University of Dayton Law Review

Volume 29 | Number 1 Article 5

10-1-2003

Tony Soprano's Privacy Rights: Internet Cookies, Wiretapping Statutes, and Federal Computer Crimes after *In re DoubleClick*

Terry W. Posey Jr.
University of Dayton

TONY SOPRANO'S PRIVACY RIGHTS: INTERNET COOKIES, WIRETAPPING STATUTES, AND FEDERAL COMPUTER CRIMES AFTER *IN RE DOUBLECLICK*

Terry W. Posey, Jr.[*]

Log off – that cookies [stuff] makes me nervous.

- Tony Soprano[1]

I. INTRODUCTION

Tony Soprano, like every New Jersey made-man on HBO's *The Sopranos*, demonstrates a constant concern about eavesdropping, particularly from Federal agents. Could casual, unguarded web surfing provide the FBI with information helpful to finally prosecuting Tony under a RICO[2] statute? If Tony fails to maintain his cautious attitude, his Internet practices may be broadcasting more personal information than the bugged basement lamp.[3] The Internet cookie,[4] while enabling shopping, personalized web services, and almost every web-based email provider, also provides a methodology for tracking your Internet usage across various web sites. This information, while virtually useless in the context of a single web site,[5] provides a detailed picture of an individual's web surfing habits in the aggregate, including the potential of being tied back to an actual person's name and address.

The Internet and the World Wide Web have created new and exciting avenues for enhancements of research, shopping, and human interaction.

---

[*] Senior Executive Editor, 2003-04, University of Dayton Law Review; J.D. expected May 2004, University of Dayton School of Law; B.A. in Government, May 2001, University of Virginia.

[1] Tony Soprano to an associate browsing the Internet, *The Sopranos*, Episode 1, Season 3, HBO (TV Series).

[2] Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961-1968 (1994).

[3] In the third season premiere of *The Sopranos*, federal law enforcement agents succeed in placing a bugged lamp in Tony's basement. HBO, *HBO: Sopranos* http://www.hbo.com/sopranos/episode/season3/episode_27.shtml (accessed Apr. 2, 2003).

[4] A cookie (in the Internet sense) is "a small text file that the server writes to the user's hard disk without the user's knowledge or permission." Bryan Pfaffenberger, *Webster's New World Computer Dictionary* 92 (9th ed., Wiley Publishing 2001).

[5] *Id.* at 391.

These interactions have been driven by advances in both server[6] side and client[7] side technologies that allow for things such as personal shopping carts,[8] web sites delivering personal information, and the ability to login to view your bank or credit card information. While all of these technologies enhance online experiences, they also facilitate marketers and other corporations in accessing an individual's personal information.

With cookies and web bugs,[9] online marketing agencies are now able to compile significant amounts of personal data about your browsing habits, shopping preferences, and even your personal banking transactions. Even more frightening is the potential that exists to tie this information to the actual person, resulting in the removal of any personal privacy expectations on the Internet.

Lawsuits have been filed pursuant to the Stored Communications Act (under Title II of the Electronic Communications Privacy Act, "ECPA"),[10] the Federal Wiretap Act,[11] and the Computer Fraud and Abuse Act ("CFAA")[12] to hold liable those companies that would aggregate this data without the home Internet user's knowledge. In almost every case, courts rule against the Internet user in a motion for summary judgment or motion to dismiss. The preeminent decision on these issues remains *In re DoubleClick Privacy Litigation*.[13] This decision, which has been cited as persuasive authority by several other jurisdictions revisiting similar issues, is plagued with technological misunderstandings resulting in incorrect statutory interpretations.

This comment argues that web-monitoring actions violate provisions of the ECPA, the Wiretap Act, and the CFAA, and that the correct interpretation of these statutes would provide their intended protection: to

---

[6] An Internet server is "a program that supplies information when it receives external requests via Internet connections." *Id.* at 331.

[7] A client for Internet service is "a program that can communicate with a server . . . to exchange data of a certain type, such as a Web document or an e-mail message." *Id.* at 75.

[8] A "shopping cart" or "shopping basket" is "a method of implementing an online store in which users can select items and add them to a virtual shopping basket; when shopping is done, users then see all the items they have selected on an order page." *Id.* at 333. Shopping carts require cookies to function. *Id.* Amazon.com provides a thorough explanation of shopping carts and how they are used on their site in the help section of their web site. Amazon.com, *Amazon.com: Help / Ordering from Amazon.com / Using the Shopping Cart*, http://www.amazon.com/exec/obidos/tg/browse/-/468468/ (accessed Apr. 28, 2003).

[9] A "web bug" is a small graphic, invisible to the Internet user that is used to track information. Richard M. Smith, *FAQ: Web Bugs*, http://www.privacyfoundation.org/resources/webbug.asp (accessed Apr. 1, 2003).

[10] 18 U.S.C. §§ 2701-2710 (2000).

[11] *Id.* at §§ 2510-2520.

[12] *Id.* at § 1030.

[13] 154 F. Supp. 2d 497 (S.D.N.Y. Mar. 28, 2001).

safeguard against unauthorized access to communications. Section II of this comment provides a background of the Internet tools used to invade privacy as well as provisions of the Stored Communication Act, the Wiretap Act, and the CFAA. Further, section II provides a legal and factual background on recent cases tackling this issue. Section III of the comment is a critical analysis of the inaccurate interpretations of the courts that used *DoubleClick* as persuasive authority. Additionally, section III describes alternative suggestions for protecting online privacy so that, even in the absence of proper federal statutory protection, web surfers may continue to pursue appropriate methods of securing future privacy rights. Section IV consists of a warning regarding the difficulties in applying complex technical statutes to new or variant mediums by concluding that privacy rights do have a place on the Internet, as in the real world.

II. BACKGROUND

On the Internet, nobody knows you're a dog.

- Caption from 1993 *New Yorker* magazine cartoon[14]

This now-famous caption to a 1993 *New Yorker* cartoon emphasizes one of the great original principles of the Internet—that your online activities are conducted with the anonymizing intermediary of the computer and keyboard between others and yourself, be it corporations or individuals, who would seek access to identifiable information or your personal habits. However, with the advent of the World Wide Web and its interactive enabler, the cookie, it is no longer certain that the dog portrayed in the cartoon would not eventually reveal itself to be a canine. This section outlines the technologies that reduce any privacy expectation during Internet use. Further, this section details the seminal cases attacking the use of these technologies, as well as the Federal statutes under which redress is sought.

