South Carolina Law Review

Volume 52
Issue 4 *ANNUAL SURVEY OF SOUTH CAROLINA LAW*

Article 8

Summer 2001

The Cookie Monster: From Sesame Street to Your Hard Drive

Jessica J. Thrill

THE COOKIE MONSTER: FROM SESAME STREET TO YOUR HARD DRIVE

I. INTRODUCTION

DoubleClick, Inc. is on the verge of becoming the cookie monster of the decade, but instead of gobbling cookies up, DoubleClick, Inc. is giving Internet "cookies" out by the handful. The use of Internet cookies by DoubleClick and similar firms has sparked criticism by consumer protection groups and privacy advocates over current trends involving companies that market an Internet user's identity as a commodity and the underlying privacy issues these practices raise.

Cookies are numerical identifiers deposited onto a user's hard drive in order to recognize an Internet user each time she accesses a certain website.[1] Internet companies use cookies primarily to collect information about the user-site preferences, shopping habits, search queries, clickstreams and sometimes even a user's name, e-mail address, and other personal information.[2] However, cookies also allow websites to personalize site information, offer shopping cart capabilities, remember user names and passwords for future visits, and monitor website traffic statistics.[3]

Cookies may provide valuable benefits to online consumers, but their application comes at the cost of relinquishing personal information. That cost equation is significantly compounded by an Internet user's expectations of privacy. Privacy expectations among Internet users likely vary, depending upon that user's understanding of the Internet.[4] The majority of everyday Internet

---

1. Joe Ashbrook Nickell, *Tracking the Elusive User*, INDUSTRY STANDARD (Nov. 6, 2000), *available at* http://www.findarticles.com/cf_0/m0HWW/45_3/66673084/print.jhtml (defining a cookie as a tiny text file containing unique identifying characteristics or long string of random characters, placed on a user's computer by a Web server); Ronaleen R. Roha, *Prying Eyes*, KIPLINGER'S PERS. FIN. MAG. (Aug. 2000), *available at* http://www.findarticles.com/cf_0/m1318/8_54/63668182/print.jhtml; Hope Viner Samborn, *Nibbling Away at Privacy: Cookies are Lurking in Your Hard Drive, Ready to Grab User Data*, A.B.A. J., June 2000, at 26.

2. Nickell, *supra* note 1; Roha, *supra* note 1; Samborn, *supra* note 1, at 26.

3. DOUBLECLICK, INC., ABOUT ONLINE ADVERTISING, *at* http://www.privacychoices.org/content_cookies.htm (last visited Oct. 17, 2000).

4. The Georgia Institute of Technology conducted a survey examining how aware users are of cookies and how users implement available cookie security options. *See* GEORGIA INSTITUTE OF TECHNOLOGY, GVU'S EIGHTH WWW USER SURVEY: COOKIE POLICY™ (October 1997), *at* http://www.gvu.gatech.edu/user_surveys/survey-1997-10/graphs/use/Cookie_Policy.html [hereinafter COOKIE POLICY SURVEY]. The survey was broken down into four sub-surveys: (1) location (all, U.S.A., and Europe), (2) gender, (3) age, and (4) experience. *Id.* The Survey concluded:

> A full quarter of respondents don't know what cookies are (25%) which suggests that an education effort might be in order. For the rest, 22% always accept cookies and about the same percentage (23%) receive a

users, who have acclimated themselves enough with Internet technology to point and click, probably use the Internet under the false pretense of anonymity.[5] At most they realize they are identified online as myalias@ipaddress.com. However, few are aware that cookies exist, how they work or what their function is, or their effect on the user's privacy or anonymity.[6] Other Internet users may have heard the term in passing or may even be aware cookies are lurking on their hard drive, but fail to realize the privacy implications and continue using the Internet with a subjective expectation of privacy.[7]

Even users who understand what a cookie is and believe they are taking adequate precautions against them may still be leaving themselves vulnerable to online profiling.[8] Most Internet users would be shocked to know that

---

> warning before cookies are set, allowing them to make a decision on a case-by-case basis. Interestingly, only 14% of user[sic] don't know what their cookie policy is suggesting that the rest (61%) have made an explicit choice about their policy. Respondents from Europe and males tend to be more knowledgeable about cookies. Females who are knowledgeable about cookies, however, tend to be more cautious: 48% of knowledgeable females ask for warnings compared to 38% of knowledgeable males and 33% always accept cookies compared to 41% of males. As we would expect, novices are much less knowledgeable about cookies than experts.

Id. Of the novices polled, 47% did not know what a cookie was, while only 7% of users who consider themselves experts did not know what a cookie was. *Id.* The survey did not address whether the individuals who knew what a cookie was understood how they were implemented or what the privacy ramifications are. *Id.*

5. *See generally* Jerry Berman & Deirdre Mulligan, *Privacy In the Digital Age: Work In Progress*, 23 NOVA L. REV. 551, 558 (1999) ("When individuals surf the World Wide Web, they have a general expectation of anonymity, more so than in the physical world where an individual may be observed by others."); *On the web, No One is Anonymous*, FORBES (Nov. 29, 1999) *at* www.forbes.com/forbes/1999/1129/64131182s1_print.html ("On the web you sense that you're invisible."); Scott Woolley, *We Know Where You Live*, FORBES GLOBAL (Nov. 13, 2000), *available at* www.forbes.com/global/2000/1113/0323130a_print.html ("At its heart the Internet has always been an anonymous medium. Internet addresses, a series of up to 12 numbers designed to locate computers on a network, leave few clues to where in the world a computer user actually sits.").

6. *See* COOKIE POLICY SURVEY, *supra* note 4. If 47% of novices and 7% of experts are unaware of what a cookie is, it is unlikely they understand how cookies work, what their function is, or a cookie's effect on their privacy or anonymity. *See id.*

7. *See id.* Among novices, 52% claim to know what a cookie is as compared to 81% of intermediates, but 19% of novices and 12% of intermediates do not know what their cookie preferences are set to. *Id.*

8. Only 9% of novices, 28% of intermediates and 33% of experts have set their preferences to warn the user before accepting a cookie. *See id.* Although the survey addresses cookie policy options implemented by users, it does not provide data on those users who choose to be warned but accept or decline cookies regardless, nor does it address the basis for a user's acceptance or declination. *See id.* Users who implement warning preferences may believe they are taking adequate precautions to protect their privacy. But the novice and intermediate users may not be able to differentiate between the cookies they are accepting and declining. For example, it is unlikely a user can differentiate between a cookie used for site recognition or shopping cart capabilities versus a cookie used to collect personal information or for data

someone given only a user's Internet Protocol (IP) address could obtain the user's name, address, birth date and social security number, all with the click of a button and in less than five minutes,[9] or that in a single visit a website can identify a user's computer type, e-mail address, Internet address, browser and operating system, and installed plug-ins.[10] In addition, a user would be astounded to know that the same individual could also obtain information such as unlisted or unpublished telephone numbers, financial accounts, salaries, utility bills, vehicle registration, previous addresses, names and addresses of relatives and neighbors, and so forth.[11] Even when a consumer has voluntarily relinquished their information to a website for various purposes, it is doubtful she knows this information is being aggregated with other databases and disbursed or sold to other corporations.[12] Therefore, Internet users are paying for online convenience with personal information—one of today's most valuable commodities—without their knowledge.

However, the word is getting out and users are catching on. Recent surveys show Internet users want to regain control of their personal information.[13] According to a survey by Odyssey, a market research firm, ninety-two percent

---

profiling. *See generally* David Cartwright, *Learn More About Who Uses Your Site*, INTERNET MAG. (June 2000), *available at* http://www.findarticles.com/cf_0/m0CXD/2000_June/63329680/print.jhtml (explaining how to profile users when their browsers reject cookies or do not support them).

9. Adam L. Penenberg, *The End of Privacy*, FORBES.COM (Nov. 29, 1999), *at* www.forbes.com/forbes/1999/1129/6413182a.html.

10. Rob Fixmer, *Traveling the Web Without Leaving Footprints*, N.Y. TIMES (Aug. 16, 1999), *available at* www.nytimes.com/library/tech/99/08/biztech/articles/16data.html.

11. Penenberg, *supra* note 9; *see also* AUTOTRACK, http://www.autotrackxp.com (an online database service that, for a fee, will provide some or all of the following information: all names, aliases, companies and addresses associated with an individual; an individual's social security number, including the state and date of issuance; names and addresses of relatives and neighbors; all vehicles registered or associated with an individual; and indications of possible criminal records).

12. Craig Bicknell, *DoubleClick's Single Focus: You*, WIRED NEWS (June 14, 1999), *available at* http://www.wired.com/news/print/0,1294,20205,00.html; Stuart McClure, *Security Watch: 'Personal' Marketing Appeals to Sellers and Some Consumers, But Your Privacy Will Suffer*, INFO WORLD (Dec. 13, 1999), *available at* http://www.findarticles.com/cf_0/m0IFW/50_21/58238838/print.jhtml; Chris Oakes, *Groups Keep Heat on DoubleClick*, WIRED NEWS (June 29, 1999), *available at* http://www.wired.com/news/print/0,1294,20485,00.html; Roha, *supra* note 1.

13. Denise Caruso, *Exploiting–and Protecting–Personal Information*, N.Y. TIMES (Mar. 1, 1999), *available at* www.nytimes.com/library/tech/99/03/biztech/articles/01digi.html (citing 1997 Georgia Tech survey showing that eighty-seven percent of Internet users "want 'complete control' over their personal data"); *see also* Fixmer, *supra* note 10 (stating Harris poll showed "fears of losing privacy were the top reason people decided not to go online"); Andrew Leonard, *Your Profile, Please*, SALON (June 26, 1997), *available at* www.salon.com/june97/21st/article970626.html (stating surveys show Internet users do not trust Internet companies with personal information); Bob Tedeschi, *Targeted Marketing Confronts Privacy Concerns*, N.Y. TIMES (May 10, 1999), *available at* www.nytimes.com/library/tech/99/05/cyber/commerce/10commerce.html (stating users are uneasy about the amount of information websites know about them).

of Internet users do not trust Internet companies to keep personal information confidential, regardless of the company's privacy policy, and eighty-two percent believe the government should regulate the use of personal information on the Internet.[14] However, as Andrew Leonard points out in his article *Your Profile, Please*, "The Catch-22 is obvious: to truly protect user privacy would negate the Net's direct-marketing potential."[15] Therefore, the questions remains how to effectively allow Internet companies to use cookies and online profiling without compromising users' rights to protect the privacy of their personal information.

Part II of this Comment uses DoubleClick, Inc. as a primary example of an Internet advertising company that employs cookies and online profiling. It also discusses pending litigation against DoubleClick, Inc., including a complaint filed by the Electronic Privacy Information Center (EPIC) and the responses of DoubleClick, Inc., the Federal Trade Commission (FTC), various legislators, technologies firms, and privacy advocates. Part III analyzes the basis for claims and relief, including the foundation for the right to privacy, the traditional privacy torts, trespass, and anti-stalking laws. It also discusses the ramifications of the proposed FTC regulations on civil claims.

