PRIVACY LAW IN THE INTERNET ERA: NEW DEVELOPMENTS AND DIRECTIONS

By Seth Richard Lesser[1]

Reflecting the growth of the Internet itself, interest in Internet privacy issues has increased dramatically in the last year.[1] Widely-publicized reports of the manner in which some Web-based companies obtain personal information about Internet users has fueled not only a wide outpouring of press attention, but also investigations by the Federal Trade Commission[2] and state regulatory agencies, the establishment of government task-forces and industry associations, and the commencement of several private lawsuits.[3]

This article will (1) provide background for understanding the issues, (2) outline some of the governmental responses; and (3) identify legal theories that are being used or might be used to challenge covert online data collection – the practice that has caused most alarm among consumer and privacy advocates.

1. Online Technologies With Privacy Implications

    1. Monitoring Technology Used for Covert Data Collection

---

[1] Mr. Lesser is a partner with Bernstein Litowitz Berger & Grossmann LLP in the firm's New York and New Jersey offices. His practice concentrates on consumer law litigation with an increasing emphasis on privacy law and privacy issues. He is a lead counsel for plaintiffs in several of the cases discussed in this article, including the *RealNetworks*, *DoubleClick* and *Amazon/Alexa* litigations. He can be reached at seth@blbglaw.com.

Without question, the Internet privacy issue which has provoked the greatest publicity has been the capture and/or dissemination of Internet users' personal information by Web-based companies. Until recently, average Internet users, for the most part, were oblivious to a new Internet industry devoted to the collection and sale of consumers' Internet habits. Even where actual use of personal information has not occurred, the mere collection of it raises the concern that this information could be used in the future and, perhaps, in violation of several federal and state statutes and state common laws (discussed *infra*).

Although there are some technical variations, what has been occurring is most often tied to the use of "cookie" technology. Cookies are pieces of code that are placed on Web-users' computers which can inform a Web-site about information concerning the user the next time the user returns to the Web-site. For example, Web sites can provide personalized greetings, create shopping baskets and remember passwords. This use of cookies, without more, has not raised particular concerns.

Some companies, however, having been using cookies as a means of identifying particular users' computers and, possibly, the users themselves, in order to create databases or as a means of sending information back to the companies. An example that has received extensive press coverage has been the major Web advertising agency, DoubleClick.

1. ***The DoubleClick Example.*** The first time that a consumer opens a Web page which is part of DoubleClick's network, a cookie is placed on that users' computer. This contains a globally unique identifier, commonly called a GUID. As the user surfs the net thereafter and either visits Web sites that are part of DoubleClick's network or clicks on banner advertisements which DoubleClick has placed for its clients, the GUID is transmitted back to DoubleClick. This would permit DoubleClick to

compile a database of detailed information about the users, their internet surfing habits and perhaps even personalized information the users have provided to Websites. While DoubleClick has stated that it has not compiled any databases of such information, DoubleClick's technology has raised concerns that (1) in the future, the company could start compiling such information (a concern that was heightened by DoubleClick's purchase, for $ 1.7 billion, of Abacus, a company which had compiled a massive consumer database[4]) and (2) that such information is being sent back to DoubleClick (even if it is not compiled at DoubleClick) without the users' knowledge or consent. DoubleClick has acknowledged the latter fact.[5] Indeed, consumers most likely have never even visited DoubleClick's own site but instead have visited sites of companies within DoubleClick's network or clicked on banners which go to those sites. The concern of DoubleClick's practices has led to announced investigations by several state regulators[6] as well as a flurry of lawsuits by Internet users.

A related piece of Internet technology which has also received scrutiny is the manner in which information is transmitted back to Internet companies. Two prominent examples here are RealNetworks and Amazon.com's Alexa software.

2. ***The RealNetworks Example.*** Consumers downloading RealNetworks' RealJukebox software may assume it simply helps them play and electronically store music, yet this software also monitors users' music selections and sends that information to RealNetworks. During the registration process for RealJukebox, users disclose personal information included their names, mailing and email addresses. RealNetworks assigns a GUID to each copy of the software that is downloaded and links this information to the users' name and address. Hence, the information RealNetworks collects is not anonymous.

RealNetworks' actions – once publicized – led to lawsuits and state investigations.