A. *Tracking You on the Internet*

There are several methods by which an enterprising online company or individual can seek to aggregate your personal data while you are surfing

[14] Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, Vol. 69 No. 20 New Yorker 61 (July 5, 1993).

the web. Some of these methods are necessarily intertwined with what is considered a "traditional" Internet experience, while others merely serve to record your data and surfing habits. This section provides a brief description of these data aggregating devices.

1. The Cookie

It is difficult to begin an academic discussion on the importance of the cookie to Internet privacy without first understanding exactly what a cookie is and how it is used. An Internet cookie is a file transmitted by a web site to an end user. It resides on the Internet user's computer and may contain a variety of information, including the user's Internet Protocol address ("IP address"),[15] any passwords needed to access the site, any selections or options the user has chosen to personalize his or her experience on the site, and the time and dates during which the individual site has been accessed by the user. All Internet cookies contain an expiration date, after which the web site ignores them as invalid.[16]

This myriad of descriptive features begs the question: what is an Internet cookie used for? An Internet cookie has an integral, but transparent role in casual web browsing.[17] One major role in which Internet cookies play a part is web site authentication.[18] Practically every site requiring a username and password uses a cookie to contain this information.[19] As briefly described above, cookies can be used to send personalized content to the web surfer.[20] This personalized content can be based on explicit preferences chosen by the user (i.e. personal zip code), or based on factors related to the Internet surfing (i.e. time spent at a site, date the site was last accessed, etc.).[21]

---

[15] An Internet Protocol address uniquely identifies every computer on the Internet. Pfaffenberger, *supra* n. 4, at 201.

[16] David Whalen, *The Unofficial Cookie FAQ*, http://www.cookiecentral.com/faq/ (last modified June 8, 2002).

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] For example, first time visitors to the MSNBC web site are greeted with a pop-up window requesting their zip code, so that personalized news and weather information may be provided. MSNBC, *MSNBC Cover*, http://msnbc.com (accessed May 1, 2003).

[21] Whalen, *supra* n. 16.

2. The Web Bug

A web bug is a tool used by a web site solely to obtain information about the visitors to the site. It exists in one of two forms: either a small image or a small program. As a small image, a web bug is sent to the web page being viewed in an extremely small size designed to be invisible to the web viewer. A user receiving such an image gives the web site several identifying characteristics, among which are the user's IP address and the time that particular web site was visited. A company that tracks web bugs across multiple web sites may be able to tell how long it takes you to get from site A to site B and that you visited both sites.[22]

A web site may also use a small program to affect a similar result, through either a Java applet[23] or JavaScript code.[24] Again, such a method provides no enhancement of service to the web site, yet it still allows the web site to receive your IP address and the time the site was accessed.[25] Additionally, it is possible in using one of these "program" methods to obtain referrer information[26] of *previous* sites the Internet surfer may have visited, regardless of the relationship to the current site.[27]

3. "GET" Submissions

"GET" submissions are one of the most common ways information may be unknowingly tracked on the Internet. This method of data collection involves harvesting data contained in a uniform resource locator ("URL").[28] While this method involves nothing more than retrieving

---

[22] Smith, *supra* n. 9.

[23] A Java applet is a small program designed to work across multiple operating systems on the Internet. Pfaffenberger, *supra* n. 4, at 205.

[24] Similar to a Java applet, JavaScript is code that executes when a web site is visited. *Id.* at 206.

[25] Smith, *supra* n. 9.

[26] Referrer information includes such data as the previous sites visited, and what links were followed. *See* Real Networks, *Privacy Policy > Referring URLs*, http://www.realnetworks.com/company/privacy/urls.html (accessed Sept. 30, 2003) (discussing the use of referrer information in the context of business use).

[27] Smith, *supra* n. 9.

[28] A URL, or uniform resource locator, specifically identifies the Internet location at which a web page or document can be found. Pfaffenberger, *supra* n. 4, at 378. An example of a "GET" submission is contained in the search for "Dayton Law Review" on Google: http://www.google.com/search?query=dayton+law+review. Any of the information past the question mark is text processed by the web server that is capable of being stored, analyzed, and compared to cookies, web bugs, or any other data collection mechanism. *See* Chuck Musiano & Bill Kennedy, *HTML, The Definitive Guide* 305 (2nd ed., O'Reilly 1997) (discussing the "GET" method as it may be used in web design); World Wide Web Consortium, *HTTP: The Get method*,

information already being sent over the Internet, it is again possible to correlate this information with other forms of data mining[29] as described in this section.

4. "POST" Submissions

"POST" submissions are the most common way a web site gains information about its visitors. "POST" submissions provide the most direct method of contact between a surfer and a web site. Whenever an Internet surfer fills out a form on a web page to register for a site or to provide information, this information is collected in what is called a "POST" submission. It is obvious the user knows (or should know) that such information is being transmitted, but such transmissions do raise privacy issues when the submitted data is correlated to other collected data without the user's knowledge.[30]

Like the other methods of collection listed, a "POST" form also records the surfer's IP address.[31] This, in turn, can be correlated with other data *not* associated with the transaction for which the user would be submitting information in a "POST" submission. For example, data contained in cookies or collected in web bugs on sites both of which are unrelated to the "POST" submission, can be tied back to the user who made such a submission through the use of data mining. It is in this way that an actual name or physical address can be tied to a person casually web surfing.

B. Milestone Cases for Web Privacy

In the several cases that have been brought against companies that use web-tracking tools without the knowledge or consent of the Internet surfer, all have been decided on a motion to dismiss or a summary judgment motion. This section discusses the facts and holdings of three of those cases: *In re DoubleClick Privacy Litigation*,[32] *In re Pharmatrak Privacy*

---

http://www.w3.org/Protocols/HTTP/Methods/Get.html (accessed Oct. 14, 2003) (discussing the "GET" method in extreme technological detail).

[29] "Data mining" seeks associations between a "variety of different and even mutually incompatible databases." Pfaffenberger, *supra* n. 4, at 103.

[30] Musiano & Kennedy, *supra* n. 28, at 305 (discussing the "POST" method as it is used in web design). *See also* World Wide Web Consortium, *HTTP: A protocol for networked information: The POST method*, http://www.w3.org/Protocols/HTTP/Methods/Post.html (accessed Oct. 14, 2003) (discussing the "POST" method in technological detail).

[31] An IP address is described in *supra* n. 15.

[32] 154 F. Supp. 2d 497.

Litigation,[33] and *In re Toys R Us Privacy Litigation*.[34] These cases involved civil claims utilizing the Stored Communications Act,[35] the Federal Wiretap Laws,[36] and the CFAA[37] in an attempt to penalize the companies in question for obtaining personal data without the consent of the Internet surfer.