II. BACKGROUND

A. DoubleClick, Inc.

DoubleClick, Inc., a Delaware corporation with its principal office in New York, is the largest Internet advertising provider on the market, delivering 1.5 billion ads per day to Internet users.[16] When a user accesses a website displaying a DoubleClick banner ad, a cookie is electronically deposited onto the user's hard drive.[17] Between 1996 and 1997 alone, DoubleClick deposited more than forty million cookies.[18] Usually, the user is oblivious to the deposit, and this is precisely what has privacy advocates concerned.[19] Advertising firms are tracking consumer behavior and collecting personal information, without the consumer ever knowing a cookie is documenting her every move.[20]

---

14. Steve Lohr, *Survey Shows Few Trust Promises on Online Privacy*, N.Y. TIMES (Apr. 17, 2000), *available at* www.nytimes.com/library/tech/00/04/biztech/articles/17data.html.

15. Leonard, *supra* note 13.

16. FEDERAL TRADE COMMISSION, ONLINE PROFILING: A REPORT TO CONGRESS 3 n.9 (June 2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf [hereinafter FTC JUNE 2000 REPORT]; Elizabeth H. Wang, *Tackling the Web's Privacy Problems*, NAT'L L.J., Apr. 24, 2000, at B1.

17. Roha, *supra* note 1; Brenda Sandburg, *Class-Action Lawsuits Becoming the Way to Police Privacy Matters on the Internet*, MIAMI DAILY BUS. REV., July 3, 2000, at A1.

18. Kristi Coale, *DoubleClick Tries to Force Hand into Cookie Jar*, WIRED NEWS (Mar. 17, 1997), *available at* http://www.wired.com/news/print/0,1294,2615,00.html.

19. *Id.*

20. *See infra* note 118.

These concerns heightened in June 1999 when DoubleClick, Inc. announced it was acquiring Abacus Direct in a $1 billion stock swap.[21] Abacus Direct, a Colorado firm, runs America's largest catalog database, collecting data on the buying behavior of individual consumers.[22] The database currently has buying profiles spanning five years on eighty-eight million American households.[23] Abacus Direct not only collects this information, but it also sells the user profiles to advertisers who want to target consumers.[24]

DoubleClick's acquisition of Abacus Direct opens an entirely new pandora's box of privacy issues. The merger of Doubleclick's online database with Abacus' offline database would allow DoubleClick to cross-reference user information, specifically identifying an individual and destroying the false security created by screen names and the anonymity associated with Internet use.[25] DoubleClick was using this information to engineer individually-tailored advertising,[26] but the current onslaught of lawsuits and investigations has forced DoubleClick to rethink its position.[27] However, DoubleClick is not alone; other web companies are also joining forces with ad targeting firms.[28] For example, Engage Technologies is working closely with Accipiter Technologies, portal player Excite just bought MatchLogic, and Imgis entered into an exclusive agreement with Metromail.[29]

B. Pending Litigation against DoubleClick, Inc.

DoubleClick has become the target for widespread litigation and has been named as defendant in a number of individual lawsuits and class actions in both

---

21. *See* Bicknell, *supra* note 12.
22. *See id.*
23. *See id.*
24. *See id.*
25. Michael S. Yang, *E-Commerce: Reshaping the Landscape of Consumer Privacy*, MD. B.J., July-Aug. 2000, at 14.
26. Bicknell, *supra* note 12; McClure, *supra* note 12.
27. Yang, *supra* note 25, at 15.
28. Craig Bicknell, *For Sale: Your Tastes, Interests*, WIRED NEWS (June 24, 1998), *available at* http://www.wired.com/news/print/0,1294,13212,00.html; *see also* Marius Meland, *The Other Online Profiler*, FORBES.COM (Feb. 25, 2000), *at* http://www.forbes.com/2000/02/25/mu2.html (stating 24/7 Media has been even more successful than DoubleClick at collecting consumer profiles for its database because consumers share their personal information when they sign up for an e-newsletter, but consumers may be unaware the extent of information used and for what purpose).
29. Bicknell, *supra* note 28.

federal and state courts.[30] In July 2000, DoubleClick was estimated to be the defendant in fifteen pending lawsuits.[31]

1. Bases for Claims and Relief[32]

The claims and requested relief vary. No federal statute specifically addresses the issue of non-consensual collection of personal consumer information on the Internet, except the Children's Online Privacy Protection Act of 1998 (COPPA), which prohibits collecting personal information of children under the age of thirteen.[33] Thus, plaintiffs have looked to analogous federal statutes enacted to protect consumer's privacy rights in electronic communications and in the collection of personal information by other

---

30. However, DoubleClick is not the only one. In November 2000, suits were filed against Avenue A and MatchLogic alleging trespass and violations of the Electronic Communication Privacy Act and the Computer Fraud and Abuse Act. *See* Evan Hansen, *Online Ad Companies Hit With Privacy Suits*, CNET NEWS.COM (Nov. 22, 2000) *at* news.cnet.com/news/0-1005-202-3821026.html.

31. Sandburg, *supra* note 17, at A1; *see also* Wang, *supra* note 16, at B3 (stating Doubleclick is the target of six class actions in California and New York with at least eight other class actions having been filed in those jurisdictions).

32. Several class actions against DoubleClick were consolidated in the United States District Court, Southern District of New York. *In re* DoubleClick Inc. Privacy Litig., No. 00 CIV 0641 NRB, 2001 WL 303744, at *1 (S.D.N.Y Mar. 29, 2001). The plaintiffs brought three claims under federal law: (1) Title II of the Electronic Communications Privacy Act, (2) the Wiretap Act and (3) the Computer Fraud and Abuse Act; and four claims under state law: (1) invasion of privacy, (2) unjust enrichment, (3) trespass to property and (4) violation of the New York General Business law. *Id.* The court dismissed the three federal claims with prejudice on summary judgment and declined to exercise supplemental jurisdiction over the remaining state law claims. *Id.* at *24-25. In summary, the federal claims failed primarily on statutory construction grounds and the court repeatedly found DoubleClick's actions fell within statutory exceptions or exemptions. *Id.* at *13, *18, *24. In its conclusion, the court also stated:

> The absence of evidence in the legislative . . . history of any of these Acts to suggest that Congress intended to prohibit conduct like DoubleClick's supports this conclusion. . . .
>
> . . .
>
> Although proposed legislation has no formal authoritative weight, it is evidence that Congress is aware of the conduct plaintiffs challenge and is sensitive to the privacy concerns it raises. Where Congress appears to have drawn the parameters of its regulation carefully and is actively engaged in the subject matter, we will not stray from its evident intent.

Id. at 24. As the court's ruling is only binding upon the class itself as to the federal claims, it certainly will be interesting to see whether other federal district courts will follow suit. It will be even more interesting to see whether Congress accepts the court's invitation to stand by or overturn its decision with legislation.

As the court found, the federal violations alleged are obviously less malleable to the contours of cookie litigation, but plaintiffs may fair better in state court. Meanwhile, DoubleClick may have its first victory, but the battle about cookies is far from over.

33. Andrew J. Frackman & Rebecca C. Martin, *Surfing the Wave of On-Line Privacy Litigation*, 223 N.Y.L.J., March 14, 2000, at 1, 7; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (West Supp. 2000).

industries, such as credit reports, cable TV, banking, video rentals, and student records.[34] None of these statutes, however, provide for a private right of action for individuals to sue and recover damages for their injuries.[35]

State statutes on the subject are also lacking. Although most states have adopted consumer protection laws that address certain deceptive and unfair trade practices and do provide a private cause of action, the majority of claims against companies using cookies or online profiling have arisen under traditional tort law.[36] These tort claims include trespass, invasion of privacy, public disclosure of private facts, and misappropriation of name or likeness.[37] Some complaints have even gone so far as to allege violations of state anti-stalking laws.[38]

C. EPIC Complaint

The EPIC complaint against DoubleClick, Inc. is one of the most publicized challenges of online profiling and cookie use. The EPIC filed a complaint on February 10, 2000 with the FTC, alleging DoubleClick had engaged "in unfair and deceptive trade practices by tracking the online activities of Internet users and combining that tracking data with detailed personally-identifiable information contained in a massive, national marketing database."[39] The complaint requests that the FTC initiate an investigation, order

---

34. Frackman & Martin, *supra* note 33, at 7 n.14. Such statutes include the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (1989) (governing individual bank records); the Fair Credit Reporting Act, 15 U.S.C. § 1681 (1998) (governing consumer credit reports); the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(c) (West Supp. 2000) (governing the accessing and obtaining of information from a computer used in interstate communication without authorization); the Electronic Communication Privacy Act, 18 U.S.C. §§ 2510-2520 (West Supp. 2000) (governing interception of telecommunications and placing restrictions on disclosure of e-mails and stored computer data); the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. § 2701 (West Supp. 2000) (governing disclosure of stored electronic communications); the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g) (West Supp. 2000) (governing student records); and the Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1991) (governing cable TV subscriber information). *See* Yang, *supra* note 25, at 15 (stating that "state and federal statutes exist to protect consumers from the unauthorized distribution of personal information including their bank records, video rental history, and private, personal facts"); *see also* Samborn, *supra* note 1, at 26 (citing the Electronic Communication Privacy Act and the Stored Wire and Electronic Communications and Transactional Records Access Act).

35. *See* Frackman & Martin, *supra* note 33, at 7.

36. *See id.*

37. *See id.*; Samborn, *supra* note 1, at 26.

38. Samborn, *supra* note 1, at 26. *See generally* Dick Kelsey, *Yahoo Accused Of Stalking*, NEWSBYTES (Jan. 28, 2000), *at* http:www.computeruser.com/news/00/01/28/news2.html (discussing Texas case where plaintiff alleged Yahoo violated state anti-stalking laws by tracking users via cookies).

39. Electronic Privacy Information Center, In the Matter of DoubleClick Inc., Complaint and Request for Injunction, Request for Investigation, and Other Relief, at 1 (February 10, 2000), *available at* http://www.epic.org/privacy/Internet/ftc/DCLK_complaint.pdf [hereinafter EPIC

DoubleClick to obtain express consent of any Internet user, and pay civil penalties and permanently enjoin DoubleClick from violating the FTC Act.[40] On January 22, 2001, the FTC sent a letter to DoubleClick's outside counsel announcing "it was ending its investigation with no finding that DoubleClick had engaged in unfair or deceptive trade practices."[41] The FTC found DoubleClick had never used or disclosed personal user information for purposes outside its privacy policy. DoubleClick had amended its privacy policy in mid-1999 by "removing its assurance that information gathered from users online would not be associated with their personally identifiable information."[42] Therefore, it was not surprising to find that the FTC cleared DoubleClick of privacy policy violation allegations, especially when DoubleClick had specifically tailored its policy to allow for online profiling.