3. ***The Amazon.com/Alexa Example.*** Alexa is a "software agent", a program that Amazon.com's wholly-owned subsidiary, Alexa, offers to Web users free of charge. What Alexa does is provide guidance to Web surfers as they go from Web site to Web site. When they click on a site that, for example, deals with sporting equipment, the program will "pop-up" and provide a list of other sporting equipment or other sites that might be of interest. However, the technology is set up in such a way that not only are the visited sites transmitted back to Amazon/Alexa but personal information which a person may have entered on a form at a Web site may also be transmitted to Amazon/Alexa – *e.g.*, names, email addresses, social security numbers – if such information happens to be embedded in the URL (i.e., uniform resource locator, or, Web address) string of a particular site. This capturing of information and disseminating it back to Amazon/Alexa has led to the filing of several lawsuits.

4. Search Engines

Few consumers realize that some search engines (or their affiliates) use monitoring technology to collect and compile search terms into profiles that are associated with individual computers' without the consumer's knowledge or consent. For example, Alta Vista, one of the most popular search engines, is part of Doubleclick's network. No lawsuits, apparently, have been filed concerning this.

B. Other Online Technologies With Privacy Implications

While "cookie" technology (broadly described) has led to the most recent press reports, there exist other online technologies, which have privacy implications:

1. Filtering Software

Generally speaking, filtering software refers to software which enables computer owners to

block access to certain sites. The most popular use of filters is the commercial sale of programs designed to limit the sites children can visit. There is also "outgoing filtering" software which prevents children from disclosing certain types of information to others on the Internet – *e.g.*, names, addresses, telephone numbers and software that can enable parents (and employers) to track and monitor Internet usage. Additionally, businesses are now beginning to purchase software that can surreptitiously monitor and track employees' e-mail or Internet use while on the job.[7] The privacy concerns raised by the use of such software have largely, to date, entailed First Amendment objections about the use of filtering software on computers in public libraries.[8] However, the increased monitoring of employee Internet usage by employers could well, in the future, lead to disagreements and, possibly, lawsuits.

2. Encryption

Encryption is one way Internet users can preserve the privacy of their Internet communications. Encryption software scrambles information so that it cannot be understood by unauthorized persons.[9]

The use of encryption was of particular concern to lawyers. Some were concerned that they had a professional duty to encrypt communications with clients to satisfy their obligation to preserve the privileged, confidential nature of these communications. The American Bar Association, however, issued an ethics opinion concluding that lawyers who send unencrypted communications to their clients do not violate the Model Rules of Professional Conduct (and state rules based on the Model Rules).[10] Most state bar associations, which have considered the issue have concluded lawyers may communicate with their clients through unencrypted email, as well.[11]

Many commercial Web sites use technology known as Secure Sockets Layer ("SSL") to

encrypt credit card information which is sent over the Internet. In essence, this occurs by breaking credit card information into small packets that are sent to a receiving site over different Internet routes so that the interception of any one of the small packets by itself would not be informative. Notwithstanding the widespread use of this technology (which, supposedly, makes the Internet credit card safe), ingenious hackers have been able to obtain consumer credit card numbers from Web sites by hacking onto those sites and obtaining the information. A recently publicized example involved the display of more than 1,000 confidential records, including credit card numbers, on the Internet because of an apparent security breach at one of Canada's largest Internet service providers, Look Communications.[12]

3. Anonymous Remailers

Anonymous remailers are email services that remove return address information from messages before sending the e-mail to the intended recipients. Although such services enhance Internet users' ability to maintain their privacy, government officials are concerned that these services could thwart law enforcement efforts.

A Georgia statute prevented residents from using anonymous remailer services was declared unconstitutional in *ACLU v. Miller*.[13] The ACLU challenged the statute that made it a crime to transmit data through a computer network anonymously or with pseudonyms. A federal court in Georgia concluded the statute imposed an impermissible content-based restriction on free speech rights. The court, applying a strict scrutiny analysis, determined that although preventing fraud was a compelling state interest, the law was not narrowly tailored to achieve that purpose.

II. Governmental Responses to Internet Privacy Concerns

A. Federal

As discussed in detail below, it appears fair to say that thus far, two of the three federal branches of government have done little to protect Internet users' privacy rights. In numerous publications, executive branch officials have announced their preference for permitting the Internet industry to develop and enforce standards for safeguarding consumer privacy.[14] Other than a statute to protect the privacy rights of children, Congress has, as yet, failed to enact any of the myriad legislative proposals relating to this issue.

