



TOURO UNIVERSITY
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

Touro Law Review

Volume 20
Number 2 *Symposium: The Fifteenth Annual
Supreme Court Review*

Article 11

December 2014

Cookie Monster: Balancing Internet Privacy with Commerce, Technology and Terrorism

Nichoel Forrett
Touro Law School

Follow this and additional works at: <https://digitalcommons.tourolaw.edu/lawreview>



Part of the [Commercial Law Commons](#), [Communications Law Commons](#), [Internet Law Commons](#), and
the [Privacy Law Commons](#)

Recommended Citation

Forrett, Nichoel (2014) "Cookie Monster: Balancing Internet Privacy with Commerce, Technology and
Terrorism," *Touro Law Review*: Vol. 20: No. 2, Article 11.

Available at: <https://digitalcommons.tourolaw.edu/lawreview/vol20/iss2/11>

This Annual Supreme Court Review is brought to you for free and open access by Digital Commons @ Touro Law
Center. It has been accepted for inclusion in Touro Law Review by an authorized editor of Digital Commons @
Touro Law Center. For more information, please contact lross@tourolaw.edu.

COOKIE MONSTER: BALANCING INTERNET PRIVACY WITH COMMERCE, TECHNOLOGY, AND TERRORISM.

Nichoel Forrett¹

INTRODUCTION

“People are reluctant to have their reading and viewing habits exposed because we correctly fear that when isolated bits of personal information are confused with genuine knowledge, they may create an inaccurate picture of the full range of our interests and complicated personalities.”² This fear is more prevalent than ever in the context of the Internet.

The Internet has the potential to be an impressive marketing tool. Aspects of web technology, such as cookies, give advertisers unprecedented ability to personalize advertisements to the consumers viewing web sites. Consumers, however, are traditionally wary of advertising efforts, and online marketing brings such trepidation to new heights. Even the benefit of only receiving targeted advertisements that match their habits, needs or interests is not enough to calm uneasiness about the information collected to achieve that benefit. Similar information is available

¹ J.D. Candidate, May 2004, Touro Law Center; B.S., Cornell University, 2001. I would like to thank Professor J. Ezor for his time and assistance in mentoring me on this article.

² JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* 167 (Vintage Books 2001).

online as offline, but the ease of availability of personal data on the Internet makes consumers feel violated and vulnerable. Are online advertising technologies violating users' rights to privacy, and if so, are the laws providing enough protection to balance consumer right to privacy interests with the needs of marketers?

This article will examine how the needs of marketers and Internet content providers can be balanced with consumers' need for privacy. As an introduction, a brief overview of cookies technology is provided, along with a discussion of the advantages and disadvantages of cookies. It will explore the tort liability issues that cookies raise, including invasion of privacy and trespass. Furthermore, the current Federal Trade Commission (FTC) findings and federal law relating to cookies are addressed. This article will conclude with possible solutions and recommendations concerning Internet privacy.

INTRODUCTION TO COOKIES

Cookies are perhaps the most familiar and obvious form of web technology a user comes into contact with. A cookie is a text file that a web site places on a user's hard drive, allowing the web site to store information about the user for later retrieval.³ The web

³ Marshall Brain, *How Stuff Works*, at www.howstuffworks.com/cookies.html (last visited February 3, 2004). An example of a cookie for this site: HSWid84926004howstuffworks.com/1024137330892830785632149386752029557255

* RMID ce95ca143e99daa0 howstuffworks.com/ 1024 3567004032 301243581508767520 29557255 *

site places and retrieves this information via the computer's web browser, and this information can include an ID for the computer, the date, time and length of each separate visit, the path to and from the site, the time spent on each page, and which links are clicked during the visit.⁴

The process of depositing and accessing cookies functions as follows: the user types the web site they wish to see into the browser, and the browser requests the page from the web site, which either creates a cookie to send to the browser or uses a cookie already on the browser's computer from a previous visit to that site. The web site then updates the cookie as the user browses.⁵ Without cookies, there would be no continuity between the web site and the user's browser, and the user would need to repeatedly retype information. Cookies were invented because:

Between page downloads, the server does not have to do anything. . . .The main problem, though, is that there are not many convenient ways to keep the server and the [browser] in sync during this 'silent period.' Real-world tasks demand multiple transactions connected by a consistent set of circumstances – a consistent state.⁶

This is called state maintenance, where the web site stores information in cookies regarding what state the browser was in the last time it visited the site.⁷ Cookies are the easiest way to provide

⁴ *Id.*

⁵ *Id.*

⁶ SIMON ST. LAURENT, COOKIES 15 (McGraw-Hill 1998).

⁷ *Id.*

continuity between visits to the site because they are stored within the user's computer and can be returned to numerous times.

Cookies are not a new concept. Programmers regularly use small text files containing information as a bridge between parts of a program that will not communicate with each other. Operating systems use cookie-like files to store user preferences while the computer is turned off. Netscape was the first browser to use cookies as part of its version 1.1 in 1991. Version 2.0 was the first browser to provide the option of turning cookies off.⁸ That option can be used to block cookies from the hard drive, but not many average users are aware of it. In browser applications, such as Netscape and Internet Explorer, advanced options in the preferences menu allow users to completely disable cookies, to only allow cookies that are not sent to a third party site, i.e. an advertising site, or to enable all cookies.⁹ Anti-virus software or other software can also be used to perform the same function. However, when cookies are disabled, many sites will not function properly. Another option available to advanced users is altering the properties of the folders that store cookie files on the hard drive to make them read-only so that no new cookies can be written and stored.¹⁰

The providers of the two most popular Internet browsers, Netscape and Microsoft, limit the number of cookies that can be

⁸ *Id.*

⁹ Interview with William J. Bayard, Computer Consultant, Bayard Computer Consulting, in Glens Falls, N.Y. (October 27, 2002).

¹⁰ *Id.*

placed on the hard drive to approximately 300 cookies at one time.¹¹ When the temporary Internet files of a computer are full of cookies and other files accumulated during browsing, the browser discards the oldest cookies and files to clear hard drive space for new cookies and files. The default size of the temporary Internet files folder is two percent of total hard drive storage space.¹² These figures should help the reader understand the small size of cookies and the space allotted to those and other Internet files on a computer.