D. Proposed Regulation by the Federal Trade Commission

The FTC has been studying online privacy issues and monitoring the data collection practices of Internet companies since 1995.[43] The FTC's authority over collection and dissemination of personal data stems from Section 5 of the Federal Trade Commission Act (FTC Act)[44] and COPPA.[45] In 1998 the FTC

Complaint]; *see generally* Press Release, Electronic Privacy Information Center, EPIC Files FTC Complaint Against DoubleClick, Alleges "Deceptive and Unfair Trade Practices" in Online Data Collection (Feb. 10, 2000), *available at* http://www.epic.org/privacy/Internet/FTC/DCLK_comp_pr.html (summarizing the catalyst for and substance of complaint).

40. EPIC Complaint, *supra* note 39, at 11.

41. Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, FTC, to Christine Varney, Esq., Hogan & Hartson, Outside Counsel for DoubleClick, January 21, 2001, *cited in In re DoubleClick Inc. Privacy Litig.*, No. 00 CIV 0641 NRB, 2001 WL 303744, at *6 (S.D.N.Y Mar. 29, 2001) (class action suit filed by people who had information about them accessed by DoubleClick or had DoubleClick cookies on their hard drives); *see also* Linda Harrison, *DoubleClick Beats Back Privacy Suits*, THE REGISTER, Mar. 3, 2001, *available at* www.theregister.co.uk/content/6/18020.html (stating investigation ended without finding of violation); Kieren McCarthy, *FTC Clears DoubleClick of Privacy Invasion*, THE REGISTER, Jan. 23, 2001, *available at* www.theregister.co.uk/content/6/16305.html (discussing dismissal of investigation and DoubleClick's reaction in an attempt to better public perception of company's attitude toward privacy).

42. *In re DoubleClick*, 2001WL 303744, at *5.

43. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, at *i (May 2000), *available at* http://www.ftc.gov/os/2000/05/index.htm#22 [hereinafter FTC MAY 2000 REPORT]; *see generally* Frackman & Martin, *supra* note 33, at 7 (stating FTC has been "at work on this matter since 1996" by referencing the 1998 report and the establishment of Advisory Committee); Terri J. Seligman & James D. Taylor, *FTC Reverses Privacy Policy*, N.Y.L.J., June 18, 2000, at S8 (discussing FTC policy and analyzing 2000 Report on Online Privacy).

44. 15 U.S.C. §§ 41 (West Supp. 2000).

45. 15 U.S.C. §§ 6501-6506 (West Supp. 2000). "'COPPA' governs the collection of information from children under the age of 13." 15 U.S.C. § 6501 (West Supp. 2000).

issued a report entitled *Privacy Online, A Report to Congress* (1998 Report),[46] which developed the "fair information practice principles."[47] These principles include notice, choice, access, security, and enforcement.[48] Previously, the FTC favored voluntary compliance and self-regulation, but it is now starting to re-evaluate its position.[49]

In February and March of 2000, the FTC surveyed ninety-one of the one-hundred busiest websites and found that ninety-nine percent collect personal information and one-hundred percent post some version of a privacy policy, but only forty-two percent implement the policy according to standards recommended by the 1998 Report.[50] In order to address these problems, the FTC convened an Advisory Committee on Online Access and Security.[51] The forty-member group was instructed "to provide advice and recommendations to the Commission regarding the implementation of the fair information practice principles."[52]

The FTC, in conjunction with the U.S. Department of Commerce, also held a public workshop about online profiling on November 8, 1999.[53] The goals of the workshop were "to educate government officials and the public about online profiling and its implications for consumer privacy, and to examine current profiling industry efforts to implement fair information practices."[54] At the workshop, Internet advertising members announced the formation of the Network Advertising Initiative (NAI).[55] The NAI is "comprised of the leading Internet Advertisers—24/7 Media, AdForce, AdKnowledge, Avenue A, Burst!

---

46. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (JUNE 1998), *available at* http://www.ftc.gov/reports/privacy3/index.htm [hereinafter FTC 1998 REPORT].

47. FTC MAY 2000 REPORT, *supra* note 43, at *i, 3-5; FTC 1998 REPORT, *supra* note 46, at 7-11.

48. FTC MAY 2000 REPORT, *supra* note 43, at *ii, 3-5; FTC 1998 REPORT, *supra* note 46, at 7-11.

49. Seligman & Taylor, *supra* note 43, at S8. The scope of this Comment does not encompass the probability of future FTC policy changes, with the entry of the Bush administration and confirmation of FTC Chairman nominee, Timothy J. Muris. This Comment is limited solely to the position taken by the FTC up to the time of the July 2000 Report. *See infra* note 53.

50. *See* FTC MAY 2000 REPORT, *supra* note 43, at *ii.

51. *See id.* at 6.

52. *Id.*; *see* FEDERAL TRADE COMMISSIONM, ADVISOR COMMITTEE ON ONLINE ACCESS AND SECURITY, FINAL REPORT (May 15, 2000), *available at* http://www.ftc.gov/acoas/papers/finalreport.htm.

53. *See* Press Release, Federal Trade Commission, FTC and Commerce Dept. To Hold Public Workshop on Online Profiling (Sept. 15, 1999), *available at* http://www.ftc.gov/opa/1999/9909/profiling.htm [hereinafter Workshop Press Release]; FTC JUNE 2000 REPORT, *supra* note 16, at 1.

54. Workshop Press Release, *supra* note 53; *see also* FTC JUNE 2000 REPORT, *supra* note 16, at 1.

55. FEDERAL TRADE COMMISSION, ONLINE PROFILING (PART 2): RECOMMENDATIONS 4 (July 2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf [hereinafter FTC JULY 2000 REPORT].

Media, DoubleClick, Engage and MatchLogic."[56] The FTC instructed the NAI to develop a framework of self-regulation for the online profiling industry, and, subsequently, the NAI submitted drafts of self-regulatory policy (NAI proposals) for the FTC and Department of Commerce to review.[57] In the interim, the FTC released its May 2000 Report, entitled *Privacy Online: Fair Information Practices in the Electronic Marketplace* in which the FTC recommended that Congress enact a basic level of privacy protection for all consumers.[58] The recommendation would require Internet companies to (1) comply with the FTC fair information practice principles, to the extent not covered by COPPA; (2) follow additional agency regulations; and (3) increase participation in self-regulation.[59]

In its subsequent June 2000 Report, the FTC addressed issues raised at the workshop including the current practice of online profiling by network advertisers, the benefits and concerns it presents for consumers, and the ongoing effort of the industry to develop self-regulatory principles.[60] While the FTC discussed the generalities of online profiling in the June 2000 Report, it refrained from making recommendations to Congress until it had the opportunity to consider the NAI proposals.[61] In a 4-1 vote, the FTC approved the NAI proposal and incorporated it into the May 2000 recommendation.[62] Thus, the ultimate recommendation changed little, except for an expansion of notice requirements[63] and the addition of a requirement that companies "not use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, or social security numbers for profiling."[64] Although the FTC applauded the NAI for adopting principles remarkably similar to the fair information practice guidelines, the FTC recommended that Congress enact legislation to guarantee full compliance by all websites.[65]

---

56. *Id.*

57. *See id.*; *see generally* NETWORK ADVERTISING INITIATIVE, NAI SELF-REGULATORY PRINCIPLES GOVERNING ONLINE PREFERENCE MARKETING (OPM), *at* http://www.networkadvertising.org/press/overview.shtml (last visited Sept. 17, 2000) (summarizing NAI Self-Regulatory Principles).

58. FTC MAY 2000 REPORT, *supra* note 43, at 36-38.

59. *See id.*

60. *See* FTC JUNE 2000 REPORT, *supra* note 16, at 1-2.

61. *See* FTC JULY 2000 REPORT, *supra* note 55, at 1.

62. *See* Chris Oakes, *FTC Endorses Privacy Rules*, WIRED NEWS (July 27, 2000), *available at* http://www.wired.com/news/print/0,1294.37853,00.html.

63. *See* FTC JULY 2000 REPORT, *supra* note 55, at 11, n.33.

64. *Id.* at 9 (footnote omitted).

65. *Id.* at 9-11; Press Release, Federal Trade Commission, Federal Trade Commission Issues Report on Online Profiling (July 27, 2000), *available at* http://www.ftc.gov/opa/2000/07/onlineprofiling.htm [hereinafter Online Profiling Press Release] ("NAI constitutes over 90% of the network advertising industry. Legislative action is necessary to ensure the remaining 10% will comply with the protections outlined in NAI's Principles and to guarantee full compliance by all web sites."). *Cf. supra* text accompanying note 50 (discussing compliance with recommended standards).

E. Proposed Legislation

Legislators have also joined in the mix, proposing bills to protect consumers' privacy and their rights against the non-consensual collection of personal information. On April 15, 1999, Montana Senator Conrad R. Burns proposed the *Online Privacy Protection Act of 1999*, which would require the FTC to promulgate regulations on Internet personal information collection not covered by COPPA.[66] On July 29, 1999, New York Representative Maurice D. Hinchey introduced the *Personal Data Privacy Act of 1999*, prohibiting federal, state, or local agencies and private entities from transferring, selling, or disclosing personal data without the express consent of the user.[67] On May 23, 2000, a few days after the FTC released its May 2000 Report,[68] South Carolina Senator Ernest F. Hollings proposed the *Consumer Privacy Protection Act*, which includes a title on "Online Privacy."[69] Each of these acts is currently being reviewed by various Senate and House Committees.

F. DoubleClick's Response to Lawsuits, Investigations, Proposed Regulation & Proposed Legislation

In the wake of the lawsuits, investigations, and proposed legislation, DoubleClick has taken several steps to appease public concerns.[70] Such steps include a major media education campaign and the creation of an internal privacy evaluation board.[71] DoubleClick created a website to educate consumers about privacy protection.[72] DoubleClick even added a section to its

---

66. S. 809, 106th Cong. (1999), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s809is.txt.pdf (last visited May 24, 2001); *see also* Frackman & Martin, *supra* note 33, at 7 (discussing bill's requirement for privacy disclosure and choice of "opt-out" mechanism).

67. H.R. 2644, 106th Cong. (1999), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:h2644ih.txt.pdf (last visited May 24, 2001); *see also* Frackman & Martin, *supra* note 33, at 7 (discussing bill's requirement for choice of "opt-in" provision).

68. Sandburg, *supra* note 17, at A1.

69. S. 2606, tit. I, 106th Cong. (1999), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s2606is.txt.pdf (last visited May 24, 2001).

70. *See* Chris Oakes, *DoubleClick Plan Falls Short*, WIRED NEWS (Feb. 14, 2000), *available at* http://www.wired.com/news/print/0,1294,34337,00.html.