1. DoubleClick, the Internet Advertising Giant

The plaintiffs in *DoubleClick* represented a class of Internet users of web sites that used DoubleClick's directed advertising service.[38] At the time the suit was filed, DoubleClick provided over 11,000 web sites with online advertising. DoubleClick utilized all of the techniques described in the previous section to collect information from Internet surfers. Indeed, such cookie information was necessary to receive a banner advertisement from DoubleClick. In addition to providing the advertising service, DoubleClick maintained an online bargains site and an email address directory. Both of these services allegedly required users to submit personal information in order to fully receive access.[39]

The suit was brought in the Southern and Eastern Districts of New York (prior to consolidation).[40] The suit alleged violations of the Stored Communications Act,[41] the Federal Wiretap Act,[42] and the CFAA.[43] DoubleClick successfully brought a motion to dismiss the action pursuant to the Federal Rule of Civil Procedure 12(b)(6).[44]

---

[33] 220 F. Supp. 2d 4 (D. Me. Aug. 13, 2002).

[34] 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001).

[35] 18 U.S.C. §§ 2701-2710.

[36] *Id.* at §§ 2510-2521.

[37] *Id.* at § 1030.

[38] DoubleClick directed advertising service enables web publishers to display ads according to "key audience segments." DoubleClick, Inc., *Features & Benefits*, http://www.doubleclick.com/us/solutions/publishers/online/dartenterprise/features.asp (accessed Apr. 1, 2003).

[39] *In re DoubleClick*, 154 F. Supp. 2d at 502.

[40] *Id.* at 500.

[41] 18 U.S.C. §§ 2701-2710.

[42] *Id.* at §§ 2510-2521.

[43] *Id.* at § 1030. The suit also alleged state law claims, which the District Court declined to maintain jurisdiction over after dismissing the Federal statutory claims.

[44] Federal Rule 12(b)(6) provides that a motion to dismiss may be made for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6) (2000).

a. The Stored Communications Act Claims

The Stored Communications Act was enacted to prevent hackers from obtaining, altering, or destroying certain stored electronic communications.[45] The statute prescribes civil and criminal penalties for:

> Except as provided in subsection (c) of this section whoever--
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.[46]

The plaintiffs in *DoubleClick* argued that the placement of a cookie on the Internet surfer's hard drive constituted unauthorized access pursuant to this provision.[47] However, DoubleClick rebutted that its conduct was authorized pursuant to the statutory exception contained in § 2701 (c):

> (c) Exceptions. Subsection (a) of this section does not apply with respect to conduct authorized--
>
> (1) by the person or entity providing a wire or electronic communications service;
>
> (2) by a user of that service with respect to a communication of or intended for that user; or
>
> (3) in section 2703, 2704 or 2518 of this title.[48]

The court indicated that the question of whether DoubleClick's conduct was authorized under the statutory exception was a three part question:

> (1) what is the relevant electronic communications service?; (2) were DoubleClick-affiliated Web sites "users" of this service?; and (3) did the DoubleClick-affiliated Web sites give DoubleClick

---

[45] *In re DoubleClick*, 154 F. Supp. 2d at 527.

[46] 18 U.S.C. § 2701(a).

[47] 154 F. Supp. 2d at 507.

[48] 18 U.S.C. § 2701(c).

sufficient authorization to access plaintiffs' stored communications "intended for" those Web sites?[49]

The court first determined that the "relevant electronic communications service" was the individual Internet Service Provider ("ISP"),[50] and not the greater Internet itself.[51] The court then addressed the issue of who the "user" was for the purposes of the Stored Communications Act.[52] The definitions portion of the Stored Communications Act, 18 U.S.C. § 2510, defines a user as: "any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." The court held that the "user[s]", pursuant to §2701, were the web sites that requested to use DoubleClick's service.[53] The plaintiffs argued that the most natural reading of "user" was that the Internet surfer, not the web site, was the user. Despite the plaintiffs' protests to the contrary, the court held that their assertion was erroneous, as web sites and commercial users also use Internet access in the same manner, which fails to distinguish class members from these alternative users.[54]

The court also rejected the plaintiffs' secondary argument that because "basic property and privacy notions" require that only an individual Internet surfer can authorize access to his or her computer, then that person must be the user intended by the statute. The court rejected this argument as being incongruous with the statutory exceptions embodied in § 2701(c).[55]

However, the court seemed to entertain this argument again when it raised the argument that humans *are* the "user[s]" pursuant to § 2510 and § 2701. Ultimately, the court rejected this, stating "no direct connection ever exists between the human user and the Web site."[56] The court described the features and requirements of Internet engineering by concluding that web sites are "users" because their existence and utility depend on Internet access.[57]

---

[49] *In re DoubleClick*, 154 F. Supp. 2d at 508.

[50] More commonly referred to as an ISP, this is the direct service by which one obtains Internet access. Technically, an ISP is the company that provides Internet accounts to individuals and businesses. Pfaffenberger, *supra* n. 4, at 203.

[51] *In re DoubleClick*, 154 F. Supp. 2d at 508.

[52] *Id.* at 508-09.

[53] *Id.*

[54] *Id.* at 509.

[55] *Id.*

[56] *Id.*

[57] *Id.*

The court, having resolved the first two questions in favor of DoubleClick, had no difficulty in coming to the conclusion that, as purported by the statutory exception under § 2701(c), the DoubleClick-affiliated web sites "authorized" the conduct, thereby removing DoubleClick from liability pursuant to § 2701(a).[58] The court first concluded that the "GET," "POST" and web bug methods of data collection, as generated by the Internet surfer's mouse click requests, were "intended for" the DoubleClick-affiliate. Thus, the methods were approved by the affiliate and found to be within the scope of § 2701(c)(2). Ultimately, this meant that no liability attaches.[59] The court held that cookies were similarly outside of the scope of the Stored Communications Act's protection, because "they are not in 'electronic storage' [pursuant to § 2701(a)] and, even if they were, DoubleClick is authorized to access its own communications."[60] Given that all three of the necessary determinants of a statutory exception were found to be in DoubleClick's favor, the court held that the Stored Communications Act claims were barred.[61]

b. The Wiretap Act Claims

The Wiretap Act provides a civil claim of action against anyone who: "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication [except as provided in the statute]."[62] DoubleClick admitted that, as pled, its conduct violates this statute.[63] However, it contended that it was again saved by the statutory exception in 18 U.S.C. § 2511(2)(d):