Advantages and Disadvantages of Cookies

Advantages

Without cookies, there would be no continuity between web site visits and it would be harder for site managers to determine the success of their sites or to identify which parts of the site are underutilized. Such determination is best accomplished by tracking a unique person, the user, as he or she progresses through the site. The only accurate way for a web site to count users who view the site is to set a cookie with a unique ID for each user.¹³ The use of cookies allows the site to count how many visitors it receives, how many of those visitors are new or repeats, and how

¹¹ ST. LAURENT, *supra* note 6.

¹² David Whalen, *The Unofficial Cookie FAQ Version 2.54*, at <http://www.cookiecentral.com/faq/#2.5> (last visited Feb. 3, 2004).

¹³ Brain, *supra* note 3.

often the repeats have visited.¹⁴ Using a database, the site can match the ID in the cookie file with the ID in the database associated with that user if the user previously entered personal information on that site.¹⁵ Such state maintenance provides web sites with vital statistics about user online behavior, which is a boon for advertisers. Advertising on web sites is what funds most content on the Internet.¹⁶ The information collected about users also allows advertisers to better target their marketing so that only interested users receive specific advertisements for certain products or services.

In addition, this targeting of audiences allows web sites to alter their appearance according to preferences the user set during previous visits, which can be a great convenience for users.¹⁷ The web site recognizes a cookie file and uses that to retrieve the information regarding the user's preferences stored on the web site, which then customizes itself for the visitor. For example, a user who registers on Amazon.com in order to buy a book finds that on the next visit, Amazon remembers what areas the user clicked on and what topics the user browsed and bought, prominently displaying similar items for the user's consideration. Or, a Yahoo user can customize the site to show weather for certain cities, news from certain sources, a television listing for the local cable provider, and the user's horoscope.

¹⁴ Brain, *supra* note 3.

¹⁵ ST. LAURENT, *supra* note 6, at 30.

¹⁶ ST. LAURENT, *supra* note 6, at 30.

¹⁷ Whalen, *supra* note 12.

E-commerce sites use cookies to speed online transactions by matching the ID in cookie files to information in the database regarding items the user clicked on to purchase, their billing information and shipping addresses.¹⁸ The site then puts this information in the order form for the user, expediting checkout. This enables the user to place orders quickly and get on to other tasks, saving time and the hassle of having to constantly look up information. Similarly, the user's log in and password can be stored so the user does not have to type them in for every site they visit, which is also a convenience if the user forgets what their password was.

Disadvantages

Cookies have been accused of all kinds of mayhem, from stealing email addresses to opening holes that unscrupulous developers use to collect enough bits about your identity to let them break into your computer and financial accounts. The repeated claims of the browser vendors that cookies are not capable of such dealings seem only to breed more concern among users. Unfortunately, for the myths swirling around the Internet, the vendors are right – but there are still a number of issues that deserve a much closer examination. Cookies cannot spread viruses, steal your personal information, read your hard drive, or empty your bank account surreptitiously. On the other hand, cookies can allow server operators to track your movements much the way a grocery store check-cashing card or

¹⁸ Whalen, *supra* note 12.

even a credit card can, and you may not appreciate being followed.¹⁹

The same aspects that make cookies useful and beneficial also make them potentially invasive. The view that cookies are a growing problem is mostly a backlash to advertising. Consumers are angered by the constant bombardment of advertising both in email and on the web sites they visit. Consumers are well aware of traditional methods of marketing through the distribution of offline marketing lists consisting of names, addresses and telephone numbers. Television and radio commercials can be ignored and junk mail thrown out, but consumers are less forgiving of spam (unsolicited commercial email) or web sites blatantly mining information about consumers to sell to advertisers who can, in return, send more advertisements to them. Telemarketers are mostly reviled, and online advertising is not viewed much more favorably. The Internet makes traditional direct marketing techniques, such as compiling mailing lists from recent purchasers of a product to use in mass mailings regarding similar products, even more effective since it allows marketers to examine consumer behavior in unprecedented minute detail and at minimal marketing and distribution costs.²⁰

Most advertising on web sites is handled by brokers, who send cookies to the user's hard drive in order to track sites visited, keywords searched, purchases made, and any personal information

¹⁹ ST. LAURENT, *supra* note 6, at 30.

²⁰ Shaun Sparks, *The Direct Marketing Model and Virtual Identity*, 18 DICK. J.

INT'L L. 517, 527 (2000).

entered, as long as the sites visited are members of the broker's network. In the case of large brokers with networks of thousands of popular sites, visiting a member site of a broker network is not out of the ordinary.²¹ Most sites can only read the cookies they place, but a broker can place and read cookies from any site on their network. It is this ability that creates the ability to track a user throughout a good portion of the Internet.

Other Privacy Threats

Online, the greatest threat to privacy comes from the electronic "footprints" users leave, with which it is possible to monitor and trace nearly everything we read, write, browse and buy.²² Most web browsers are configured to reveal to every site visited the address of the site viewed just before; they also reveal the user's Internet Protocol (IP) address, a unique number which may reveal the individual user, not just the computer being used.²³ An IP address is not as good an identification as cookies since the address a user has may change. For dial-up users, the Internet Service Provider (ISP) may assign a different IP address each time a user connects, so the number used at any one session is only unique to that user for that session. A web site can link the unique ID in cookie files or the IP address with any information in its

²¹ ROSEN, *supra* note 2, at 163.

²² ROSEN, *supra* note 2, at 163.

²³ ROSEN, *supra* note 2, at 163.

database associated with that ID, and sites may sell this often personal information to third parties.