1. Executive

(a) The Administration

With a 1999 Executive Order, President Clinton established an interagency Working Group on Unlawful Conduct on the Internet ("President's Working Group"). In a March 2000 report, the Working Group affirmed the federal government's commitment to promoting private sector leadership on consumer protection issues.[15]

(b) The FTC

The FTC has begun to play a prominent role in Internet Privacy. It has issued two reports to Congress these issues. In its first report, in June 1998, it concluded that "substantially greater incentives are needed to spur self regulation and ensure widespread implementation of basic privacy principles."[16] This report also recommended specific legislation to control sites' collection and use of information from children.

In a second report, submitted to Congress in July 1999, the FTC acknowledged that the vast

majority of Web sites had not implemented its fair information practice principles, which, among other things, recommend that businesses provide consumers with notice of their data collection practices and the opportunity to choose whether and how their information may be used.[17]

The FTC has taken the following actions as well:

- On November 8, 1999, it convened a public workshop on the issue of online profiling by companies using monitoring technologies like those described above.[18]
- It permits consumers to file complaints online and reportedly receives 1,000 complaints each week.[19]
- It created a special site, www.consumer.gov to provide information about how consumers can protect their privacy on and off the Internet.
- Doubleclick, Amazon.com, HealthCentral.com, and Ivillage.com reportedly are all being investigated by the FTC regarding their use of customer data.[20]

2. Legislative Developments

Even prior to the recent spate of publicity over privacy issues, Congress has passed several laws involving specific areas of privacy and the Internet.

(a) Children's Online Protection Act of 1998

The Children's Online Protection Act of 1998 requires operators of Web sites directed to children under 13 to: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide parents the ability to review the personal

information collected from their children; (4) provide parents the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

The Act does not explicitly provide for private civil actions; it is enforceable by the FTC or state attorneys general.

In October 1999, the FTC issued a final rule, effective April 2000, implementing this Act. The FTC's role creates a safe harbor for industry groups engaged in self regulation.

(b) Cable Communications Policy Act

The Cable Communications Policy Act of 1984 ("Cable Act") includes provisions protecting the privacy of cable subscribers. Specifically, it requires cable operators to provide written notice that "clearly and conspicuously" informs consumers of the nature of personally identifiable information that will be collected and the way in which the operator intends to use such information.[21] The Cable Act prohibits service providers from disclosing personally identifiable information without first obtaining subscriber consent, subject to certain exceptions. Cable operators may disclose personally identifiable information if the disclosure is: (1) necessary to the performance of a business activity relating to cable or other service supplied by the provider; (2) required by a court order; or (3) the provider has first given the subscriber the opportunity to prohibit or limit disclosure and the disclosure does not reveal, directly or indirectly, the extent of any viewing or other use of the cable service or the nature of any

transaction made by the subscriber over the cable system.[22] Courts may award statutory damages of $100 per day for each day of the violation or $1000 whichever is higher, as well as punitive damages, and attorneys' fees.[23]

Now that cable companies often provide Internet access it is unclear whether Internet users will be able to take advantage of these privacy protections. Two courts have acknowledged the potential conflict between the Cable Act and the Electronic Communications Privacy Act ("ECPA") (discussed *infra*), which governs disclosures by Internet service providers, but neither court decided whether cable/Internet service providers must provide their Internet customers with the same type of privacy protections they are required to provide to their cable customers.[24]

(c) Legislative Proposals

The recent increased publicity over Internet privacy issues has led to a series of legislative proposals which are now pending. The following is a partial list of proposals relating to Internet privacy that have been put forward in the 106th Congress: Consumer Internet Privacy Protection Act, H.R. 313; Personal Data Privacy Act of 1999, H.R. 2644; Online Privacy Protection Act, S. 809; Electronic Rights for the 21st Century Act, S. 854.

2. State

1. New Laws

Virginia, Georgia, and West Virginia all have laws prohibiting the use of computers or computer networks to examine personal information without authorization.[25]

2. Significant Cases

Significant legislation by state governments on Internet issues may be chilled, however, by

several cases that invalidated state attempts to regulate the Internet under the Commerce Clause.[26] In *American Ass'n v. Pataki,* for example, the court held a state statute prohibiting use of the Internet to distribute material that would be harmful to minors violated the Commerce Clause because the Internet is one of those areas of commerce that "must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether."[27] The state did not appeal this decision.