71. *See id.*

72. The website is located at http://www.privacychoices.org. The website is divided into five sections: (1) About Online Advertising, (2) Understanding Your Rights, (3) Resource Center, (4) About DoubleClick, and (5) Opt Out. *See* DOUBLECLICK INC., PRIVACY CHOICES, *at* http://www.privacychoices.org (last visited Oct. 17, 2000). The section "About Online Advertising" discusses what constitutes online advertising, how consumers benefit, and how cookies work. *Id.* "Understanding Your Rights" establishes guidelines that will help users protect their privacy. *Id.* The section suggests that a user should read the website's privacy policy, check if the website has a third-party privacy seal, decide what information to disclose, not reveal any passwords, and use a secure browser. *Id.* The "Resource Center" provides links to governmental and organizational websites on privacy, third-party seal program websites, and privacy product

own website[73] that explains to consumers what cookies are, how to accept and/or decline them, and how to implement an opt-out provision.[74]

G. *Response to Privacy Concerns by Privacy Advocates & Technologies Firms*

Concerns about cookie abuse have caused privacy advocates to step to the forefront. The four key players have been the EPIC,[75] the Center for Democracy & Technology,[76] the World Wide Web Consortium,[77] and the Internet Engineering Task Force (IETF).[78]

Privacy concerns have also prompted innovative technologies firms to launch massive privacy campaigns. The market has boomed with various software programs dealing specifically with cookies.[79] While most of these

---

websites. *Id.* The "Opt Out" section explains what opting out means and how to do so. *Id.*

73. DOUBLECLICK INC., *at* http://www.doubleclick.net (last visited Oct. 17, 2000).

74. DOUBLECLICK INC., *at* http://www.doubleclick.net/us/corporate/privacy/default.asp (last visited Sept. 17, 2000).

75. The EPIC, the lead organization campaigning against DoubleClick's use of cookies and online profiling, is a public interest research center located in Washington, DC. ELECTRONIC PRIVACY INFORMATION CENTER, *at* http://www.epic.org (last visited Sept. 19, 2000). EPIC was "established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values." *Id.* Interestingly, the EPIC privacy policy directly states, "We do not enable cookies." ELECTRONIC PRIVACY INFORMATION CENTER, EPIC PRIVACY POLICY, *at* http://www.epic.org/epic/privacy_policy.html (last visited Sept. 19, 2000).

76. The Center for Democracy & Technology is a group "committed to helping users find ways to maximize their privacy online and still enjoy the Internet." CENTER FOR DEMOCRACY & TECHNOLOGY, *at* http://www.cdt.org/privacy/pet/ (last visited Sept. 17, 2000).

77. The World Wide Web Consortium (W3C), a group founded by major Internet companies, established the Platform for Privacy Preferences Project (P3P). WORLD WIDE WEB CONSORTIUM, PLATFORM FOR PRIVACY PREFERENCE PROJECT, *at* http://www.w3.org/P3P/ (last visited May 23, 2001). P3P is a "standardized set of multiple-choice questions, covering all the major aspects of a website's privacy policies . . . [and] present[s] a clear snapshot of how a site handles personal information about its users." *Id.*

78. The IETF is a "large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet." INTERNET ENGINEERING TASK FORCE, OVERVIEW OF THE IETF, *at* http://www.ietf.org/ overview.html (last visited Sept. 16, 2000). The IETF has proposed a way to track cookie deposits, so that companies such as DoubleClick could not deposit cookies on a users hard drive without the user's knowledge. Coale, *supra* note 18.

79. The following list includes some of the various software programs available, but the list is by no means exhaustive. Microsoft recently released an Internet Explorer privacy add-on, which allows the user to deal with cookies via their browser. *See MS Releases Privacy Patch*, WIRED NEWS (Sept. 1, 2000), *at* http://www.wired.com/news/print/0,1294,38578,00.html. Intracept, Inc., a Georgia corporation, has created X-Ray Vision, a program designed to prevent transmission or retrieval of cookies. *See* Chris Jones, *Shutting the Door on Cookies and Applets*, WIRED NEWS (Oct. 24, 1997), *available at* http://www.wired.com/news/print/0,1294,7975,00.html. The program enables the user to configure individualized privacy protection. *See id.* IDcide, a California firm, created Privacy Companion™, a free application that allows the user to "[s]ee when [she is] being watched on

programs are free or available at minimal cost to Internet users and downloadable from the firm's website, relatively few users are taking advantage of them.[80] This may be occurring for various reasons: (1) users may not be aware they even need these programs to protect their privacy; (2) users may not know where these programs are available; or (3) they may be overwhelmed by the complicity and variance of options, and thus are unable to determine really what their privacy needs are or which software will best accommodate them. Yet, others may see the limitations of the programs and decide not to use them. As websites have become privy to the new technologies protecting consumer privacy, website administrators have enabled their sites to include and exclude users based upon criteria, such as acceptance and declination of cookies and use of protection software.[81] For example, a user who has opted to decline all cookies may find the website will not open, or protection software may keep certain portions of the website from opening.[82] For some users, complete access to the Internet may mean they are willing to

---

the Net" and the ability to "[c]hoose [her] level of privacy protection" by deciding "how much personal information, if any, [she] want[s] to give away." IDCIDE, PRODUCTS, *at* http://www.idcide.com (last visited Sept. 17, 2000). Junkbusters, a consumer privacy firm, offers Internet Junkbuster Proxy™, a free software ridding personal computers of banner ads, cookies, and other "junk communications." *See* Junkbusters, *Internet Junkbusters Headlines*, *at* http://www.junkbusters.com (last visited Sept. 17, 2000). Mark Sweeney created CookieCop, an application which allows a user to accept or reject cookies by site. *See* Mark Sweeney, *Accept Cookies by Site*, PC MAG. (Feb. 29, 2000), *available at* http://www.zdnet.com/pcmag/sorties/solutions/0,8224,2430351,00.html. Privista, a group comprised of 2M Technology Ventures, Equifax, Vector Development, LLC, Warburg, Pincus Equity Partners, LP, and Masada Group Technologies, has created a website, www.privacychoices.com, dedicated to providing consumers with tools to protect a user's personal and credit information. Privista, *at* http://www.privacychoices.com (last visited Sept. 16, 2000). Other programs available for purchase include Privacy Software Corporation's NSClean (Privacy Software Corporation, *at* http://www.nsclean.com (last visited Sept. 17, 2000)), IDzap's Idsecure (IDzap, *at* http://www.idzap.com (last visited Sept. 17, 2000)), Anonymizer's Safe Cookies™, URL Encryption™, and Window Washer. (Anonymizer, *at* http://www.anonymizer.com/services/index.shtml (last visited Sept. 17, 2000)).

80. *See* Philip Hunter, *Spies On our Hard Drive*, COMPUTER WEEKLY (Sept. 30, 1999), *at* http://www.findarticles.com/cf_0/m0COW/1999_Sept_30/56706114/print.jhtml.

> The only way of tracing such agents is either by extreme vigilance or via background software that monitors all agent activities carefully. The latter is not widely installed at present and, although Web browsers present the option of flagging all cookies so that users can decide whether to let them in or not, in practice this feature is normally disabled.
>
> As cookies become increasingly prevalent, it becomes too time-consuming for users to inspect every one.

Id.

81. *See id.* ("[I]f cookies are automatically rejected, much of the functionality of many Web pages is lost."); McClure, *supra* note 12 ("[S]ome sites won't allow access to their pages without setting certain state cookies.").

82. *See* Hunter, *supra* note 80; McClure, *supra* note 12.

sacrifice the right to protect their privacy.[83] Therefore, for one reason or another, Internet users are slow to utilize options like protection software.

III. ANALYSIS

DoubleClick has become the target of widespread litigation.[84] Without any regulations in place, the courts face the daunting task of weeding through claims ranging from privacy torts to trespass to anti-stalking violations.[85] Current federal and state statutes provide little guidance, and traditional tort claims are being forced to conform to the contours of a legal area not yet fully developed.

A. Right to Privacy Background

In pursuing claims against cookie use and online profiling by companies like DoubleClick, individual consumers often allege an invasion of privacy. In determining an individual's right to privacy under tort principles, courts have relied primarily on state rather than federal law.[86] Each state has, at one time or another, been faced with deciding whether it will choose to recognize the right to privacy and to what extent that right will be applied. Cases determining that issue after 1965 generally begin their analysis with the consideration of two leading authorities.[87]

The first is a 1890 Harvard Law Review article written by the Honorable Louis D. Brandeis and Samuel D. Warren entitled *The Right to Privacy*.[88] Brandeis and Warren realized that societal change meant the recognition of new rights and that the common law must adapt to accommodate those needs, particularly the individual's right to be let alone.[89] They stated the common law

---

83. This user attitude is reflected by the fact that 33% of females and 41% of males always accept cookies. COOKIE POLICY SURVEY, *supra* note 4.

84. *See supra* note 30.

85. *See supra* notes 33-34.

86. The right to privacy provided for under federal law deals with limitations on governmental action rather than private actors. For example, the reasonable expectation of privacy guaranteed by the Fourth Amendment, which protects against unreasonable searches and seizures, extends only to government, not private actors. *See, e.g.*, Burdeau v. McDowell, 256 U.S. 465, 475 (1921) ("The Fourth Amendment . . . was not intended to be a limitation upon other than governmental agencies."). Therefore, in order to hold a private individual liable for invading another's privacy, the courts have mainly relied on the causes of action available under state tort law.

87. These two authorities are Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) and RESTATEMENT (SECOND) OF TORTS (1977). *See, e.g.*, Swinton Creek Nursery v. Edisto Farm Credit, ACA, 334 S.C. 469, 477, 514 S.E.2d 126, 130 (1999) (discussing the Brandeis & Warren article); Schulman v. Group W. Prod., Inc., 955 P.2d 469, 473, 477-78 (Cal. 1998) (discussing the Brandeis & Warren article).

88. Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

89. *Id.* at 193, 205.

already protected an individual's right to determine the scope of an individual's communication to others.[90] This protection took various forms in the law via doctrines resounding in contract and trust.[91] However, Brandeis and Warren understood the limited applicability of these doctrines:[92]

> The narrower doctrine may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.[93]

Brandeis and Warren used the advent of photographic technology as an example, showing that where an individual may have had to consciously sit for a picture previously, advances in technology now allowed for a picture to be taken surreptitiously.[94] Brandeis and Warren concluded that the principle protecting such invasions was the right to privacy, which encompassed six principles: (1) any publication of matter which is of public or general interest is not prohibited;[95] (2) "communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel" is not prohibited;[96] (3) there is no redress for the invasion of privacy by oral publication in the absence of special damage;[97] (4) publication of the facts by the individual or with her consent is not protected;[98] (5) truth is not a defense;[99] and (6) the absence of malice is not a defense.[100] Brandeis and Warren also recognized that an action of tort for damages applied in all cases, while an injunction may be applicable in a limited number of cases.[101]

---

90. *Id.* at 198-99.
91. *Id.* at 210-11.
92. *Id.*
93. *Id.*
94. Brandeis & Warren, *supra* note 88, at 211.
95. *Id.* at 214.
96. *Id.* at 216.
97. *Id.* at 217.
98. *Id.* at 218.
99. *Id.*
100. Brandeis & Warren, *supra* note 88, at 218.
101. *Id.* at 219.