As noted above, the information gathered from this tracking can be extensive, detailing online movements, purchases and interests. Information tracked by marketers, particularly in potentially sensitive areas such as healthcare or financial status, are often deemed more invasive by consumers than other areas. Such actions could alert others of facts that the user had intended to keep private, such as an impending divorce that could be tracked through web sites directed to individuals seeking a divorce attorney. This accounts for the unsettling experience of being bombarded with targeted ads after expressing an interest in a particular topic.²⁴

Direct marketers are not the only people who are interested in consumer profiles and electronic footprints. Drug companies may send unsolicited mail to a user who researched an illness. An insurance company might be interested in such medical information as well. Potential employers might want to know financial information or interests of job applicants that might show unreliability. Now, more than ever before, the government is taking a keen interest in who is browsing in certain topics and new laws, such as the Patriot Act²⁵ and Homeland Security Act,²⁶ allow it to access user's email and Internet activities.²⁷ In the face of

²⁴ ROSEN, *supra* note 2, at 163.

²⁵ U.S.A. Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.).

²⁶ Homeland Security Act of 2002, 6 U.S.C. §101 et seq. (2002).

²⁷ ROSEN, *supra* note 2, at 164.

such potential intrusion into online information, privacy is more important than ever to consumers.

THE RIGHT OF PRIVACY

Constitutional Protection

Privacy is not a right specifically enumerated in the Constitution. Instead, this right is implied through the Fourth, Fifth, and Ninth Amendments. The Fourth Amendment states that, “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”²⁸ The Ninth Amendment reassures the public that “the enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people.”²⁹ The Fifth Amendment states that “no person . . . shall be compelled, in any criminal case, to be a witness against himself.”³⁰ In *Griswold v. Connecticut*,³¹ the Supreme Court recognized that the Bill of Rights provides “zones of privacy” where a person would reasonably expect his or her actions to be private.³² The right of privacy created by the Amendments is, the

²⁸ U.S. CONST. amend. IV.

²⁹ U.S. CONST. amend. IX.

³⁰ U.S. CONST. amend. V.

³¹ 381 U.S. 479 (1965).

³² *Id.* at 484 (“Specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy.”).

Supreme Court ruled, a fundamental right.³³ Most privacy inquiries focus on a Fourth Amendment analysis.³⁴

It is arguable whether the Internet constitutes a “zone of privacy.” One argument is that there can be no privacy because the exchange of information takes place in public, and consumers do not expect privacy with traditional retailers they visit in public. The definition of “public” is that which belongs to the community at large, under no entity’s protection and subject to appropriation by anyone.³⁵ The Internet, by this definition, is a public domain and, therefore, any action one takes within the Internet without special effort taken to ensure one’s privacy and security could be considered a public act.

In addition, Internet users are, for the most part, aware that the Internet does not provide privacy. According to the *Pew Internet & American Life Project*, eighty-four percent of Internet users are concerned about businesses and other strangers obtaining their personal data.³⁶ *Harris Interactive Inc.* reported that fifty-three percent of users are afraid that financial information may be stolen during online transactions and thirty-five percent are wary of online hackers.³⁷ These studies indicate that the population is

³³ *Id.* at 485 (“We recently referred in *Mapp v. Ohio*, 367 U.S. 643, 656 (1961), to the Fourth Amendment as creating a ‘right to privacy, no less important than any other right carefully and particularly reserved to the people.’”).

³⁴ See *infra* note 46.

³⁵ BLACKS LAW DICTIONARY 995 (7th ed. 2000).

³⁶ Dick Kelsey, *Almost No One Rejects Cookies - Study*, Newsbytes (2001).

³⁷ Steve Jarvis, *Privacy’s Strange Bedfellows*, AMA’s Marketing News 18 (November 6, 2000).

not naïve about the fears regarding lack of privacy on the Internet, even if those fears do not come to pass.

Consider this example of actions taken within a public environment without an expectation of privacy. Consumers generally do not think about privacy in traditional retail environments. The majority of retailers, particularly supermarkets, scan bar codes of products. When payment is made by a credit card, these purchases can be linked to the individual's personal information. The transaction occurs in a retail environment, which is likely to be inhabited by other individuals unknown to that person, and therefore, is a public act. Thus, one may argue, there is no reasonable expectation of privacy since anyone can see what products are in the consumer's cart, or the store may somehow use the information compiled from the credit card purchase. Stores often sell the information they gather regarding people's buying habits. Most stores pay customers for information on their buying habits via frequent shopper cards that track purchases in conjunction with personal and demographic information. As an incentive to cooperate, the customer receives reduced prices on merchandise.³⁸ As with a credit card purchase offline, all

³⁸ Ronald B. Standler, *Possible Examples of Privacy Violations by Businesses* (1997), at <http://www.rbs2.com/privacy.htm> (last visited Feb. 3, 2004).

information entered online is, potentially, permanently traceable and retrievable.

Perhaps the government relied on the argument that the Internet is a public domain when drafting the new terrorism laws which allow law enforcement officials to require ISPs and web sites, upon request, to release information regarding a user's Internet activity and browsing habits.³⁹ The Cyber Security Enhancement Act⁴⁰ component of the Homeland Security Act increases the ability of law enforcement to eavesdrop on phone or Internet communications without a court order.⁴¹ It is such extreme government action that fires proponents of the alternate argument that the Internet is not a public domain.

In *Katz v. U.S.*,⁴² the Supreme Court again analyzed public and private expectations. Katz was charged with calling wagering information to other states in violation of federal law. The lower court allowed FBI evidence gathered from listening and recording devices placed outside the public phone booth Katz used, and Katz was convicted of the above charge.⁴³ He appealed on grounds that the surveillance evidence violated his Fourth Amendment right to privacy.⁴⁴ The appeals court affirmed the conviction, then the Supreme Court granted certiorari.⁴⁵

³⁹ Patriot Act § 212.

⁴⁰ Homeland Security Act § 225 (codified throughout the U.S.C.).

⁴¹ Declan McCullagh, *Pentagon Drops Plan to Curb Net Anonymity*, at <http://news.com.com/2100-1023-966894.html> (Nov. 22, 2002).

⁴² 389 U.S. 347 (1967).

⁴³ *Id.* at 348.

⁴⁴ *Id.*

⁴⁵ *Id.* at 349.