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

---

[58] *Id.* at 511.
[59] *Id.*
[60] *Id.* at 513-14.
[61] *Id.*
[62] 18 U.S.C. § 2511(a).
[63] *In re DoubleClick*, 154 F. Supp. 2d at 514.

any State.[64]

The court returned to its Stored Communications Act analysis of "consent" because the same definitional statute as before governed the term.[65] The court found that DoubleClick's interceptions were with the "prior consent" of the affiliated web site and, as such, permitted by the statute. [66]

The only issue then to be addressed was whether the communication was "intercepted for the purpose of committing any criminal or tortious act."[67] The court held that such an analysis hinged on the plaintiffs' allegation that "either (1) that the primary motivation, or (2) that a determinative factor in the actor's [DoubleClick's] motivation for intercepting the conversation was to commit a criminal [or] tortious . . . act."[68] The court distinguished the plaintiffs' allegations that DoubleClick had been committing torts from DoubleClick's *intent* to commit a tort. The court reasoned that intent was not present because the technologies used were patented and publicized. Consequently, the court held that DoubleClick lacked the necessary intent or purpose to be in violation of the statutory exclusion.[69]

c. The CFAA Claims

The CFAA creates both a criminal[70] and a civil[71] action for the unauthorized use of computers.[72] The civil action provides compensatory and punitive damages for any person who suffers a loss due to a violation of the entire section.[73] The damages are limited, however, by § 1030(e)(8): "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information" that causes loss aggregating at

---

[64] 18 U.S.C. § 2511(2)(d).

[65] *In re DoubleClick*, 154 F. Supp. 2d at 514.

[66] *Id.*

[67] 18 U.S.C. § 2511(2)(d).

[68] *In re DoubleClick*, 154 F. Supp. 2d at 514-15 (ellipses in original) (quoting *United States v. Dale*, 991 F.2d 819, 841-42 (D.C. Cir. 1993)).

[69] *In re DoubleClick*, 154 F. Supp. 2d at 519.

[70] 18 U.S.C. § 1030 states "(a) [w]hoever . . . (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains- . . .(C) information from any protected computer if the conduct involved an interstate or foreign communication . . . shall be punished as provided in subsection (c) of this section."

[71] *Id.* at § 1030(g).

[72] *Id.* at § 1030.

[73] *Id.*

least $5,000 in value during any 1-year period to one or more individuals."[74]

DoubleClick did not contest that the plaintiffs' computers were "protected" under the CFAA or that its access was unauthorized. It did contest the plaintiffs' ability to allege damage aggregating a value of at least a value of $5,000. The plaintiffs *did* argue that the $5,000 requirement could be aggregated across the class of plaintiffs and across DoubleClick's actions for the year. The court negated this by concluding that "any impairment" as described in § 1030(e)(8) required that a single incident be responsible for the loss on a single computer. Thus, the plaintiffs could not meet the $5,000 damages requirement to maintain a CFAA claim.[75]

2. *In re Pharmatrak*[76] – Is Your Medical Information Discoverable Online?

In re Pharmatrak Privacy Litigation was a suit brought by six plaintiffs against Pharmatrak, Inc. as well as several pharmaceutical companies. The pharmaceutical companies in the suit hired Pharmatrak to track and analyze personal use of their individual drug and pharmaceutical web sites (which were designed for consumers). The plaintiffs alleged that the data collected by Pharmatrak, while the plaintiffs were visiting web sites devoted to medical issues and treatment, created serious privacy concerns that were remediable under Federal and state law. Again, like the *DoubleClick* plaintiffs, the plaintiffs in *Pharmatrak* alleged a violation of the Stored Communications Act, the Wiretap Act, and the CFAA. Procedurally, however, these claims were addressed in a motion for summary judgment.[77]

a. The Stored Communications Act Claims

The *Pharmatrak* decision relied heavily on *In re DoubleClick*, but did make a few noteworthy distinctions. First, the *Pharmatrak* defendants argued, and the court agreed, that the plaintiffs' personal computers were not a "facility through which an electronic communication service is provided."[78] The court compared a computer with Internet access as being like a telephone used for its traditional purposes or a television connected

[74] *Id.* at § 1030(e).
[75] *In re DoubleClick*, 154 F. Supp. 2d at 526.
[76] 220 F. Supp. 2d 4.
[77] *Id.*
[78] 18 U.S.C. § 2701.

to cable service, in that it is not a "facility" but a "device."[79]

The court in *Pharmatrak* went on to adopt, part and parcel, the rest of the conclusory Stored Communications Act holdings in *DoubleClick*. First, the court held that cookies did not exist as "temporary electronic storage" since cookies were not an intermediary portion of an electronic transmission. Further, the court held that even if the cookies were in such storage, Pharmatrak was authorized by the pharmaceutical defendants who contracted for Pharmatrak's services. Thus, the court ruled in favor of the defendants on the Stored Communications Act claims.[80]

b. The Wiretap Act Claims

The court in *Pharmatrak* made many of the same findings as the *DoubleClick* court in ruling in the defendants' favor on the summary judgment motion. First, the court adopted the "authorized user" interpretation of the Stored Communications Act to determine that the statutory exception barred a Wiretap Act claim. Further, the court held that Pharmatrak lacked the mens rea necessary to overcome the statutory exception's protection (that is, that the determinative factor or purpose for Pharmatrak's actions was not to commit a tortious or criminal act).[81]

c. The CFAA Claims

The court again became enmeshed in the statutory exceptions as provided and interpreted in *DoubleClick*. The *Pharmatrak* court held that the plaintiffs could not meet the $5,000 requirement for civil recovery under the CFAA. In a minor distinction, the court held that damages could be aggregated between plaintiffs and computers, but only those damages resulting from a single incident. As such, the plaintiffs' allegations were insufficient to maintain a complaint, and the court again ruled in favor of the defendants on the summary judgment motion. Having decided all of the federal claims in favor of the defendants, the court declined to exercise supplemental jurisdiction over the remaining state claims, which were then dismissed.[82]

---

[79] *In re Pharmatrak*, 220 F. Supp. 2d at 14.
[80] *Id.*
[81] *Id.*
[82] *Id.* at 15.