The second authority is the *Restatement (Second) of Torts*,[102] based on Dean Prosser's article and his role as reporter,[103] which developed these principles into the four privacy torts.[104]

B. *Traditional Tort Claims*

1. *Privacy Torts*[105]

The traditional tort claims protecting privacy are public disclosure of private facts, false light, intrusion, and misappropriation of name or likeness.[106] Claims regarding online collection of private information, however, have relied mainly on public disclosure of private facts, intrusion, and misappropriation of name or likeness.[107] Jurisdictions vary in recognizing privacy torts; therefore, the first hurdle plaintiffs must overcome is whether their jurisdiction even recognizes such a cause of action.[108] For example, South Carolina recognized the right to privacy in *Holloman v. Life Ins. Co. of Virginia*[109] and later adopted three of the four categorical privacy tort invasions in *Meetze v. The Associated Press*,[110] but does not recognize the privacy tort of false light.[111] On the other

---

102. RESTATEMENT (SECOND) OF TORTS § 652A (1977).

103. *See* Swinton Creek Nursery v. Edisto Farm Credit, ACA, 334 S.C. 469, 477 n.9, 514 S.E.2d 126, 130 n.9 (S.C. 1999) ("In 1960, Dean Prosser expanded upon the Warren-Brandeis discourse by classifying invasion of privacy into four distinct causes of action. Prossers' classifications were incorporated into and elaborated upon in the Restatement." (citations omitted)); *see also* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 851, 854, 856, 863 (5th ed. 1984) [hereinafter PROSSER AND KEETON ON TORTS] (categorizing privacy torts as Public Disclosure of Private Fact, Intrusion, Misappropriation of Name or Likeness, and False Light).

104. *See Swinton Creek Nursery*, 334 S.C. at 477 n.9, 514 S.E.2d at 130 n.9; PROSSER AND KEETON ON TORTS, *supra* note 103, at 851, 854, 856, 863.

105. The existence and elements of privacy tort causes of action vary from state to state. First, a state may recognize the right to privacy, but may not necessarily recognize each of the four categorical invasions. Second, a state may adopt a version differing from the elements set forth in the *Restatement (Second) of Torts*. While acknowledging the uniqueness of each state's approach, this Comment is limited to an examination of the torts as proscribed under the *Restatement (Second) of Torts*, and will use South Carolina law and California law as examples of the potential variations.

106. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977); MARC A. FRANKLIN & ROBERT L. RABIN, TORT LAW AND ALTERNATIVES: CASES AND MATERIALS 1028 (6th ed. 1996); PROSSER AND KEETON ON TORTS, *supra* note 103, § 117.

107. *See* Frackman & Martin, *supra* note 33, at 7; Samborn, *supra* note 1, at 26.

108. *See, e.g.*, FRANKLIN & RABIN, *supra* note 106, at 1039 (stating public disclosure of private facts rejected in some states); *id.* at 1092 (stating appropriation has been recognized in most states).

109. 102 S.C. 454, 458, 7 S.E.2d 169, 171 (1940).

110. 230 S.C. 330, 335, 95 S.E.2d 606, 608 (1956); *see also* Swinton Creek Nursery v. Edisto Farm Credit, ACA, 334 S.C. 469, 478, 514 S.E.2d 126, 130 (1999) ("Later, in *Meetze v. Associated Press*, 230 S.C. 330, 95 S.E.2d 606 (1956), this Court specified three distinct causes of action for invasion of privacy: [1] the unwarranted appropriation . . . of one's personality, [2] the publicizing of one's private affairs . . . or [3] the wrongful intrusion into one's private

hand, California recognized the right to privacy in *Melvin v. Reid*,[112] and today it recognizes the four categorical privacy tort causes of action.[113]

a. Public Disclosure of Private Facts

The tort of public disclosure of private facts addresses true statements about an individual made to the public at large.[114] Under *Restatement (Second) of Torts* section 652D, an individual can recover for public disclosure of private facts when "[o]ne . . . gives publicity to a matter concerning the private life of another . . . if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[115]

Even if an individual is able to bring an action against a company like DoubleClick, Inc. for public disclosure of private facts in her jurisdiction, the case's outcome is uncertain. Using a fact-specific analysis, a court may find that a user's personal information is a private matter, disclosure of which would be highly offensive to the reasonable person and of no legitimate public concern.

The element which raises the most difficulty for the plaintiff will be the publicity requirement. The court will be faced with determining what constitutes a sufficiently large group: internal dissemination among affiliates and conglomerates, external disclosure to website clients using a web advertiser practicing online profiling, external disclosure of information by sale to other advertising companies, and whether disclosure of a user's specific identification or simply identification based upon behavior patterns from online profiling to one of these groups will constitute publicity. However, if the court determines that none of these scenarios adds up to a sufficiently large group, then the publicity element will most likely fail, leaving the user looking for alternative remedies to compensate for her injuries.

---

activities . . . .").

111. *See* Brown v. Pearson, 326 S.C. 409, 422, 483 S.E.2d 477, 484 (Ct. App. 1997).

112. 297 P. 91, 93 (Cal. D. Ct. App. 1931).

113. *See* Shulman v. Group W. Prods., Inc., 955 P.2d 469, 478 (Cal. 1998); KNB Enters. v. Matthews, 92 Cal. Rptr. 2d 713, 716-17 (Ct. App. 2000).

114. FRANKLIN & RABIN, *supra* note 106, at 1028.

115. RESTATEMENT (SECOND) OF TORTS § 652D (1977); PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 856-57. *Compare* Swinton Creek Nursery v. Edisto Farm Credit, ACA, 334 S.C. 469, 478, 514 S.E.2d 126, 131 (1999) (outlining elements of public disclosure of private facts as "(1) publicizing, (2) absent any waiver or privilege, (3) private matters in which the public has no legitimate concern, and (4) so as to bring shame or humiliation to a person of ordinary sensibilities") *with* Shulman v. Group W. Prods., Inc., 955 P.2d 469, 478 (Cal. 1998) (outlining elements of public disclosure of private fact as "(1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern").

(1) Private Matter

A matter is considered private if it is not readily available to the public or has not been voluntarily revealed to others by an individual.[116] Whether or not personal information revealed by cookies is private may depend on the type of information collected.[117] If websites only extract names, addresses, telephone numbers, or e-mail addresses from cookie data, this information would most likely be considered public, as it is usually available in telephone books or online informational directories. However, some individuals may have requested that such sources refrain from disclosing personal information.

In addition to collecting information, cookies also enable a website to profile consumer interests by tracking the user's movement within and among various sites.[118] A profile may contain data about the user accessing a pornographic website or a medical website. The user may consider this conduct to be private and thus prefer it to remain secret. This information would not be readily available to the public. Nor would the website have a basis to determine whether the individual has publicly revealed such behavior because a site can only track and monitor a user's behavior in cyberspace, not in real space. Therefore, under these circumstances, the information should be viewed as a private matter because the information is not readily available to the public and the individual has not voluntarily revealed the information to others.

It would be overly burdensome and extremely difficult for websites to differentiate between information intended to be willingly revealed by the

---

116. *See* PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 858-59.

117. It is important to differentiate between information that is considered private and information that is confidential. The privacy torts address information that an individual wishes to remain secret. There is no general duty to protect confidential information unless dictated otherwise by statute, regulation, or based upon the creation of a relationship. *See* F. PATRICK HUBBARD & ROBERT L. FELIX, THE SOUTH CAROLINA LAW OF TORTS 525-26 (2nd ed. 1997). In the context of this Comment, it is assumed that no confidential relationship exists, and therefore the analysis only addresses information the user wants to remain secret.

118. *See* Nickell, *supra* note 1. Nickell's article explains how companies like DoubleClick follow users between sites with cookie technology:

> A cookie served with a Web page can later be read by the same server, and an accumulation of clicks can thus be patched together . . . .
>
> For this to work, you need to have multiple check-in points along the user's clickstream throughout the Net, and since cookies can be accessed and read only by the server that created them, ad networks like those run by DoubleClick and Engage have found themselves in a convenient position of power. By serving ads for hundreds of advertisers on thousands of Web pages, ad networks become essential middlemen in building consumer profiles.

Id. The article also reports that an advertising company was able to track users across more than three thousand websites. *Id.*; *see also* McClure, *supra* note 12 (emphasizing that most people fail to realize cookies can track users over a long-term basis and among multiple websites); Roha, *supra* note 1 ("[User] learned that banner ads on sites in DoubleClick's ad network were leaving and reading cookies on her hard drive—even though she never clicked on the ads. The upshot: DoubleClick could track her visits to any site in its network.").

individual versus information intended to remain private. It is true the web company could differentiate between information the user has voluntarily revealed to the website such as log in information given by the user or the exercise of an opt-in procedure. However, the website would not necessarily be able to differentiate whether information it obtains through profiling has been previously voluntarily revealed to others. For example, a website collects data about a user accessing medical information; the website would have no basis to determine whether a user had publicly revealed or voluntarily disclosed information regarding the user's medical record in real space unless the user expressly volunteered such information to the website itself. Even for those users who want to utilize cookies, this line is difficult to distinguish, because privacy policy may vary significantly from person to person. For example, an individual may choose to disclose certain personal information to the website itself, but at the same time desire the information remain secure and undisclosed to third parties.

There is a strong policy argument for protecting the individuals who desire this information to remain private.[119] Therefore, unless the data collected by cookies is a matter of accessible public record, information not voluntarily disclosed by an individual should remain private and secret.[120]

Proponents of personal information collection may argue that users should be aware the Internet is a public arena, and thus, an individual has implicitly consented to such collection solely by accessing the website. This argument is countered by the user's perception of anonymity and consent and on general ideas of reasonableness.

First, many, if not most, consider the Internet a type of anonymous forum.[121] The user's identity is protected by screen names and IP addresses, providing users with the ability to access information, chat rooms, and websites with the security of a fictional identity.

---

119. Even over a century ago, Brandeis and Warren were in tune with these policies when they wrote:

> 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 .... Nor is the harm wrought by such invasions confined to the suffering of those who may be made the subjects of journalistic or other enterprise. In this, as in other branches of commerce, the supply creates the demand .... Even gossip apparently harmless, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people.

Brandeis & Warren, *supra* note 88, at 196.

120. In this context, "voluntarily" would mean information the user knows is already available to the public or information the user has willingly provided with consent for it to made public.

121. *See supra* text accompanying note 5.