The Court ruled that even eavesdropping in a public place could constitute invasion of privacy, stating that “what a person knowingly exposes to the public, even in his own home or office, is not subject of Fourth Amendment protection . . . but what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”⁴⁶ The Court also declared that the electronic devices used by the FBI, even though they did not penetrate into the phone booth, were an invasion of privacy.⁴⁷ From this opinion one can extrapolate that even Internet surfing in public places does not negate the user’s right to privacy when the user means his or her browsing to be private. The argument, then, is that if the user has a reasonable expectation of privacy while browsing the Internet, even if others could potentially witness such action in some fashion, such as using cookies, then the user’s privacy interest is still protected.

To gain Fourth Amendment protection under this interpretation, users must then make some effort to keep their information private.⁴⁸ These efforts could include any of the number of software programs available that either block cookies from being deposited and accessed or hide the user’s identity. A *Web Side Story* survey of more than one billion web page views revealed that cookies were only disabled seven percent of the

⁴⁶ *Id.* at 351.

⁴⁷ 389 U.S. at 353.

⁴⁸ *Cf. Katz*, 389 U.S. at 351. Extrapolating from the Court’s statement, “what he seeks to preserve as private,” the inference can be made that for privacy to be protected, the person must take steps to keep his or her action as private as possible in those circumstances.

time.⁴⁹ In a slightly more forgiving study by *Pew Internet & American Life Project*, ten percent of Internet users made efforts to block cookies.⁵⁰ Although failure to block cookies may mean some consumers merely prefer convenience over privacy, these studies indicate that not many people are taking steps to gain protection of their privacy by blocking cookies. In circumstances where the Constitution does not protect one's privacy, protection may still be possible under state tort law.

Tort Law Protection

Tort law provides protection for privacy under actions for trespass or invasion of privacy. As the Court stated in *Katz*, physical penetration or intrusion by electronic technology is not necessary to prove invasion of privacy,⁵¹ but online, it may be the only physical evidence of such intrusion. Hence, software files such as cookies could be considered an intrusion, not just physical hardware devices.

In *CompuServe Inc. v. CyberPromotion*,⁵² CyberPromotions sent spam email for its clients to CompuServe members.⁵³ CompuServe notified CyberPromotions that this practice was prohibited by CompuServe policy and employed technological

⁴⁹ See Kelsey, *supra* note 37.

⁵⁰ See Kelsey, *supra* note 37.

⁵¹ 389 U.S. at 353.

⁵² 962 F. Supp. 2d 1015 (S.D. Ohio 1997).

⁵³ *Id.* at 1017.

blocks. However, the spam did not cease.⁵⁴ The district court held that CompuServe had a viable claim for trespass and was entitled to injunctive relief.⁵⁵ Because CompuServe owned its computer equipment and was a private company, CyberPromotions' spam was, thus, a physical intrusion upon the property of CompuServe.⁵⁶ The court decided the loss of quality to its property, or chattel (the computer equipment) and loss of its customers injured CompuServe.⁵⁷

It is arguable whether cookies could be considered just as much a physical intrusion to computers as spam. The question is whether consumers are injured by the cookies' intrusion into their hard drives. Loss of private information as invasion of privacy is understandable as an injury, as is lost property. Unlike CompuServe, most consumers are not running a business that would be harmed by files invading their equipment. Under trespass, the plaintiff must suffer some injury or loss by the intrusion. Compared to spam, cookies are very small files, so it is unlikely the space they take on a hard drive would effectuate a loss of resources argument.

CompuServe references *Glidden v. Szybiak*,⁵⁸ which required some form of damage to the chattel for the trespasser to be held liable.⁵⁹ The case involved Glidden claiming an injury

⁵⁴ *Id.*

⁵⁵ *Id.* at 1027.

⁵⁶ *Id.*

⁵⁷ *CompuServe*, 962 F. Supp. 2d at 1028.

⁵⁸ 63 A.2d 233 (N.H. 1949).

⁵⁹ *Id.* at 235.

which Szybiak argued was barred because Glidden was engaged in trespass against the dog. Damage to the dog could not be documented, so the court dismissed the cause of action for lack of damages.⁶⁰ The case addressed the need for substantial interference to a chattel for tort liability to be applied. By analogy, the placement of cookies on a computer hard drive might not constitute this substantial interference because there is no method of proving damage to the computer or its user. Also, for a defendant to be liable for trespass to chattels, a plaintiff must again take actions to protect its property from the defendant.⁶¹ Simply interfering with a chattel is not grounds for legal action. Again, by analogy, it would seem that an Internet user must act via browser, anti-virus, or downloadable software to prohibit the deposit and access of cookies on their computer before legal actions can be taken.

An ISP or online retailer may be liable for trespass to chattels if it engages in the intermeddling of another's chattel and, in so doing, dispossesses the other of the chattel; the chattel is impaired in condition, quality, or value; the possessor is deprived

⁶⁰ *Id.*

⁶¹ *Id.* The Court referenced RESTATEMENT (SECOND) OF TORTS §218 (1979) which states:

One who without consensual or other privilege to do so, uses or otherwise intentionally intermeddles with a chattel which is in the possession of another is liable for a trespass to such person if, but only if, (a) the chattel is impaired as to its condition, quality or value, or (b) the possessor is deprived of the use of the chattel for a substantial time, or (c) bodily harm is thereby caused to the possessor or harm is caused to some person or thing in which the possessor has legally protected interest.

of the use of the chattel for a substantial time; or bodily harm is caused to that which the possessor has a legally protected interest.⁶² For the average Internet user, the chattel in question would be the resources and physical space on a hard drive. A data exchange occurs when cookies are deposited or accessed on an Internet user's computer, constituting intermeddling with the chattels in another's possession. Due to the insignificant amount of resources cookies use, it is unreasonable to state that cookies in any way dispossess Internet users of their computer or online experience. The space taken up on a hard drive neither inhibits the use of the computer nor affects the computer negatively in any substantial way. Again, some other invasion to the user's privacy, not just privacy in the physical use of their computer, must be shown.