The 10th Circuit, relying on the *Pataki* analysis, reached the same conclusion in its evaluation of a similar New Mexico substitute. *ACLU v. Johnson,* 194 F.3d 1149 (10th Cir. 1999), relying on the analysis in the *Pataki* case.

3. Industry Response

The recent publicity has also caused heightened activity in the private sector. Some Web-based groups have addressed Internet privacy by offering such certification programs, a well-known one of which is Truste, which puts a seal on sites that agree to comply with certain privacy protection principles. Other new efforts include the Better Business Bureau's online division, BBBOnline, which is taking steps to move self regulation efforts forward. With the assistance of industry, consumer and government representatives, BBBOnline is developing a voluntary code to provide online merchants with guidelines for protecting data privacy and implementing other consumer protections.

III. SUBSTANTIVE LEGAL THEORIES FOR CHALLENGING COVERT ONLINE DATA COLLECTION

The law involving Internet privacy is still in its infancy. In the lawsuits that have thus far been filed various causes of action have been asserted, and in other lawsuits that may hereafter be brought, additional causes of action may be employed.

A. Federal Statutes

Three other statutory provisions are being principally employed in the lawsuits thus far brought:

1. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act 18 U.S.C. 1030 ("CFAA") was originally enacted in 1984, as part of the Crime Control Act. It was the first law to address computer crime with a specific statute.[28] In 1990, Congress amended it "to cover all computers used in interstate commerce or communications" and "to prohibit forms of computer abuse which arise in connection with, and have a significant effect upon, interstate or foreign commerce."[29]

(1) Substantive Provisions

The following CFAA provisions could be used to challenge conduct that might be considered online privacy violations:

Subsection (a)(2)(c)

> Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication . . . shall be punished;[30] or

Subsection (a)(5)(A)

> Whoever . . . knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct intentionally causes damage without authorization, to a protected

computer . . . shall be punished; or

Subsection (a)(5)(C)

Whoever . . . intentionally accesses a protected computer without authorization, and as a result of such conduct causes damage . . . shall be punished.

The phrase "protected computer," which is used in each of the above sections, is defined by CFAA to include **any** computer used in interstate commerce or communication.[31] As used in subsections (a)(5)(A) and (a)(5)(C), the term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information, that (A) causes loss aggregating at least $5000 in value during any 1-year period to one or more individuals." Thus, plaintiffs bringing claims under these two subsection (a)(5)(A) or (a)(5)(C) must prove that defendants' unauthorized transmission of a program, code, or command or access to their computers caused losses of at least $5,000. By contrast, plaintiffs alleging a violation of subsection (a)(2)(C) have no such requirement. Instead, plaintiffs need only prove that defendant obtained unauthorized access to plaintiffs' computers and used that access to obtain information.

(b) Cases Under The CFAA

In one of the few reported decisions under the CFAA that involved a defendant accused of inappropriately obtaining information from non-governmental computers, America Online ("AOL") successfully used CFAA § 1030 (a)(2)(C) against a company that had obtained an AOL account and then used that account to extract information about AOL members which it thereafter used to send a significant amount of unsolicited email messages to AOL members.[32]

The CFAA has also been asserted in the primary Internet privacy class actions, those discussed *supra*.

3. Relief

Compensatory damages, injunctions and other equitable remedies are available under CFAA.[33] Plaintiffs bringing claims pursuant to Subsections (a)(5)(A) and (a)(5)(C) are entitled to receive only economic damages.

2. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA), an amendment to the federal wiretapping statute, is the primary federal legal protection against the unauthorized interception, use or disclosure of electronic communications while in transit or in storage.[34] It has two substantive provisions that may apply in Internet privacy litigation – its prohibition on illegal interceptions of electronic communications and its prohibition on illegal access to stored electronic communications.

(a) Illegal Interceptions of Electronic Communications

(i) Substantive Provisions

The following ECPA provisions could be used to challenge conduct that might be considered online privacy violations:

Subsection 2511(1)(a)

> [A]ny person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished . . . or subject to suit.

Subsection 2511(1)(c)

> [A]ny person who intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection . . . shall be punished . . . or subject to suit.

Subsection 2511(1)(d)

> [A]ny person who intentionally uses, or endeavors to us, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection . . . shall be punished . . . or subject to suit.