Second, most users are completely oblivious to the deposit of cookies.[122] Few users understand what a cookie is, let alone the mechanics of its placement on their hard drive.[123] Thus, the deposit commonly occurs without the user's knowledge.[124] An individual can not be aware of, or consent to, an activity when they have no knowledge that it is occurring.

Third, even if the user should be aware or implicitly consents to personal information collection by accessing the website, it is unclear exactly what the user is authorizing. Is the user consenting to the deposit of the cookie and the collection of personal information? If so, does the consent include the collection of all personal information or only certain information? Are they also consenting to the dissemination or sale of that information?

The "should be aware" or "implicit consent argument" has no basis. Internet users, especially novices or intermediate users, are provided no foundation for such knowledge. There is a strong perception that the Internet is an anonymous medium.[125] It is true that a user's expectation of privacy must be reasonable, and it is important to keep in mind that a court may not always find the user's perception be found "reasonable." However, the nature of the Internet itself and its ability to provide an anonymous forum should be enough to support users' privacy expectations as reasonable, especially when users have never been provided information to the contrary. If the user does become aware that the Internet is not an anonymous forum, it most likely occurs after she becomes aware that her anonymity and privacy rights have been breached. By then, the injury has already occurred and does not dissipate the reasonableness of her expectation.

(2) Publicity

The publicity element of the tort of public disclosure is very different from publication.[126] Rather than the isolated disclosure that suffices for publication, the public disclosure tort requires widespread dissemination to a group.[127] This

122. *See supra* text accompanying notes 4-5.

123. *See supra* text accompanying notes 4-6.

124. *See id.*

125. *See generally supra* note 5 (providing basis for the preposition that most users believe the internet is an anonymous forum).

126. *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977); FRANKLIN & RABIN, *supra* note 106, at 1028; PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 856; *see also* Swinton Creek Nursery v. Edisto Farm Credit, ACA, 334 S.C. 469, 478-80, 514 S.E.2d 126, 131-32 (1999) (distinguishing publicity from "mere publication" as the difference between private—dissemination to single person or small group of persons—and public, which includes any publication in small circulation newspaper, handbills distributed to large number of persons, or any radio broadcast or statement in address to large audience); Rycroft v. Gaddy, 281 S.C. 119, 124, 314 S.E.2d 39, 43 (Ct. App. 1984) ("Communication to a single individual or to a small group of people, absent a breach of contract, trust, or other confidential relationship, will not give rise to liability." (citations omitted)).

127. *See supra* note 126.

element raises significant problems for the Internet user and requires line drawing. It would seem if a website collects personal information for its own use, then the publicity element would not be met. However, this is dependent upon the size and nature of the web company. Today, many web companies are expansive, comprised of subsidiaries, affiliates, and occasionally are members of conglomerates. For example, DoubleClick uses cookies to collect user information and preferences. Use of this information by DoubleClick internally may not meet the publicity requirement, but when the acquisition of Abacus Direct is taken into account,[128] the distribution is expanded. Under these circumstances, even the internal dissemination of the information may constitute publicity. The nature of the industry may also play a decisive factor. The internal use of information by DoubleClick, a web-advertising agency that primarily uses cookies for personal-information collection and online profiling, may have different publicity ramifications than the internal use of information by a website such as the Weather Channel, which only uses cookies to recognize a user's computer in order to facilitate a weather update on a user's homepage.

The publicity question certainly arises when the website collects information and either sells or distributes it externally to other companies. However, it is difficult to measure where widespread dissemination begins and ends. For example, if DoubleClick outright sells user data to a third party web advertiser, the publicity implications are clear, but the same logic may not apply when DoubleClick provides information to a website hosting a DoubleClick banner ad or paying for DoubleClick's online profiling services. The issue becomes even murkier depending upon the type of information DoubleClick is providing to such third parties. For example, the publicity issue may be applicable when DoubleClick provides personal information about the user, but it is not so clear whether disclosure of information based solely on behavioral patterns, without more, would constitute the requisite dissemination. Therefore, the courts are left to determine whether internal dissemination of information is considerable enough or of a sufficient nature to constitute publicity. Publicity requires the more difficult and higher standard of widespread dissemination, so this may be a difficult hurdle for the plaintiff to clear. However, if the company either outright sells or distributes information to other advertisers, the publicity element would probably be met because external, versus internal, publication would be sufficient to constitute widespread dissemination.

128. *See supra* Part II.A.

(3) Highly Offensive to the Reasonable Person

The offensiveness element requires that the disclosure of an individual's information be highly offensive to a reasonable person.[129] This element follows quite closely with the private matter argument discussed previously.[130] Although a reasonable user may not find collection and dissemination of her address highly offensive, the collection and dissemination of her sexual preference or private conduct very well could be. Therefore, the offensiveness element must be determined on a case-by-case basis.

(4) Legitimate Public Concern

The last element of the public disclosure of private facts cause of action requires that the disclosed information not be of legitimate public concern.[131] The website's collection and dissemination of a user's personal information has limited purposes, such as tailoring advertising to the individual or selling that information to other advertisers.[132] Therefore, it would be difficult to see how a user's personal information would qualify as a legitimate public concern.

Accessing a website should not strip a user of her rights to keep her personal information private because she is unaware that the web constitutes a public arena. By not understanding that implication, a user is not making an informed decision about releasing her right to keep her information private and behavior secret. Therefore, websites that choose to implement cookies and online profiling should carry the burden of explaining the terms and conditions of entering the site and allow users to choose whether they are willing to make their information public. At a minimum, websites should: (1) inform users that accessing the website equates entering a public arena, (2) explain to users specifically what data is being collected and for what purposes the data is collected, and (3) explain to what extent the information is being utilized. This may be as simple as website access triggering a hyperlink to a consent window containing boilerplate language regarding cookies and data profiling. This tactic is similar to security certifications used by websites to alert a user when they are entering or leaving a secured connection. Until such mechanisms are put into place and a user is aware that accessing the web has pierced the privacy veil, her personal information should remain completely private.

---

129. RESTATEMENT (SECOND) OF TORTS § 652D(a) (1977); FRANKLIN & RABIN, *supra* note 106, at 1028; PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 856-57.

130. *See supra* Part III.B.1.(a)(1).

131. RESTATEMENT (SECOND) OF TORTS § 652D(b) (1977); FRANKLIN & RABIN, *supra* note 106, at 1028; PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 857.

132. *See supra* note 12.

b. Intrusion

The tort of intrusion concerns the collection of information about, or from, an unwilling source.[133] *Restatement (Second) of Torts* section 652B states, "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."[134] There is no intrusion when the information is public or voluntarily revealed to others.[135]

The intrusion elements closely parallel the argument for the elements of public disclosure of private facts.[136] Neither personal information (name, address, telephone numbers, or e-mail address) nor user preferences (websites accessed) would be considered public, unless the information was a matter of public record or the website was able to determine that the user had already revealed the information to others voluntarily. Based on the policy of protecting individuals who desire to keep this information secret, the personal information should be classified as private.[137]

Similar arguments also apply for the offensiveness element.[138] Although users may not find collection and dissemination of their address highly offensive, the collection and dissemination of their sexual preference or private conduct very well could be. Therefore, the offensiveness element is fact specific.

---

133. *See* FRANKLIN & RABIN, *supra* note 106, at 1028.

134. RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see also* Nader v. General Motors Corp., 255 N.E.2d 765, 769 (N.Y. 1970) (requiring that the defendant's conduct be intrusive, the collected information be confidential, and the intrusion be highly offensive to a reasonable person). *Compare* Craig v. Andrew Aaron & Assoc., Inc., 947 F. Supp. 208, 213 (D.S.C. 1996) (outlining the elements of intrusion as (1) intrusion, which may consist of prying, besetting or other similar conduct; (2) into a private matter; (3) the intrusion was substantial and unreasonable; and (4) the defendants' conduct was intentional; and (5) when there has been no public disclosure of information, plaintiff must show blatant and shocking disregard of their rights and serious mental or physical injury or humiliation therefrom) *with* Shulman v. Group W. Prod., Inc., 955 P.2d 469, 490 (Cal. 1998) (outlining the elements of intrusion as "(1) intrusion into a private place, conversation or matter, [and] (2) in a manner highly offensive to a reasonable person").

135. *Nader*, 255 N.E.2d at 769; *see also* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) (stating there is no liability for examination of public record or of documents plaintiff makes available for public inspection, nor is there liability for observing him in a public place); PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 855 (stating plaintiff has no right to seclusion when in public).

136. *See supra* Part III.B.1.(a).

137. *See supra* text accompanying note 119.

138. *See supra* Parts III.B.1.(a)(1) & III.B.1.(a)(3). *But see* Sanhez-Scott v. Alza Pharm., 103 Cal. Rptr. 2d 410, 419 (Ct. App. 2001) (analyzing the offensiveness element of intrusion under the following factors: "(1) the degree of intrusion; (2) the context, conduct and circumstances surrounding the intrusion; (3) the intruder's motives and objectives; (4) the setting into which the intrusion occurs; and (5) the expectations of those whose privacy is invaded").

Where collection of personal information might fail to meet all the elements of public disclosure of private facts, the absence of the publicity requirement allows for recovery under intrusion. Therefore, a user would likely be able to recover for injuries sustained from an invasion of privacy via the tort of intrusion.

c. Misappropriation of Name or Likeness

The following elements of misappropriation were outlined in *White v. Samsung Electronics America, Inc.*:[139] "(1) the defendant's use of plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury."[140]

Misappropriation of name or likeness primarily deals with the right of publicity, a subset of the right of privacy.[141] Celebrities, who have a property interest in their identity and seek control over and compensation for the commercial exploitation of their name or likeness, have primarily invoked this tort.[142] However, some cases have stated that the misappropriation tort applies equally to non-famous plaintiffs.[143] Either way, an individual does not have an exclusive right to her name unless another uses it tortiously to exploit the user's

---

139. 971 F.2d 1395, 1397 (9th Cir. 1992).

140. *Id.*; *see also* RESTATEMENT (SECOND) OF TORTS § 652C (1977) ("One 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."); PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 851 (stating the appropriation of plaintiff's name or likeness for the defendant's benefit or advantage was first privacy invasion tort recognized by courts). *Compare* Snakenberg v. Hartford Cas. Ins. Co., 299 S.C. 164, 171, 383 S.E.2d 2, 5 (Ct. App. 1989) (outlining elements of appropriation as (1) intentional (2) unconsented (3) use of the plaintiff's name, likeness, or identity by the defendant (4) for her own benefit) *with* KNB Enter. v. Matthews, 92 Cal. Rptr. 2d 713, 717 (Ct. App. 2000) Section 3344, a commercial appropriation statute, states:

> Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent . . . shall be liable for any damages sustained by the person or persons injured as a result thereof.

Id.