Tort invasion of privacy is defined as "intentionally intruding, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns."⁶³ In *Dwyer v. American Express Co.*,⁶⁴ the plaintiffs sued American Express, stating that American Express invaded the cardholders' privacy by

⁶² *Glidden*, 63 A.2d at 235.

⁶³ GERALD FERRERA ET. AL., *CYBERLAW* 192 (Thomson Learning 2000). The elements of the cause of action are: intent to intrude or knowledge of intrusion, reasonable expectation of privacy, and intrusion that was substantial and highly offensive to a reasonable person. *Id.* at 192.

⁶⁴ 652 N.E.2d 1351 (Ill. App. 1995).

compiling and analyzing the spending habits of its cardholders.⁶⁵ The Illinois Supreme Court stated that American Express did not unreasonably invade the plaintiffs' privacy because they voluntarily gave information to American Express and voluntarily used their credit cards.⁶⁶ This information, when analyzed, revealed the cardholder's spending habits.

One can apply the ruling in *Dwyer* to the voluntary admission of information by users who register with a web site and the subsequent dissemination of their online habits into a behavioral profile. Only when the online user provides information is that profile associated with a specific individual. By entering the web site where actions can be recorded via cookies and providing information, the users have consented, in essence, to online profiling. Therefore, under *Dwyer*, it can be argued that such users have waived their privacy interest by voluntarily providing information or entering sites that use cookies.

Dwyer references *Shibley v. Time, Inc.*,⁶⁷ where the Ohio appellate court denied the plaintiff's claim of misappropriation when Time, Inc. sold the names and profiles of its subscribers to direct mail advertisers.⁶⁸ The Court explained:

The right to privacy does not extend to the mailbox and therefore it is constitutionally permissible to sell subscription lists to direct mail advertisers. It necessarily follows that the practice complained of here does not constitute an invasion of privacy even

⁶⁵ *Id.* at 1353.

⁶⁶ *Id.* at 1354.

⁶⁷ 341 N.E.2d 337 (Ohio App. 1975).

⁶⁸ *Id.* at 339.

if appellants' unsupported assertion that this amounts to the sale of 'personality profiles' is taken as true because these profiles are only used to determine what type of advertisement is to be sent.⁶⁹

This decision by the Ohio State Appellate Court clearly allows the use of personal information for personal profiling and advertising purposes, regardless of sale, without infringement upon the right of privacy. Under this precedent, ISPs are not liable for invasion of privacy when they merge online profiles created via cookies with the names of Internet users. The federal government is also interested in the creation of such online profiles.

FEDERAL INVOLVEMENT

Federal Trade Commission Regulations

The Federal Trade Commission's (FTC) responsibilities include enforcement and administrative functions aimed at "prohibiting the unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce."⁷⁰ The duty of the FTC that is most applicable in this instance is that of determining and regulating unfair trade practices by the businesses and organizations that use online technology, including cookies,

⁶⁹ *Id.* at 339-40.

⁷⁰ Federal Trade Commission, *Online Profiling: A Report to Congress* 17 (2000), at <http://www.ftc.gov/os.2000/06/onlineprofilingreportjune2000.pdf>.

for online profiling. In June 2000, the FTC issued a preliminary report of the status of self-regulation in the online environment,⁷¹ but delayed making recommendations until July.⁷² The FTC's recommendations consisted of a scheme for self-regulation already in use by the Network Advertising Initiative (NAI).⁷³ These principles, named the NAI Principles, include:

Notice: requiring that sites which choose to collect information about users must disclose their information practices before doing so;

Choice: consumers are given options regarding the manner in which they want the data to be used beyond what it was specifically collected for;

Access: consumers have the ability to review information for purposes of accuracy and completeness of the data;

Security: data collectors are held under a duty of care to ensure that the data collected is correct and it is reasonably safe from unauthorized use;

Enforcement: that there is a reasonable method of identifying and sanctioning web sites which do not comply with these practices.⁷⁴

⁷¹ *Id.*

⁷² Federal Trade Commission, *Online Profiling: A Report to Congress Part 2* (2000), at <http://www.ftc.gov/os/2000/07/onlineprofiling.htm>.

⁷³ See Federal Trade Commission, *supra* note 70, at 22. The NAI is an organization of the largest Internet advertisers, formed to develop a self-regulation framework.

⁷⁴ See Federal Trade Commission, *supra* note 71, at 1-2.

In contrast to the FTC's previous recommendations, it determined in the 2000 report that legislation is also necessary to regulate the entire industry according to the proposed NAI Principles, and no longer focused on self-regulation of the industry.⁷⁵ The FTC has a considerable task ahead of it, especially since more than sixty federal web sites were found to be currently using cookies to track the users in violation of the federal privacy policy.⁷⁶

Applicable Federal Laws

Of the federal laws currently in effect regarding privacy, only a few apply to the issue of privacy and online technology, either directly or analogously. The Cable Communication Protection Act (CCPA)⁷⁷ deals with the rights of cable subscribers. Cable operators must get subscriber permission before they collect any information about the subscriber and must notify the subscriber about what information is collected and for what purpose.⁷⁸ The subscriber must then be allowed to review the information and correct it if necessary.⁷⁹ The cable operator is not allowed to disclose the information to third parties, nor can it sell

⁷⁵ See Federal Trade Commission, *supra* note 71, at 4.

⁷⁶ CNN, *Report: Federal Web sites violate privacy rules* (2001), at <http://www.cnn.com/2001/TECH/Internet/04/17/Internet.privacy.02/index.html>.

⁷⁷ 47 U.S.C. § 551 (2003).

⁷⁸ *Id.* § 551(a)(1)(A-E).

⁷⁹ *Id.* § 551(b)(2)(d).

mailing lists without subscriber approval.⁸⁰ Web sites provide education and entertainment in much the same way as cable companies do. One interpretation of the CCPA suggests that the use of cookies to collect information on users' web site viewing is analogous to collecting information on cable viewing habits and should be prohibited for web sites just as it is for cable companies.