3. *In Re Toys R Us*[83] – They *Know* You Want to Be a Toys R Us Kid

The 2001 decision in *In re Toys R Us Privacy Litigation*, involved similar parties to those of *DoubleClick* and *Pharmatrak*.[84] Toys R Us, operator of retail toy stores, began an online counterpart to their retail stores.[85] The Toys R Us web site utilized web tracking services from a co-defendant, Coremetric.[86] Coremetric utilized cookies, web bugs, "GET" submissions, and "POST" submissions[87] to correlate Toys R Us customer data with data from other web sites using similar Coremetrics tools.[88] The plaintiffs in the complaint again brought suit under the Stored Communications Act, the Wiretap Act, and the CFAA.[89]

a. The Stored Communications Act Claims

Contrary to *Pharmatrak*, but citing *DoubleClick*, the court held that personal computers used by Internet surfers were "facilities" for the purposes of 18 U.S.C. § 2701. The court rejected the argument made by Toys R Us, but held that at the time, no cases existed to support that opinion. The court went on to state that the issue requiring resolution was whether the Coremetrics's cookies were placed in "electronic storage."[90]

The court in *Toys R Us* adopted wholeheartedly the *DoubleClick* discussion in coming to the conclusion that cookies on a hard drive are not in "electronic storage," and thus, not protected by § 2701. However, the plaintiffs contended that the storage of the cookie in a computer's RAM[91] prior to its storage on the hard drive created the "temporary electronic storage" sufficient to create a § 2701 claim. The court rejected this argument, as first not being in the complaint, and second, because Coremetrics's access of the cookie occurred when it was on the hard drive. Having made this determination, the court held that the plaintiffs failed to plead a necessary element of the Stored Communications Act claim.[92]

---

[83] 2001 U.S. Dist. LEXIS 16947.

[84] *In re DoubleClick*, 154 F. Supp. 2d at 497; *In re Pharmatrak*, 220 F. Supp. 2d at 4.

[85] *In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947 at *3.

[86] *Id.*

[87] As discussed *supra* in section II(A).

[88] *In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947 at *3.

[89] *Id.* at *5.

[90] *Id.* at *8.

[91] Random Access Memory, is a temporary holding place for data, "in which program instructions and data are stored so they can be accessed directly by the [CPU]." Pfaffenberger, *supra* n. 4, at 309.

[92] *In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947 at *14.

The court went on to state that, even in the absence of the necessary pleading, Coremetrics's actions fell under the statutory exception in § 2701(c)(3). It determined that "consent" was obtained for the access, premised on the *DoubleClick* analysis of the actual web site being considered the user authorizing the connection.[93]

b. The Wiretap Act Claims

The court again adopted the *DoubleClick* court's determination of consent in holding that the Wiretap Act exclusions for interception with consent applied in this case. It then had to address whether or not Coremetrics had the "criminal or tortious" intent necessary to void the exclusion. In dismissing the claim, the court held that, like in *DoubleClick*, no evidence or pleading addressed Coremetrics's intent in using the web tracking tools.[94]

c. The CFAA Claims

As with the previously mentioned cases, the issue again became whether or not the plaintiffs had alleged a sufficient amount of damages ($5,000) to seek recovery under 18 U.S.C. § 1030(g). The court in *Toys R Us*, again branching away from *DoubleClick*, held that the allegations, of placing cookies on multiple hard drives, could be aggregated. Further the court stated that the plaintiffs had sufficiently pled an amount exceeding $5,000. Therefore, the claim was not dismissible and was ripe for litigation.[95]

III. ANALYSIS

Imagine that the following is an introduction to the fifth season of *The Sopranos*. Tony awakens, and in his traditional boxer shorts, tank top, robe, and slippers, pads over to the computer to do some morning Internet surfing. While waiting for his coffee to percolate, he first checks his stock prices.[96] Then, he surfs to read about the side effects of the latest

[93] *Id.* at *18.

[94] *Id.* at *27.

[95] *Id.* at *36.

[96] Presumably not the phony stock Tony had Christopher selling to senior citizens in the Season 2 premiere. HBO, *HBO: Sopranos*, http://www.hbo.com/sopranos/episode/season2/episode_14.shtml (accessed Apr. 1, 2003).

psychiatric medicines he's been prescribed by Dr. Melfi.[97] He then checks the daily newspapers of northern New Jersey to make sure his name has not been mentioned. Before signing off, he orders his son A.J. some football equipment.

The preceding all seems relatively innocuous, but in reality, if the web sites Tony was surfing used any or all of the Internet marketing/tracking firms described in the previous section, a substantial amount of information could be gained and correlated. First, Tony's IP address was logged at every site (meaning he could be tracked across each site, since the IP address is usually unmaskable and continuous). Second, his browsing habits (including the stocks he was interested in, and the drugs about which he requested information) could be aggregated by his IP address. Moreover, the time he spent at each web site, and whether or not he moved on to other web sites by direct links or by bookmarks, could be correlated. If all of the sites he surfed used the same web tracking firm, the information provided to secure his final sporting goods purchase would identify Tony by name and address. All of this gives Tony's quote from the Season Three premiere, "Log off – that cookies [stuff] makes me nervous,"[98] a little more meaning.

Primarily due to statutory exclusions, courts dealing with privacy issues created by web tracking companies have consistently found the Federal statutes in question, the Stored Communications Act, the Wiretap Act, and the CFAA, inadequate to address such claims.[99] However, all of these rulings are plagued with technical misunderstandings and incorrect statutory interpretations. Instead, the statutes in question *should* provide a redress for the privacy issues created by the use of cookies, web bugs, and other tracking mechanisms. This section describes in detail how the statutory exclusions claimed by the Internet tracking companies fail to provide a roadblock for the average Internet user seeking relief. Further, in light of the various court decisions holding otherwise, this comment discusses alternatives to protect the privacy of casual users on the Internet, be it through alternative legal action, Federal regulations, or personal cautiousness.

The Internet has enabled the digital future, where new access to information, shopping, and interaction is placed in the hands of those who fail to realize the ramifications or exposure of their activities. An important consideration in advancing the Internet and the potential it promises is

---

[97] Dr. Melfi is Tony Soprano's psychiatrist. At one time, Tony was taking both Prozac and Lithium to handle his ups and downs. HBO, *HBO: Sopranos*, http://www.hbo.com/sopranos/episode/season1/episode_12.shtml (accessed Apr. 1, 2003).

[98] *The Sopranos*, Episode 1, Season 3, HBO (TV series).

[99] As discussed *supra* in section II(B).

ensuring that those with greater technical expertise do not abuse this naiveté.