Private plaintiffs bringing interception-based ECPA claims must prove that defendants intentionally intercepted plaintiffs' electronic communications.[35] Disgruntled consumers seeking relief from surreptitious online profiling could allege that defendant Web sites use cookies the way traditional spies use "bugs." Web sites plant cookies on consumers' computers and these cookies monitor consumer Internet behavior by intercepting communications between consumers' computers and other Web sites and/or obtaining access to temporarily stored communications between consumers' computers and other Web sites.

ECPA also includes an express exemption for interceptions made with the consent of one of the parties to the communication, a provision which might be argued to be an affirmative defense to an invasion claim:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a[n] . . . 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 interception is 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.[36]

In asserting this provision as an affirmative defense to an interception claim, it would appear that the question of "consent" could well involve what, if anything, has been set forth in an Internet company's disclosures about its practices and whether, in fact, its disclosures were sufficiently clear so that meaningful consent had actually been obtained. In the Amazon/Alexa private litigation, for instance, defendants' first substantive response to plaintiffs' claims (an opposition to class certification), Amazon/Alexa has taken the position that defendants' Privacy Policy and Frequently Asked Questions put (at least some) users of the Alexa software on notice as to what Alexa did and thus, implicitly, caused them to consent. Plaintiffs, not surprisingly, are challenging (a) the quality of the disclosure – *i.e.*, that it did not actually inform users what information was being transmitted to the company -- and the manner in which this alleged consent was obtained – *i.e.*, that a vague statement does not constitute valid consent and (c) that, in any event, Amazon cannot point to any actual manifestation of an understanding "prior consent."

(2) Relief

This section of ECPA authorizes injunctions, damages (including punitive damages in appropriate cases), and attorneys' fees. [37] Prevailing plaintiffs may receive the greater of (a) the sum of actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation or (b) statutory damages of either $100 dollars a day for each day of violation or $10,000. [38]

2. Illegal Access to Stored Electronic Communications

(2) Substantive Provisions

The following ECPA provisions could be used to challenge conduct that might be considered online privacy violations:

Section 2701(a)

> Whoever intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to a[n] electronic communication while it is in electronic storage in such system shall be punished.

To prevail on a storage-based ECPA claim, plaintiffs must prove defendants intentionally obtained access to "a facility through which an electronic communication service is provided" without or in excess of authorization, and thereby obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it is in storage in such system."[39] The phrase "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[40] Thus, to use storage-based ECPA claims to seek

redress for online profiling activities, counsel must argue that a plaintiff's personal computer is a "facility through which an electronic communication service is provided."

As under the illegal interceptions of electronic communications provisions of the ECPA, the issue of what constitutes use "in excess of authority" can be expected to be litigated. Again, this issue is dividing the two sides in the Amazon litigation for the reasons described *supra*.

(3) Relief

Courts are authorized to award injunctive relief, punitive damages ,attorneys' fees, and for violations of ECPA's stored communications' provisions. [41] Prevailing plaintiffs may receive an award of "the sum of actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall the violator recover less than the sum of $1000."

B. State Statutes

3. State Anti-Wiretapping and Anti-Hacker Laws

Several states have enacted statutes similar to ECPA and CFAA[42] Counsel should examine state anti-wiretapping and/or anti-hacking laws in order to determine whether any variances between federal and state versions could provide additional relief.

2. Consumer Fraud Statutes

(1) Substantive Provisions

Every state has a statute that, like the Federal Trade Commission Act, protects consumers from deceptive and unfair trade practices.[43] Unlike the FTC Act, however, many of these statutes permit private actions.[44] Moreover, some of these statutes also permit successful plaintiffs to recover attorneys' fees and punitive, treble, or minimum damage awards.[45]

At least one court found that an offline practice similar to surreptitious online profiling violated a state consumer fraud law. *Dwyer v. Amer. Express Co.*, 273 Ill. App.3d 742 (1st Dist. 1995). In *Dwyer*, an Illinois court concluded that the failure of a credit card company to inform card holders that their spending habits would be analyzed and their names sold to advertisers constituted a deceptive practice under the Illinois Consumer Fraud Statute. There, the court noted that:

> It is highly possible that some customers would have refrained from using the American Express Card if they had known that defendants were analyzing their spending habits. . . . Defendants had a strong incentive to keep their practice a secret because disclosure would have resulted in fewer cardholders using their card.[46]

(b) Relief

Statutory Damages – Approximately half of the state consumer fraud statutes permit prevailing plaintiffs to obtain minimum damage awards ranging from $25 to $5000, even if actual damages cannot be proved.[47] Other states, particularly California, provide for equitable restitution of the amounts that the defendant may have received from its allegedly wrongful acts.[48]

Actual Damages – Other states provide for actual damages or damages to compensate for plaintiff's "ascertainable loss."[49] Under Connecticut's consumer fraud statute, for example, plaintiffs can establish ascertainable loss by proving "only that he has purchased an item partially as a result of an unfair or deceptive practice or act and that the item is different from that for which he bargained."[50] The applicability of such a standard to an Internet privacy case is unclear.