One direct application of the CCPA could occur with the recent proliferation of cable operators who also provide access to the Internet via cable modem through their cable network. These cable operators who are also ISPs raise the question of whether CCPA regulations apply to their online collection of information. For example, Optimum Online's privacy policy indicates the service collects personal information that users "voluntarily" provide in order to use the service and states it only shares non-personal information with third parties.⁸¹ It does not, however, get user permission before collection or use or allow users to view or correct the information it collects.⁸² The service also uses cookies to track users on the web site, but insists such information collected is non-personal, despite the requirement that users must first log in to use the site or its services.⁸³

⁸⁰ *Id.* § 551(b)(2)(c)(1).

⁸¹ Optimum Online, *Privacy Policy* (2003) at <http://www.optonline.net/Cservice/Article/0,3994,channel%3D68%26article%3D1993854%26type%3Dreg,00.html>.

⁸² *Id.*

⁸³ *Id.*

The Video Privacy Protection Act (VPPA)⁸⁴ states that video stores may not use or disclose titles of the videos their customers rent or purchase combined with personal information about those customers.⁸⁵ They may, however, sell mailing lists that include names, addresses and subject matter viewed to marketers as long as the customer is given an opportunity to prohibit disclosure.⁸⁶ This type of legislation could apply by analogy to similar products online, or this legislation could be a model for potential laws that would directly apply. There is not much difference between videos rented or purchased and web site subjects visited and viewed. Another recent development that this law might directly apply to is streaming video in cases where web sites charge users to view video clips over the Internet. Consumers assume both are private actions and the opt-out procedure used by most web sites is similar to the opt-out provision in the VPPA. These two statutes, CCPA and VPPA, imply that protection could exist under federal law, not just state tort law, for user privacy of browsing.

Next, Congress extended limited protection to personal information itself. The Children's Online Privacy Protection Act (COPPA)⁸⁷ protects children's personal information on the Internet, but not adults' personal information. This law states that anyone operating a commercial web site or online service directed

⁸⁴ 18 U.S.C. § 2710 (2003).

⁸⁵ *Id.* § 2710(b)(1).

⁸⁶ *Id.* § 2710(b)(2)(D).

⁸⁷ 15 U.S.C. § 6501 (2003).

at children under thirteen years of age, or with knowledge that such information could come from a child under thirteen, must obtain verifiable parental consent before collecting that child's information.⁸⁸ No such protections currently exist online for adult information. COPPA was enacted to protect vulnerable and impressionable children, so it is unlikely that one would succeed in arguing that such protection should extend to adults under COPPA.

Three other federal statutes extend protection to computers and information stored on them. In an attempt to protect against malicious hackers or those who propagate viruses, Congress passed the Computer Fraud and Abuse Act (CFAA).⁸⁹ The CFAA prohibits intentional unauthorized access to a computer that obtains protected information, transmits a program that causes damage, or causes damage through recklessness.⁹⁰

The Electronic Communication Privacy Act⁹¹ (ECPA) prohibits a trespasser from intercepting wire, oral or electronic communications. A trespasser is anyone other than a user, ISP,⁹² or someone with an existing contractual relationship with the operator of the computer for access to all or parts of the computer.⁹³ This means that the web site, or any marketer it contracts with for advertising, is excepted from liability under this statute since the web site itself is a user of its cookies, and a

⁸⁸ *Id.* § 6501(1), (2)(A), (4)(B), (9).

⁸⁹ 18 U.S.C. § 1030 (2003).

⁹⁰ *Id.* § 1030(a).

⁹¹ 18 U.S.C. § 2510 (2003).

⁹² *Id.* § 2510(5)(a).

⁹³ *Id.* § 2510(2)(B).

marketer would be under contract to access cookies on user computers.

The Stored Wire and Electronics Communications Act⁹⁴ (SCA) prohibits unauthorized access to stored communications in an electronic storage system.⁹⁵ Excepted from this prohibition are the ISP and users for whom the communication was intended or was made by.⁹⁶ These three laws have often been used by plaintiffs to unsuccessfully argue that cookies and other online technology employed by web sites and advertising brokers invaded their privacy by accessing the personal information on their computers.

For instance, in *In re DoubleClick*,⁹⁷ the plaintiffs' complained that advertising broker, DoubleClick, violated the ECPA,⁹⁸ the Federal Wiretap Act⁹⁹ and the CFAA.¹⁰⁰ The district court held that cookies do not count as electronic storage, and consumers are not ISPs, so the whole issue of cookies was outside the scope of the ECPA.¹⁰¹ *DoubleClick* went on to state that web sites accessing cookies cannot be an invasion under the ECPA because "web sites would commit federal felonies every time they

⁹⁴ 18 U.S.C. § 2701 (2003).

⁹⁵ *Id.* § 2701(a).

⁹⁶ *Id.* § 2701(c).

⁹⁷ 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

⁹⁸ 18 U.S.C. § 2510 et. seq. (2003).

⁹⁹ 18 U.S.C. § 2511 et. seq. (2003).

¹⁰⁰ 18 U.S.C. § 1030 et. seq. (2003).

¹⁰¹ *DoubleClick*, 154 F. Supp. 2d at 513-14.

accessed cookies on users' hard drives, regardless of whether those cookies contained any sensitive information."¹⁰²

DoubleClick was not liable under the Federal Wiretap Act, the court held, because its contract with the web sites in its affiliate network made it a party to any communications (i.e. cookies).¹⁰³ DoubleClick's interception of those cookies was not tortious under the Act because its intent was commercial activity and it did not intend to commit a tort.¹⁰⁴ The plaintiffs' claim under the CFAA was also thrown out, despite DoubleClick's admission that its practices did violate the act, because the plaintiffs did not meet the damage requirement.¹⁰⁵

The court ruled that none of the statutes were violated, recognizing that these statutes were enacted for very specific purposes: "punishing destructive hacking, preventing wiretapping for criminal or tortious purposes, [and] securing the operations of electronic communication service providers."¹⁰⁶ DoubleClick did none of these things. These statutes were not intended for protecting consumer privacy in situations where web sites have contracted with brokers to sell advertising and collect user information, and the court refused to read such intention into them.

