed suit alleging retaliatory discharge in violation of his First Amendment rights. The plaintiff claimed he was fired for publicly disagreeing with the superintendent's decision to transfer the plaintiff's wife. Though the *Lewis* court focused on free speech rather than invasion of privacy issues, it acknowledged that "[w]hether expression is of a kind that is of legitimate concern to the public is also the standard in determining whether a common law action for invasion of privacy is present." *Id.* at 1486 (quoting Connick v. Myers, 461 U.S. 138, 143 (1983)). The court noted that whether or not a statement is of legitimate concern to the public is determined by the content, form, and context of a given statement. *Id.* The court concluded that the plaintiff's speech was not of a legitimate concern to the public because it was "'primarily the expression of personal invective' rather than legitimate input into matters of current public concern." *Id.* at 1489. Again quoting *Connick*, the court explained that if an "expression cannot be fairly considered as relating to any matter of political, social, or other concern to the community," then an expression is likely not of public concern. *Id.* at 1486 (quoting *Connick*, 461 U.S. at 146). Thus, the argument that a person's lawful Internet use is of any political, social, or other concern to the community lacks merit.

sive," and if the actor either knew or showed "reckless disregard" concerning the "falsity of the publicized matter and the false light in which the other would be placed."[134]

It appears highly unlikely that a plaintiff could successfully allege a false light cause of action against a defendant who utilized cookies for advertising purposes. Suppose a defendant uses information contained in a cookie to place the plaintiff in a false light that would be highly offensive to a reasonable person. While this action would satisfy the first element of the false light tort, the plaintiff would still struggle mightily to prevail on a false light claim. To satisfy the second element of this tort in Arkansas, courts require a showing of actual malice by clear and convincing evidence.[135] The defendant who utilizes cookies would have acted in reliance on action taken by or information submitted by the plaintiff. Given the fact that information contained in cookies is derived from the user, or potential plaintiff, a false light claim appears nearly impossible to construct.

V. CONCLUSION

Considering once again the introductory anachronism of Samuel Warren and Louis Brandeis surfing the Internet, what words of wisdom might they impart today? What would they conclude about an E-tailer's use of cookies to collect personal information? Presumably, they would appreciate the Internet's potential for tremendous societal benefit. However, they would temper this appreciation with a concern regarding the Internet's profound potential for compromising the personal privacy of millions of Internet users. Until more expansive federal legislation is enacted to protect Internet users, Warren and Brandeis might once again seek protection under the common law.

Does an Internet user have a remedy to combat possible violations of privacy? If asked this question, perhaps Warren and Brandeis would conclude today, as they did in 1890: "Has he then such a weapon? It is believed that the common law provides him with one, forged in the slow fire of the centuries, and today fitly tempered to his hand."[136] The century-old words of Warren and Brandeis are no less applicable today. Perhaps today's weapon is the common law invasion of privacy tort.

---

134. RESTATEMENT, *supra* note 70, § 652E.

135. Peoples Bank & Trust v. Globe Int'l Publ'g, Inc., 978 F.2d 1065 (8th Cir. 1992); Stanley v. Gen. Media Communications, Inc., 149 F. Supp. 2d 701 (W.D. Ark. 2001); Dodson v. Dicker, 306 Ark. 108, 812 S.W.2d 97 (1991); Dodrill v. Ark. Democrat Co., 265 Ark. 628, 590 S.W.2d 840 (1979).

136. Warren & Brandeis, *supra* note 1, at 220.