141. *See* RESTATEMENT (SECOND) OF TORTS § 652C cmt. a, d (1977); FRANKLIN & RABIN, *supra* note 106, at 1092; PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 854.

142. *See* RESTATEMENT (SECOND) OF TORTS § 652C cmt. a, d (1977); FRANKLIN & RABIN, *supra* note 106, at 1092. Some commentators have argued that under misappropriation the protected interests should be divided into property rights and personal rights, such as dignity. *See* HUBBARD & FELIX, *supra* note 117, at 514, 519.

143. *See, e.g.*, KNB Enter. v. Matthews, 92 Cal. Rptr. 2d 713, 717 (Ct. App. 2000) ("Although the unauthorized appropriation of an obscure plaintiff's name . . . or likeness would not inflict as great an economic injury as would be suffered by a celebrity plaintiff, California's appropriation statute is not limited to celebrity plaintiffs."); HUBBARD & FELIX, *supra* note 117, at 518 ("[T]he interest protected includes intangible concern with the use of one's identity; and a plaintiff can recover for mental distress without any showing of pecuniary loss.").

identity for benefit.[144] The *Restatement* requires a commercial benefit, but it is not necessarily limited to a pecuniary one.[145] Because the website either uses the collected information internally or distributes it to others, the website has reaped a commercial benefit even in the context of the non-famous plaintiff. Therefore, although the website may not necessarily violate a user's property rights by simply collecting her name, once this information is combined to create a profile or identity of the user, the website may have invaded the exclusive property interest held by the user.

Under this framework, the collection and dissemination of a user's personal information constitutes misappropriation. Websites gather information using cookies in order to create an individual's profile.[146] Once the profile is complete, the website utilizes the user's identity to its advantage—it is either used to create individualized advertising or sold to other companies for profit.[147] The entire process usually occurs without the user's knowledge or consent.[148] Simply accessing a website does not constitute implicit consent to collect a user's personal and private information for purposes of online profiling.[149] Therefore, strictly analyzed under the elements, a user could have a cause of action for misappropriation.

d. Other Possible Tort Liability

Although privacy invasions incurred from online profiling have typically been alleged under the traditional privacy torts of public disclosure of private fact, intrusion, and misappropriation, another issue to be addressed is whether the websites are running afoul of other tort doctrines such as defamation and false light. With the use of cookies, websites are able to monitor clickstreams and determine personal tastes, interests, and preferences.[150] Some websites have employed the aid of anthropologists to study consumer behavior and to determine what cookie data is really telling them about the user.[151] Others have even employed programs to make educated inferences about profiles based on comparisons with other cookie data files.[152] However, such techniques may be

144. PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 852; *see also* RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1977) (stating interest protected is exclusive use of identity, as represented by name or likeness).

145. RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1977); PROSSER AND KEETON ON TORTS, *supra* note 103, § 117, at 853 n.39 (citing examples of alternative benefits as use to one's advantage, such as to influence or promote and posing as another individual).

146. *See supra* Part I.A.

147. *See supra* note 12.

148. *See supra* text accompanying notes 4 & 6.

149. *See supra* Part III.B.1.(a)(1).

150. *See supra* notes 1-3.

151. *See* Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 653-57 (2000).

152. *Id.* at 644 (quoting Peter McGrath, *Knowing You All Too Well*, NEWSWEEK, Mar.25, 1999).

flawed because websites may not be getting the full picture. This is especially true for sites that offer a variety of services.[153] The clickstream or information derived therefrom may not necessarily have any relation to that individual user's tastes, interests, or preferences, because the website is unable to discern the user's motivational purpose behind the clickstream. For example, the website is unable to determine whether the purpose is for business, research, or personal use, whether the user intentionally or mistakenly entered the site, or whether the user purchased an item for themselves or as a gift.

Another issue would be the use of a personal computer by a friend or family member or a personal computer shared between spouses.[154] The cookie data is able to identify the computer, but not necessarily the individual using it. Therefore, information data gathered while another person is accessing the Internet on a user's computer is not an accurate representation of the person's individual tastes, interests, or preferences, but again, the website has no way to distinguish who is using the computer at what time.[155]

At first, this argument only tends to prove the unreliability of cookie use, but the ramifications may extend further than that. If websites implement cookies techniques to profile users and create target advertising or, better yet, distribute those profiles to other companies, the website may be running afoul of other privacy violations, such as defamation or false light, and potentially incurring further liability.

2. *Trespass To Chattels*

An individual is liable for trespass to chattels[156] when the individual intentionally dispossess another of the chattel, the chattel is impaired, or the possessor is deprived of chattel use for a substantial amount of time.[157] Trespass to chattels debuted in telecommunications law in *Thrifty-Tel Inc. v. Bezenek*,[158] where a minor engaged in the unauthorized use of telephone services.[159] The court determined electronic signals generated by the child were sufficiently

153. *See* Tedeschi, *supra* note 13 (quoting interview with an Internet wine seller, who pointed out that "sites [catering] to a vast array of tastes, such as books or music . . . would have a more difficult time personalizing their merchandise" and stated that, as a result, "'[y]ou can get a bizarre set of recommendations from some of these book or music sites'").

154. *See* Roha, *supra* note 1. "[T]he information could be out of date or simply untrue because cookies are assigned to a computer, not a person. For example, if you share your computer with your teenage son, your surfing habits and his are lumped together." *Id.* This statement partially assumes no identifying information is given by each user via log-in names and passwords when they use the computer.

155. *See id.*

156. A chattel is defined as movable or transferable property. BLACK'S LAW DICTIONARY 229 (7th ed. 1999). Under this definition, a personal computer would qualify as a chattel.

157. *See* RESTATEMENT (SECOND) OF TORTS §§ 217, 218 (1977).

158. 54 Cal. Rptr. 2d 468, 471 (Ct. App. 1996).

159. *See id.*

tangible to support trespass to chattels.[160] The *Thrifty-Tel* line of reasoning was adopted in *CompuServe Inc. v. Cyber Promotions, Inc.*,[161] where the court held Cyber Promotion's transmission of "spam" (or junk e-mails) to CompuServe subscribers constituted actionable trespass to chattels.[162] The court found that even though CompuServe was not actually dispossessed of any chattel, a showing of interference which impaired the chattel's value to CompuServe was sufficient.[163] The court in *eBay, Inc. v. Bidder's Edge, Inc.* recently followed *Thrifty-Tel* when it found the electronic signals sent by Bidder's Edge to retrieve information from eBay's computer system were sufficiently tangible to support a trespass to chattels cause of action.[164] The court also found that Bidder's Edge's use of eBay's personal property deprived eBay from using its equipment's capacity for its own purposes, and the court held this was sufficient to establish impairment of value to the user.[165]

However, some commentators have argued that the analogy drawn by the *CompuServe* court, comparing "ephemeral" substances to electron signals, is misplaced.[166] Although the equipment has been contacted by electrons, it has not been touched, damaged, or rendered inoperable, and thus, the contact does not constitute a dispossession.[167] Electron signals (in the form of e-mails in *Compuserve*) are "precisely the type of communications the equipment was meant to process," and therefore, the court rationalizes "impairment by content"—impairment based solely on the fact the e-mails were unwanted.[168]

> [T]he essential elements of CompuServe trespass are readily found in almost any online activity; the cause of action might better be named "using a networked computer." The Internet operates by allowing users to exchange electrons, consume processing cycles, and occupy disc space on its constituent machines. Following the path laid out in CompuServe and Thrifty-Tel, it is quite possible to torture the doctrine of

160. *See id.* at 473 n.6.

161. 962 F. Supp. 1015, 1015 (S.D. Ohio 1997).

162. *See id.* at 1023.

163. *Id.* at 1022 ("To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.").

164. eBay, Inc. v. Bidder's Edge, Inc, 100 F. Supp.2d 1058, 1069 (N.D. Cal. 2000).

165. *See id.* at 1071 ("Even if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property.").

166. *See* Dan L. Burk, *The Trouble With Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 33-34 (2000).

167. *See id.* at 34.

168. *Id.* at 35, 37.

> trespass to chattels to cover any number of odious or inconvenient communications . . . .[169]

Although this is a compelling argument in the context of unwanted junk e-mails (or "spam"), the application of trespass to chattels to the use of Internet cookies goes beyond the line of reasoning used in *CompuServe*. While cookies cannot damage user files or read information on the hard drive,[170] the cookie initially dispossesses the user of hard drive space.[171] Under the *Restatement (Second)*, an action in trespass to chattels still lies even when the dispossession is brief, and there is no impairment to the chattel or any other interest of the possessor.[172] In this scenario, the transfer of electrons in the form of a cookie goes beyond simply "contacting" a user's computer. The website actually deposits an electronic numerical identifier in the form of a file in the user's hard drive,[173] thereby depriving the user of the ability to use that portion of their computer for their own purposes. Therefore, the mere placement of a cookie in a user's hard drive could constitute trespass to chattels by the depositing website.

In relation to the analysis of electronic trespass by "spam," cookies are distinguishable. "Spam" for all intents and purposes is a one-shot deal. When a user receives "spam," the user is notified, can open the e-mail, and can determine how to deal with it appropriately—most likely deleting it. Although the user may find "spam" a nuisance, it is no different than the hundreds of direct advertising brochures users receive in their real-space mailboxes.

Cookies, on the other hand, are a different story. Cookies are the electronic transfer of a numerical identifier file few users are privy to.[174] The cookie remains on the user's hard drive and essentially acts as a wiretap or tracking device, divulging information about the user without the user's knowledge each time she enters cyberspace.[175] While most users would agree e-mails may constitute "precisely the type of communications computers were meant to process," few would likely agree their computers were meant to provide websites with the opportunity to electronically collect personal information. However, even when a user does become aware of the cookie's existence and chooses to dispose of it, another is automatically placed on their hard drive

---

169. *Id.* at 47.

170. *See* DoubleClick, *at* http://www.privacychoices.org/content_cookies.htm (last visited Oct. 17, 2000).

171. *See* Samborn, *supra* note 1, at 26 (defining cookie as numerical identifier deposited onto a user's hard drive). If a cookie is deposited on a user's hard drive, then the cookie is occupying space that cannot be used by the user. Therefore, because the user can no longer use the space occupied by the cookie for his own purposes, the user has, in essence, been dispossessed of that hard drive space.

172. RESTATEMENT (SECOND) OF TORTS § 218 cmt. d (1977); PROSSER AND KEETON ON TORTS, *supra* note 103, § 13, at 67.

173. *See supra* note 1.

174. *See supra* text accompanying notes 4 & 6.

175. *See supra* text accompanying note 118.

upon the user's next website visit.[176] Therefore, cookies are a pseudo-permanent, continuous "touch." Cookies constitute trespass to chattel not simply because they are an "impairment by content"or a mere irritating "contact," but because they impair the user's ability to determine by whom, for what purpose and when her computer is taken or possessed by another for a third party's benefit, thereby depriving that user of the valuable resources of her computer.