In *Chance v. Avenue A*,¹⁰⁷ the plaintiffs claimed that advertising broker Avenue A violated the Wiretap Act, the SCA,

¹⁰² *Id.* at 513.

¹⁰³ *Id.* at 514.

¹⁰⁴ *Id.* at 519.

¹⁰⁵ *Id.*

¹⁰⁶ *DoubleClick*, 154 F. Supp. 2d at 526.

¹⁰⁷ 165 F. Supp. 2d 1153 (W.D. Wa. 2001).

and the CFAA.¹⁰⁸ The plaintiffs, Internet users who had cookies placed on their computers by Avenue A while visiting various websites, attempted to bring a class action suit against Avenue A on behalf of millions of similar Internet users whose electronic communications were monitored by the defendant's cookies. *Chance* found that because computers serve as conduits between users, web sites and marketers, they are facilities covered by the SCA.¹⁰⁹ The court held that since a user's computer was thus covered by the act, a web site was an excepted user of that computer under the Act. So, Avenue A, and other marketers with whom the web sites had consented to access of the site's cookies, was excepted under the SCA.¹¹⁰

Under the Wiretap Act, only one party's consent is necessary to rebut liability under the exception provision.¹¹¹ Since the web sites allowed Avenue A and other marketers access to the site's cookies, those sites had consented to the interception of the communication, the cookie.¹¹² As long as the interception, which falls under the exception, did not occur with tortious purpose, the exception stands. The court held that there was no evidence of such a purpose.¹¹³ These opinions deny plaintiffs relief but do not,

¹⁰⁸ *Id.* at 1155.

¹⁰⁹ *Id.* at 1161 ("modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities covered under the Act").

¹¹⁰ *Id.*

¹¹¹ *Id.* at 1162.

¹¹² *Chance*, 165 F. Supp. 2d at 1162.

¹¹³ *Id.* at 1163. *See also* *In re Intuit*, 138 F. Supp. 2d 1272 (C.D. CA 2001) (plaintiffs must allege either access or interception of communication); *In re Pharmatrak*, 220 F. Supp. 2d 4 (Mass. 2002) (plaintiffs' claim defeated by consent of defendant to placement of code on site and web monitoring activity,

however, rule out a similar case where tortious invasion of privacy is the cause of action, thus indicating state law may be a better option for plaintiffs than federal laws.

SOLUTIONS

There is a serious danger of federal programs forcibly resolving the privacy issue in a potentially undesirable way if the Internet community does not resolve the issue itself. The Defense Department was recently pressured to drop a plan under its Total Information Awareness¹¹⁴ program that would give users access to certain areas of the Internet only if they had a personal eDNA marker.¹¹⁵ These markers would be biometric identifiers, such as voice recognition, or fingerprints. If implemented, Congress could have then passed a law requiring ISPs to only provide access to authenticated users,¹¹⁶ whose movements online could then be

but finding that an individual user's computer was not a facility under SCA). See also *In re Toys R Us*, MDL No. M-00-1381 MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Ca. Oct. 9, 2001) where the court noted that the ECPA only covers communications in temporary storage, such as RAM, not permanently on hard drives as cookies are placed. Also defendants, as providers of the service, fall under the use exception.

¹¹⁴ DEPARTMENT OF DEFENSE, *DoD News: Total Information Awareness (TIA) Update* (Feb. 7, 2003), at http://www.defenselink.mil/releases/2003/b02072003_bt060-03.html.

¹¹⁵ McCullagh, *supra* note 41.

¹¹⁶ McCullagh, *supra* note 41.

tracked. The Defense Department would have turned this system over to law enforcement and intelligence agencies for operation if it had been completed.¹¹⁷ Absent such Orwellian government inventions, the task before regulators, whether the FTC or the industry itself, is to balance consumer privacy rights with the needs of marketers for information in order to stay in the business of providing the goods and services consumers want.

The first and quite possibly easiest remedy for all interested parties in the use of cookies in online profiling is the NAI principles discussed earlier, which the FTC adopted.¹¹⁸ The principles seem to provide a method that allows consumers some control over their information, but does not unduly restrict the use of cookies or the collection of online information.

One model for eliminating user data collection on individual web sites is the Universal Registration System. The system, I/CODE, was proposed during the FTC's workshops on consumer online privacy by a market research firm called Internet Profiles Corporation (I/PRO).¹¹⁹ To use the I/CODE system, Internet users log on to the universal registration site and provide I/CODE with varying personal information including demographics, lifestyle preferences, et cetera. In exchange, they receive an I/CODE identification code, which allows consumers to browse the Internet anonymously.¹²⁰ I/PRO can then use the

¹¹⁷ McCullagh, *supra* note 41.

¹¹⁸ See *supra* notes 74-75 and accompanying text.

¹¹⁹ Federal Trade Commission, *Enhancing Consumer Privacy Online*, FTC Staff Report (1996), at <http://www.ftc.gov/reports/privacy/privacy4.htm>.

¹²⁰ *Id.*

information to create consumer profiles for its clients' web sites.¹²¹ In this model, I/PRO functions as the gatekeeper to withhold all personally identifiable information from advertisers or marketers without their consent. Consumers may opt to disclose their email or physical addresses to the web site. The I/CODE system, despite providing anonymity on the web, does not meet all of the requirements of the NAI principles.¹²² Another problem is that the government cannot force web sites to contract their data collection and analysis to an outside vendor, so participation in this program would be voluntary and not universal.

Privacy seal programs, such as TRUSTe or BBBOnline, are an attempt to eliminate the false sense of security generated in a user when a site has a privacy policy. They provide assurance that a site carrying the seal at least follows a basic set of privacy policy rules in order to qualify for the seal.¹²³ However, the privacy policies are not standard among programs. Seal programs are also not universal, and only a few thousand web sites follow one of the programs, out of the millions of sites that are online.¹²⁴

Ironically, cookies themselves propose a solution to privacy issues that arise. In recent versions, browsers include an option allowing the user to set what information they will provide to specific web sites, and cookies to all other sites are blocked. With this method, the consumer would only have to state once what

¹²¹ *Id.*

¹²² See Federal Trade Commission, *supra* note 71.