A. *The Stored Communications Act*

The Stored Communications Act (under Title II of the ECPA) provides a cause of action for any individual or entity who accesses a "facility through which an electronic communication service is provided," or who "exceeds an authorization to access the facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."[100] Courts have raised two issues when considering Stored Communications Act claims based on Internet monitoring: (a) whether or not an Internet surfer's computer is a "facility" pursuant to the statute, and (b) whether or not the cookie is in "electronic storage" while it resides on the surfer's computer.[101]

1. The Computer as a "Facility"

The court in *Pharmatrak* contended that an Internet user's computer could not be a "facility" as required by § 2701(a) because it was merely a device through which an electronic service was accessed, like a telephone or cable-ready television.[102] The *DoubleClick* court did not directly address this issue. However, the *Toys R Us* court held exactly the contrary noting that the issue had not been previously addressed.[103]

The *Pharmatrak* characterization of "facility" is incorrect and should not stand as a hindrance to bringing a Stored Communications Act claim. Contrary to that court's description of the service, similar to a telephone or television, the interactive nature of the Internet requires that a computer be considered a crucial facility for accessing the "electronic communications service" provided by the ISP.[104] Cookies themselves, stored on the Internet surfer's computer, are passively relayed *back* to the web site in order to effectively use the service in question.[105] This is in contrast to the telephone, in which the audio communications (voices) are transmitted back and forth as the sole service. With a computer, the Internet is the

---

[100] 18 U.S.C. § 2701(a).

[101] *Id.*

[102] *In re Pharmatrak*, 220 F. Supp. 2d at 13.

[103] *In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947 at *8.

[104] As described *supra* in n. 50.

[105] Whalen, *supra* n. 16.

service. However, the Internet requires a computer to actively maintain connections and send information as required to display the web site. As such, the Internet surfer's computer should be considered a "facility" under § 2701(a).[106]

2. A Cookie in "Electronic Storage"

Next, it must be determined that a cookie stored on an Internet surfer's computer is in "electronic storage" pursuant to § 2701(a). "Electronic storage" is defined in § 2510(17)(A) as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[107] All three previously described decisions[108] held that Internet cookies were not in "electronic storage" because of their indefinite term of existence and their accessibility from a hard drive.[109]

The nature of the Internet, and of cookies themselves, belies such an interpretation. Cookies, by their technical design, are temporary and intermediate because they have a functional expiration date (be it 6 hours or 12 years) and are not designed for any functional use on the computer on which they reside.[110] The *DoubleClick* court's limited dictionary definition of "temporary" supports the argument that cookies should be considered as such.[111] In *DoubleClick*, the court stated that "temporary" means "lasting for a limited time."[112] Clearly, a listed expiration date defines that a time is limited.[113] Further, a cookie's sole existence is incidental to their request by the web site in question, rendering them intermediary. The *DoubleClick* court defined intermediate as "being . . . in the middle place."[114] This is plainly where cookies stand. They exist not for the web site as presented on

---

[106] As noted in the *Toys R Us* case, other courts have explicitly or implicitly rejected the contention that a personal computer is not a "facility." 1999 U.S. Dist. LEXIS 16947 at *8, n. 7; *Chance v. Avenue A., Inc.*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001) (holding that the plaintiffs provided sufficient evidence to characterize individual computers as "facilities").

[107] 18 U.S.C. § 2510(17)(A).

[108] *Supra* in section II.

[109] This is relevant because the decisions hold that a communication stored in RAM was held to be in "electronic storage."

[110] Whalen, *supra* n. 16.

[111] *In re DoubleClick*, 154 F. Supp. 2d at 512.

[112] *Id.* (quoting *Webster's Third New International Dictionary* 2353 (Philip Babcock Gove & Merriam-Webster Editorial Staff eds., Merriam-Webster 1993)).

[113] Even if the time is limited by the life of an individual plus 70 years, the Supreme Court has indicated that it does stand for "limited times." *Eldred v. Ashcroft*, 537 U.S. 186 (2003) (discussing the Copyright Term Extension Act in light of the Constitution's prescribed term of "limited times").

[114] *In re DoubleClick*, 154 F. Supp. 2d at 512 (quoting *Webster's Third New International Dictionary* at 1180).

the page. Rather, they exist *only* to be passed back to the web server sending the web site.[115] Even if cookies are returning to the server, which sent them, they exist only in the middle location.[116] These definitions lead to the clear conclusion that a cookie is in "electronic storage" for the purposes of a § 2701 claim.

3. Who Gives Authorization?

Given that the preceding discussion has established that a statutory claim is presentable under § 2701(a), it is next necessary to remove the statutory exclusion, which may permit such conduct. Section 2701(c) removes from liability the conduct that is "authorized— (2) by a user of that [electronics communication] service with respect to a communication of or intended for that user."[117] The important consideration then becomes determining who is a "user" for purposes of the exclusion. If the *DoubleClick*, *Pharmatrak*, and *Toys R Us* decisions are correct, the original web site visited by the Internet surfer, that caused the tracking item to be downloaded, is the "user" and may authorize such conduct. However, this analysis undermines the realities of the Internet and a common statutory understanding.

Section 2510(13) defines "user" as "any person or entity who— (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use."[118] Given this definition, it is difficult to see how the courts failed to find the Internet surfer to be a "user" pursuant to the statute. Given the plain language, an Internet surfer "uses an electronic communications service" (the Internet, as provided by the ISP), and is "duly authorized" to do so (by the requirement of authorization in logging onto the service).[119] The courts' anomalous consideration that web sites are users of the tracking service, and thus authorize it to be sent to the Internet surfer, belies the fact that the communication is between the Internet surfer and the web site, with little or no mention of the tracking service. To analogize, this situation is similar to that of person A allowing person X to read the caller ID information and listen to every phone call made to person A, without the knowledge of the calling party. This type of piggybacking without the Internet surfer's knowledge or consent is not the exception § 2701(c) is attempting to

[115] Whalen, *supra* n. 16.
[116] *Id.*
[117] 18 U.S.C. § 2701(c).
[118] *Id.* at § 2510(13).
[119] *Id.*

prevent, and other courts should not find this interpretation persuasive.

The preceding discussion indicates that first, a Stored Communications Act claim does exist pursuant to § 2701(a), as the Internet surfer's computer exists as a facility by which information in "electronic storage" is accessed without authorization. Furthermore, such access is not authorized by the proper "user" pursuant to the statute, the Internet surfer; meaning that the Stored Communications Act can serve to ensure an Internet user's privacy.