C. Anti-Stalking Laws

Some allegations have gone past the traditional tort claims and alleged violations of state anti-stalking laws.[177] State anti-stalking statutes vary; some allow solely for criminal sanctions, while others allow for civil remedies.[178] Most statutes require the plaintiff to show the following elements: (1) the defendant engaged in conduct with the intent to follow, alarm, or harass the plaintiff; (2) the conduct resulted in the plaintiff's reasonable fear for her safety; and (3) the defendant continued to act after being definitely instructed to cease from such conduct.[179]

Websites deposit cookies with the intent to follow a user around the Internet in order to develop a profile on a user's preferences.[180] Therefore, the intent-to-follow element is fulfilled even though the conduct may not be alarming or harassing.

The use of cookies may even result in a user being in fear of her safety. Cookies, or the personal information they collect, have the capacity to be used inappropriately.[181] Divulgence of a user's personal information either to an employee or to a third party provides no guarantee private information will not seep its way into the hands of someone who could use the private information to cause harm. For a user who has attempted to keep her personal information private for various reasons, the possibility that this information could be extracted without the user's knowledge through the use of cookies and distributed to any number of people, could cause a user to be in fear of her safety. Also, as there is little information provided to users about who is placing cookies or when cookies are being placed on their computers, there is

176. *See* Cartwright, *supra* note 8 (explaining how to effectuate cookie technology, such as cookie placement, "fetch-cookie" commands, and the art of getting around browsers that "aren't playing the cookie game").

177. *See generally* Kelsey, *supra* note 38 (discussing a Texas case where plaintiff alleged Yahoo violated state anti-stalking laws by tracking users via cookies).

178. *See* FRANKLIN & RABIN, *supra* note 106, at 1083.

179. *See id.* (citing Calif. Civ. Code § 1708.7 (1998)).

180. *See supra* note 118.

181. *See* Hunter, *supra* note 80 (discussing quote by Wick Hill, director at Ian Kilpatrick, a distributor of agent technology, where Hill explains how easy it is to send someone a cookie via an e-mail, collect information about the user, and then retrieve the cookie without the user even being aware that the transaction took place).

little guidance for users to distinguish between a cookie placed by a website or by an independent third party.[182] Therefore, although cookies may not directly cause users to be in fear of their safety, cookie-type technologies combined with harmful behavior could lead to illegal conduct.

The third element of the anti-stalking claim will be the most difficult to establish. It is not likely that a user has instructed a website to cease from depositing cookies on her hard drive, after which the website continued such conduct. First, as noted above, most users are unaware they are being tracked by cookies. Second, a cease demand would have to occur electronically with an affirmative action by the user, such as disabling cookies via the web browser—an option most users are not only unaware exists, but also an option they do not know how to exercise.[183]

Anti-stalking laws may address the type of conduct incurred by the use of cookies and online profiling, but it will be difficult for the user to prove that the website continued to deposit cookies after being instructed to cease. Therefore, it appears that similar state anti-stalking statutes cannot fully protect Internet users from online profiling or cookies.

The lack of federal and state statutes adequately dealing with privacy issues arising from the collection of personal information on the Internet has forced plaintiffs to resort to these other areas of the law for relief. The traditional torts are not specifically suited to address these types of privacy issues. However, users are trying to force claims into the contours of the elements. The success or failure of these claims relies heavily on a case-by-case analysis of each fact pattern and the court's definition of element parameters. Of the aforementioned torts, the strongest arguments lie in recovery based on intrusion, misappropriation, and trespass.

D. Proposed Regulation by the Federal Trade Commission

Although courts have not yet provided the user with concrete rights to protect her privacy, government agencies such as the FTC seem to be moving toward increased regulation. Until now, the conduct of web companies has relied mainly on industry custom and individual corporate discretion.[184] In other words, the industry has been self-regulated.[185] However, in the wake of increased public concern and ensuing litigation, the FTC, in conjunction with the Department of Commerce, has started to consider proposing adequate

182. *See id.* ("The only way of tracing such agents is either by extreme vigilance or via background software that monitors all agent activities carefully. The latter is not widely installed at present and, although Web browsers present the option of flagging all cookies so that users can decide whether to let them in or not, in practice this feature is normally disabled.").

183. *See supra* text accompanying notes 4 & 6.

184. FTC MAY 2000 REPORT, *supra* note 43, at 6; Online Profiling Press Release, *supra* note 65; Seligman & Taylor, *supra* note 43, at S8.

185. FTC MAY 2000 REPORT, *supra* note 43, at 6; Online Profiling Press Release, *supra* note 65; Seligman & Taylor, *supra* note 43, at S8.

regulation.[186] In its July 2000 Report, the FTC recommended that Congress adopt the fair information practice principles as agreed upon by the FTC and the NAI.[187]

When Congress decides to legislate in this area, it will have several options to choose from. Not only has it received recommendations from both the FTC and NAI, but various legislators have also proposed a number of bills.[188] Based on the combined expertise of the FTC and NAI, it is likely Congress will defer to their recommendations.[189] However, the actual statutory construction remains in the hands of Congress. Once Congress determines the parameters of the substantive regulation, the driving question remains whether they will provide for a private cause of action.

If Congress chooses not to offer a private remedy, states may adopt their own statutes and provide private remedies themselves.[190] However, varying state statutes would make compliance by web companies virtually impossible because most websites can be accessed from any place at any time.[191] An extreme example would be if one state placed an outright ban on the use of cookies while another allowed for unlimited use of cookies. These circumstances would require web companies to determine from which state a user was accessing the website and adhere to state statutory requirements on an individual user basis. Such differential treatment raises fundamental constitutional issues, such as limitations imposed by the Commerce Clause and the Supremacy Clause.[192] If regulation is to be adopted, the best solution may be for Congress to regulate cookies and online profiling exclusively, in addition to providing for a private cause of action.[193]

---

186. FTC JUNE 2000 REPORT, *supra* note 16, at 1. *Cf. supra* note 49.

187. FTC JULY 2000 REPORT, *supra* note 55, at 9-11. *Cf. supra* note 49.

188. *See supra* Part II.E.

189. *See* Senator Ernest F. Hollings, *Internet Privacy*, S.C. LAW., Nov.-Dec. 2000, at 45, 45 ("This recommendation carries with it particular credibility in light of the FTC's record of extensive analysis on this issue and its prior recommendations to allow self-regulation a chance to work.").

190. *See id.* ("First off, we know that if Congress does not act, the states will."); *see also* Declan McCullagh, *Should States Regulate Privacy*, WIRED NEWS (Feb. 1, 2001), *at* http://www.wired.com/news/print/0,1294,41511,00.html (discussing argument by two George Mason University law professors that online privacy regulation would be better left to the states).

191. Although beyond the scope of this Comment, this issue also raises the question of international or off-shore online profiling and the associated problems should Congress choose to regulate the industry.

192. *See* U.S. CONST. art. 1, § 8, cl. 3; U.S. CONST. art. VI, cl. 2. Discussion of the possible violations of the Commerce Clause and Supremacy Clause in the context of differing state regulations is beyond the scope of this Comment.

193. Hollings, *supra* note 189, at 46 ("Our legislation [grants individual Internet users control over their personal information] by coupling a strong federal standard to protect individuals online with preemption of state Internet privacy laws to ensure business certainty. . . . [The industry] cannot obtain from a mishmash of inconsistent state Internet privacy laws.").

The escalation of Internet privacy concerns by individuals, privacy advocates, government agencies, and legislators has put pressure on Congress to adopt some form of regulation. The probability of such legislation being passed seems to be evidenced in part by Congress' previous interest in governmental control over personal information collection.[194] However, the FTC recommendation has actually received little fanfare outside of the Congressional Committees. The Clinton administration had looked at, but did not act on, the development of its own privacy regulation in the Financial Privacy and Consumer Protection Initiative, focused primarily on protecting privacy relating to financial and medical records.[195] Prospects look even more discouraging with the entry of the Bush administration.[196] Republicans have strongly opposed privacy regulation, including the two Republican Commission members who disagreed with the majority's proposal.[197] Therefore, the larger question remains unanswered: whether the new Congress will consider passing some form of privacy regulation or allow the industry to self-regulate and leave the determination of privacy infringements to the courts.

IV. CONCLUSION

DoubleClick's use of cookies and online profiling has been the subject of ongoing criticism. It is clear that the use of cookies raises fundamental privacy issues; the underlying question is how to deal with them efficiently. Internet advertisers want to continue using cookies to identify users and their preferences. Privacy advocates want to make sure users retain their right to privacy. The FTC and legislators have responded by proposing regulation of cookie use and online profiling. In the meantime, a number of lawsuits and complaints have been filed, and no one is really sure what the end result will be.

---

194. *See supra* note 34.

195. President Bill Clinton, Remarks By The President on Financial Privacy and Consumer Protection (May 4, 1999), *available at* www.epic.org/privacy/financial/clinton_remarks_5_99.html.

196. *See, e.g.*, John Gartner, *New Congress to Push Privacy*, WIRED NEWS (Jan. 7, 2001), *at* http://www.wired.com/news/print/0,1294,40965,00.html ("Though the 107th Congress is evenly split between two major parties and has the potential to act as a house divided, legislators are confident that they will pass a series of tech bills including one protecting individuals' privacy online."); Declan McCullagh & Ryan Sager, *Privacy Laws: Not Gonna Happen*, WIRED NEWS (Mar. 2, 2001), *at* http://www.wired.com/news/print/0,1294,42123,00.html ("Conventional wisdom in the nation's capital says that the prospect of Congress enacting Internet privacy laws is extraordinarily likely, and perhaps even inevitable."). *But cf. Bush Rejects EC Privacy Proposal* WIRED NEWS (Mar. 27, 2001), *at* http://www.wired.com/news/print/0,1294,42647,00.html (discussing the Bush administration's strong objection to proposed European Commission online privacy rules).

197. Stephen Labaton, *White House and Agency Split on Internet Privacy*, N.Y. TIMES (May 23, 2000), *available at* www.nytimes.com/library/tech/00/05/biztech/articles/23privacy.html.

Without any existing federal and state regulation already in place, the courts are being forced to analyze various claims and requested relief, most of which do not squarely address the invasion of privacy facilitated by a website's use of cookies and online profiling.

Internet companies have renewed their commitment to self-regulation, and the FTC has attempted to reinforce that commitment by combining self-regulation and government intervention. However, these changes provide little comfort to the everyday Internet user. Users will be better informed and have the option to affirmatively protect their privacy as they choose, but implementation of the proposed federal regulation will afford no relief to the user whose rights have been violated—unless the adopted regulation provides for a private cause of action.

The courts may decide traditional tort actions offer users an adequate remedy, but until either the cases are adjudicated or Congress passes legislation, Internet advertisers better enjoy their cookies while they can.

Jessica J. Thill

*