¹²³ Kalinda Basho, *The Licensing of Our Personal Information: Is it a Solution to Internet Privacy?*, 88 CALIF. L. REV. 1507, 1522 (2000).

¹²⁴ *Id.* at 1523.

information they were comfortable providing and in subsequent visits, they would not be bothered by requests for information. This eliminates the problem of retail or password protected sites the user wishes to access not displaying because the user set the browser to block all cookies.

The user may also employ services and programs such as ZipLip, Anonymizer, and Zero-Knowledge. ZipLip allows users to send encrypted email for free, with the option of signing in or remaining anonymous.¹²⁵ Anonymizer lets users browse privately by connecting to its web site. It removes all identifying information, retrieves the desired sites for the user so that the user does not receive cookies and is not identified, and displays the sites on the user's browser.¹²⁶ Anyone tracking Internet use would not be able to tell what sites the user viewed. Zero-Knowledge markets a program with which users create pseudonyms assigned to different online activities and wraps email and browsing in multiple layers of encryption and re-routing.¹²⁷

Another possible solution is to provide a market for the sale of user data through the creation of a personal information licensing system.¹²⁸ The Uniform Computer Information

¹²⁵ ROSEN, *supra* note 2, at 174-77.

¹²⁶ ROSEN, *supra* note 2, at 174-77.

¹²⁷ ROSEN, *supra* note 2, at 174-77.

¹²⁸ Basho, *supra* note 123, at 1525.

Transactions Act (UCITA),¹²⁹ part of Article 2 (Sale of Goods) of the Uniform Commercial Code, was drafted to standardize electronic transactions involving information and software licenses.¹³⁰ It is broad enough in scope to allow users to license their personal information to a marketer for a period of time for a fee.¹³¹ This would require a considerable amount of consumer involvement, which is difficult to mandate, but does address most of the NAI principles.

Privacy legislation is limited to targeting specific industries collecting personal information from consumers. However, there are no laws that protect all consumers' information online.¹³² Any useful legislation must require online entities to: collect only that personal information functionally necessary to accomplish the transaction; provide consumers notice; get consumer consent for information collected beyond what is functionally necessary; provide consumers with the ability to access, delete, or correct information collected; and take reasonable security precautions to protect the collected information.¹³³ Such a law must also govern any potential transaction involving collection of personal

¹²⁹ National Conference of Commissioners on Uniform State Laws, Uniform Computer Information Transactions Act (Drafted 1999) (formerly in Article 2B of the Uniform Commercial Code).

¹³⁰ Basho, *supra* note 123, at 1530.

¹³¹ Basho, *supra* note 123, at 1530.

¹³² Major Ken Pippin, *Consumer Privacy on the Internet: It's Surfer Beware*, 47 A.F.L. REV. 125, 141 (1999).

¹³³ Lawrence Jenab, *Will the Cookie Crumble?*, 49 KAN. L. REV. 641, 664 (2001).

information, not just web sites, since ISPs and third party affiliates would also profit from disclosing information to marketers.¹³⁴

FTC officials once believed self-regulation and consumer education would be sufficient to monitor the actions of web sites.¹³⁵ It is now clear that these only provide part of the solution. As each generation becomes more proficient with technology, consumers will be at less of a disadvantage and more prepared to protect their online privacy. If self-regulation by the industry fails, then the government may step in with potentially draconian measures such as eDNA, which would be worse than the current situation.

CONCLUSION

“The architecture of cyberspace is political . . . and political choices will determine whether cyberspace embodies values that enhance privacy or values that accelerate its destruction.”¹³⁶ It is up to Internet users to inform their congressional representatives which of those values they prefer. Until recently, the government showed reluctance to interfere with the Internet, preferring the industry to regulate itself with consumer outrage creating impetus for new methods of online privacy protection. Congress was content to pass statutes tailored to specific concerns, such as children or hacking, and let the FTC make recommendations for

¹³⁴ *Id.* at 665.

¹³⁵ See Federal Trade Commission, *supra* note 71, at 5-6.

¹³⁶ ROSEN, *supra* note 2, at 168.

online businesses to consider.¹³⁷ The Patriot Act and Homeland Security Act have changed that reluctance, and now the online industry is faced with the knowledge that it must act to solve the privacy concerns or the government will take such actions out of its hands.

The new terrorism laws provide users with no greater protection of their privacy than the federal statutes designed to prevent hacking since they contain no provisions for a user safeguarding personal information from others. While privacy is a fundamental right under the Constitution,¹³⁸ federal laws give a user no way to protect that right in an online situation. State tort laws protecting privacy seem to be the best option for users, but state courts' decisions differ on their acceptance of applying tort law to the Internet.

Where industry self-regulation fails to satisfy and users are bombarded with invasive advertising, the user may feel there is no choice but to use programs or methods to completely eliminate sharing of personal information. This creates a vacuum where business and marketing, which require information on consumer habits, can no longer function. In return, the consumer loses information about products and services, and so makes fewer purchases. The cycle results in a weaker economy. The industry, therefore, must balance consumer privacy concerns with its need

¹³⁷ See Federal Trade Commission, *supra* note 71.

¹³⁸ See *supra* notes 28-30 and accompanying text.

for consumer information and exercise restraint on how much and what types of advertising it will use.

The ideal solution appears to be a combination of industry and user regulation. The online business industry needs to make providing information more palatable to consumers with incentives such as free merchandise and with policies that allow users to set what information will be collected and how it will be shared. Users choosing to accept some advertising should do their part to put pressure on the industry by only frequenting those web sites that have and comply with privacy policies and which respect the user's privacy by not advertising at the expense of that privacy. This form of self-regulation, where the dual parts of business and consumer are both involved and acting affirmatively, is the only stable and palatable alternative to government regulation.

[This page intentionally left blank]