B. The Wiretap Act

The Wiretap Act provides a civil remedy against "any person who--intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication."[120] DoubleClick and the other online monitoring companies did not contest that their conduct, as pled, violated this provision. However, they claimed that they were saved by the statutory exception in 18 U.S.C. § 2511(2)(d), which excludes from liability any violation of § 2511(1) and when the interception has been consented to, unless the interception occurs for criminal or tortious purposes.[121]

All three of the courts analyzed the issue of "consent" along the same lines as the Stored Communications Act as described in the previous section.[122] That is, they determined the proper entity to authorize the interception was the web site visited by the Internet user. As described above, this conclusion is erroneous, and as a result, the "authorization" is not present here as well. This removes the statutory exception from consideration and the Wiretap Act claims should have proceeded.

However, assuming that consent did occur (via a click through license, user agreements, etc.), it is entirely plausible that the data collection *is* with a tortious or criminal intent. Section 2511(2)(d) creates an exception to the consent exclusion of the Wiretap Act. The exception is not applicable to a communication "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[123]

The *DoubleClick* court recants cases in which "tortious intent" cannot

---

[120] *Id.* at § 2511(1).

[121] *In re DoubleClick*, 154 F. Supp. 2d at 514; *In re Pharmatrak*, 220 F. Supp. 2d at 11; *In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947 at *22.

[122] *Supra* section III(A)(3).

[123] 18 U.S.C. § 2511(2)(d).

be proven by simply showing a tort was committed.[124] Rather, the act giving rise to the Wiretap Act violation must be contemporaneous with the commission of the tort.[125] The court further asserted that DoubleClick's intent could not have been tortious because their activities were conducted with significant media publicity.[126]

However, as noted in Section D, *infra*, a variety of state privacy torts may provide a cause of action against online marketers like DoubleClick. Most of them are specific intent causes, and unlike the broadcast media cases cited by the *DoubleClick* court,[127] all of the data collection actions were conducted towards the goal of profile building (which may or may not constitute a state tort).[128] As such, the *DoubleClick* court's summary dismissal of the possibility of "tortious intent" requires a more thorough understanding of potential state tort claims. This understanding of "tortious intent" may provide a cause of action under the Wiretap Act even if the correct "consent" analysis is not adopted as described in section III(A)(3) above.

Thus, it is apparent that no statutory exception should preclude a Wiretap Act claim, and the option to protect an Internet surfer's privacy from organizations that would seek to impair it is viable. Further, if the definition of "consent" and "authorization" utilized by the *DoubleClick* court maintains its persuasiveness, the question of whether such an exclusion is barred by a "tortious intent" requires a much more significant evaluation.

C. The Computer Fraud and Abuse Act

The CFAA creates a civil remedy for anyone who suffers damages or losses because of an individual's or entity's unauthorized access to a protected computer in order to obtain information involved in an interstate or foreign communication.[129] However, the incident must cause loss

---

[124] *In re DoubleClick*, 154 F. Supp. 2d at 515-17 (citing *Sussman v. ABC*, 186 F.3d 1200 (9th Cir. 1999) (holding that the purpose of the act constituting an alleged Wiretap Act violation was the primary focus of a § 2511(2)(d) exception); *J.H. Desnick v. ABC*, 44 F.3d 1345, 1353 (7th Cir. 1995) (holding that the commission of a tortious act does not necessarily require a tortious purpose)).

[125] *Id.* at 519.

[126] *Id.*

[127] *Id.* at 519, n. 26 (citing *Berger v. Cable New Network, Inc.*, 1996 U.S. Dist. LEXIS 22524 at *11 (D. Mont. Feb. 26, 1996); *Russell v. ABC*, 1995 U.S. Dist. LEXIS 7528 at *4 (N.D. Ill. May 30, 1995)).

[128] *Infra* section III(D)(3).

[129] 18 U.S.C. § 1030(a)(2)(C).

aggregating at least $5,000 to one or more individuals.[130]

This is the primary assertion that has managed to avoid summary judgment or a 12(b)(6) dismissal, although only in limited circumstances.[131] The courts in *DoubleClick* and *Pharmatrak* found the legislative history precluded aggregation across incidents, and thus, claims from individuals like those in the present cases failed to meet the $5,000 requirement.[132] However, the court in *Toys R Us* held (along with several other courts interpreting the statute on different issues) that the sending of a cookie (even if uniquely identified) counted as a "single act" from which damages could be aggregated across the class of plaintiffs in order to reach the $5,000 limit.[133]

The split between the district courts was never resolved at a higher level because the 2002 amendments to § 1030 removed the $5,000 damages limit.[134] Hence, the $5,000 limit should not have existed (and indeed, now does not exist) as a bar to bringing a CFAA claim. Therefore the CFAA also stands as a legitimate tool to protect Internet privacy.

D. Alternative Methods of Privacy Protection

Methods of protecting Internet privacy exist outside the scope of Federal remedial law. First, there exists the potential for agency action, in order to ensure that the conduct of companies, like DoubleClick, Pharmatrak, and Coremetrics, do not step outside the bounds of legality. Second, personal awareness can be heightened through web sites promoting knowledge about the information tracking, how the tracking could affect the individual surfer, and what to do about it. Lastly, state tort laws may provide a method of pursuing such protection.

1. The Regulatory Agencies

Regulatory agencies like the Federal Trade Commission ("FTC") have

---

[130] *Id.* at § 1030(e)(8).

[131] *In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947 at *36; *In re America Online, Inc. Version 5.0 Software Litigation*, 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001).

[132] *In re Pharmatrak*, 220 F. Supp. 2d at 15; *In re DoubleClick*, 154 F. Supp. 2d at 526.

[133] *In re Toys R Us*, 2001 U.S. Dist. LEXIS 16947 at *36; *In re America Online*, 168 F. Supp. 2d at 1374.

[134] Pub. L. No. 107-296, 116 Stat. 2158 (2002). As noted by the court in *In re America Online*, "the CFAA has been increasingly broadened by Congress." 168 F. Supp. 2d at 1374.

had an effective role in the Internet privacy arena.[135] The FTC has been effective in forcing Internet companies to abide by its privacy policies.[136] Furthermore, the FTC plays an advisory role to Congress in suggesting further legislation.[137] Although the Stored Communications Act, the Wiretap Act, and the CFAA should provide protection from such activities, it may be necessary to create more directed legislation. It is heartening to see an agency tasked with protecting the privacy of Internet users, but their effectiveness can only be measured by the cases and instances that exist today.

2. Consumer Awareness Efforts

Industry self-regulation is occurring through informational efforts. Many sites publish their own privacy policies and Internet-based programs, like the Better Business Bureau's ("BBB") privacy program, which exists to inform consumers about web privacy and highlights sites that comply with the BBB's privacy standards.[138] Such programs are a step in the right direction, but again, concerns should be raised over the affirmative duty of awareness for the individual consumer.

Individual online web sites also offer extensive information about what data is collected.[139] However, this information is usually placed in an obscure location on the home page.[140] The transparency created by the explanation of cookies and their use on a particular site is important in evaluating the "trustworthiness" of the site, but it does not necessarily compel the site to follow that policy. Such notices, again, provide an aid

---

[135] *See* Rachel K. Zimmerman, *The Way the Cookies Crumble: Internet Privacy and Data Protection in the 21st Century*, 4 N.Y.U. J. Legis. & Pub. Policy 439, 454 (2000) (discussing the FTC's role in resolving an issue concerning GeoCities' violation of its privacy policy).

[136] *Id.*

[137] Federal Trade Commission, *Guide to the Federal Trade Commission*, http://www.ftc.gov/bcp/conline/pubs/general/guidetoftc.htm (accessed Aug. 8, 2003).

[138] The BBB runs an informative, but somewhat outdated privacy information web site. *See* Council of Better Business Bureau, Inc., *Consumer Toolbox*, http://www.bbbonline.org/UnderstandingPrivacy/toolbox/ (accessed Apr. 3, 2003).

[139] Amazon, for example, has a privacy page on which they detail the information they collect. *See* Amazon.com, *Amazon.com: Help / Privacy & Security / Privacy Notice*, http://www.amazon.com/exec/obidos/tg/browse/-/468496 (accessed Apr. 28, 2003). Amazon goes on to describe and link several anonymizing features, but notes "[a]lthough we will not be able to provide you with a personalized experience at Amazon.com if we cannot recognize you, we want you to be aware that these tools exist." *Id.* The *New York Times* web site maintains a "Cookies FAQ" in its help section, but it requires three clicks from the main page to find it. *See* New York Times, *Frequently Asked Questions About Cookies*, http://www.nytimes.com/ref/membercenter/help/cookiesfaq.html (accessed May 3, 2003).

[140] *Id.*

only to the savvy surfer, and while helpful, stronger measures would guarantee greater informational privacy.

Additionally there are a number of companies, similar to TRUSTe, allowing web sites comporting to TRUSTe's requirements to display a "trustmark" indicating their compliance.[141] A collective mark organization, like TRUSTe, goes a long way towards ensuring that member web sites comport to a standardized policy, but does little to protect those web sites which fail to opt-in to TRUSTe's requirements (or those who wish to avoid TRUSTe's $600-$75,000 fees).[142]

Still the Internet can be a hidden danger, in that an expensive web site by a corporation involved in privacy protection may look identical to a web site by a company seeking to exploit any personal data. As such, educational programs and informational notices are a good step in the right direction, but do little to guarantee an enhancement of privacy while on the Internet.

3. State Tort Actions

State tort actions regarding privacy may provide a method of redress for those Internet surfers directly affected by such an abuse.[143] The Arkansas concept espoused by McKinney and Whitten asserts positively that state tort claims for Intrusion upon Seclusion,[144] Appropriation of Name or Likeness,[145] Publicity Given to Private Life,[146] and Publicity

---

[141] According to the TRUSTe web site, "the trustmark is awarded only to sites that adhere to established privacy principles and agree to comply with ongoing TRUSTe oversight and consumer resolution procedures." TRUSTe, *TRUSTe for Consumers*, http://www.truste.org/consumers/users_how.html (accessed May 3, 2003). The TRUSTe privacy principles include: adoption and implementation of a privacy policy, notice and disclosure of information collection and use practices, choice and consent regarding a use of a surfer's information, and data security and access measures to prevent abuse of this information. *Id.*

[142] TRUSTe, *TRUSTe Seal Programs*, http://www.truste.org/programs/pub_how_join.html (accessed May 3, 2003).

[143] This concept is extensively addressed in the scope of Arkansas tort law. Bryan T. McKinney & Dwayne Whitten, *Arkansas Surfers and Their Privacy, or Lack Thereof: Does the Common Law Invasion of Privacy Tort Prohibit E-Tailer's Use of Cookies?*, 24 UALR L.J. 751 (2002).

[144] *Restatement (Second) of Torts* § 652(B) (1976), defines the tort of intrusion upon seclusion as "[o]ne 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."

[145] *Id.* at § 652(C) defines the tort as creating liability for "[o]ne who appropriates to his own use or benefit the name or likeness of another . . . ."

[146] "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized . . . (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." *Id.* at § 652(D)

Placing a Person in a False Light,[147] may provide a state law remedy for privacy violations due to web tracking technologies. Unfortunately, none of the preceding tort claims have resulted in appellate level caselaw.

This section has positively identified several methods, in addition to Federal statutory protection, that Internet users may use to protect their privacy rights. Consumer education should play a large role in Internet use. Just because the Internet is an easily accessible medium does not mean that traditional notions of guardedness and informational privacy should not control.[148] Industry programs, including self-regulation, provide a good keystone for responsible Internet development; but again, constant vigilance and consumer participation is important. Lastly, state tort laws still provide a relatively unexplored avenue for protecting privacy rights against Internet marketing organizations.

IV. CONCLUSION

The Internet, and the technological advances that have accompanied it, has created new avenues for communication, shopping, researching and interconnecting. While the Internet's massive growth has expanded its possibilities, it has also created a circumstance where technology is enabling others to invade personal privacy. Personal privacy should exist on the Internet as much as it does in the real world, and a large variety of remedies exist to ensure that surfing habits remain private.

Lawsuits brought to protect this privacy have met many hurdles posed by courts that improperly apply Federal statutes to the Internet. Courts handling such claims have placed an overly large reliance on the incorrect holding in *In re DoubleClick*, removing the ability of plaintiffs to maintain successful claims against Internet marketers under the Stored Communications Act, the Wiretap Act, and the CFAA. A proper interpretation of these three statutes indicates that such claims *should not* be precluded as they currently are.

---

[147] *Id.* at § 652(E) provides that,

> [o]ne who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

[148] Generally, you would not give your personal information to purchase a newspaper at the machine on the corner. However, the *New York Times* web site requires you to register (and give personally identifying information) in order to view its free content and allow the *New York Times* to track your usage across the site. New York Times, *Registration Help*, http://www.nytimes.com/ref/membercenter/help/reghelp.html (accessed May 3, 2003).

Furthermore, a wide variety of alternative measures exist for protecting privacy. Agency action, industry self-regulation, and state tort actions also serve an important function in ensuring that Internet tracking companies do not overstep their bounds. As with any real world activity, personal privacy precautions should not fall away just because the activity has been translated into a new medium.