Multiple and/or Punitive Damages – Half of the state consumer fraud statutes authorize treble or other multiple damage awards under specified conditions. Ten consumer fraud statutes

explicitly authorize punitive damages.[51]

Injunctions – Most consumer fraud statutes expressly authorize private injunctive relief.[52]

Attorneys' Fees – Virtually all consumer fraud statutes which authorize private remedies, also authorize attorneys' fees.[53]

3. State Anti-Stalking Laws

Yahoo, an Internet portal that uses cookie technology to monitor consumers' Internet usage, is the defendant in a class action suit filed in January, 2000, which accuses it of violating Texas' Anti-Stalking Statute. The operative term in the statute, "harassing behavior" is defined to mean "conduct by the defendant directed specifically toward the claimant, including following the claimant, that is reasonably likely to harass, annoy, alarm, abuse, torment, or embarrass the claimant." [54] In addition to proving that a defendant engaged in "harassing behavior" on more than one occasion, a plaintiff must prove, among other things, that defendant's conduct created reasonable fears about safety and that plaintiff demanded that defendant end the harassing behavior. [55]

C. State Common Law Theories

1. Trespass to Chattel/Personal Property

Trespass to chattel claims have been used successfully against hackers and spammers, i.e., those who distribute massive quantities of unsolicited email.[56] This common law tort, recognized in the Restatement of Torts, prohibits the unauthorized use or interference with plaintiffs' personal property. [57] Several courts have concluded that electronic signals sent between computers are sufficiently tangible to support the trespass tort. [58] An actionable trespass occurs even in situations where, although there is no physical harm to plaintiffs' property, defendants' intrusion injures an intangible, but protectable interest,

such as business goodwill.[59]

Trespass claims are also permitted in instances where a defendant's actions exceeded its authorization to use plaintiff's property. For example, a federal court in California concluded that Hotmail Corporation was likely to prevail on the merits of its claim that defendants' use of their authorized Hotmail accounts to send spam in violation of Hotmail's official policies constituted an actionable trespass to Hotmail's chattel.[60]

2. Invasion of Privacy

Although some states have statutory privacy protections,[61] most have adopted one or more of the following four common law tort doctrines: (1) misappropriation, (2) public disclosure of private facts,(3) intrusion on seclusion, (4) false light.[62] The first three, which do not require plaintiffs to prove that improperly disclosed information is false, appear to be the best vehicles for plaintiffs complaining about online profiling or other possible invasions of privacy which result in the disclosure and use of truthful personal information.

(a) Misappropriation

Plaintiffs bringing misappropriation claims typically must establish that (i) defendants appropriated plaintiff's likeness or name for the value associated with it and not for any newsworthy purpose, (ii) the plaintiff can be identified by the publication, and (iii) some advantage or benefit accrued to the defendant.[63]

The misappropriation doctrine safeguards individuals' interests in the exclusive use of their identities. Under this theory, privacy interests are akin to other types of intangible property interests.[64] Although some courts preclude non-celebrity plaintiffs from taking advantage of the misappropriation

doctrine,[65] others permit ordinary people to recover when their names or likenesses have been put to commercial use without their permission.[66]

Companies that buy, sell, rent or use lists of consumers' names, addresses, and purchasing preferences have shielded themselves from misappropriation claims by relying on two decisions – *Shibley v. Time, Inc.* and *Dwyer v. Amer. Express.*[67] In both cases, courts rejected plaintiffs' privacy claims, in part, by referring to state statutes that authorize motor vehicle departments to sell similar information.[68] This rationale, however, may be unavailable to defendants in Internet privacy suits. In 1994, Congress enacted the Driver's Privacy Protection Act, a statute which restricts states' ability to disclose drivers' personal information without their consent.[69] The Supreme Court upheld the constitutionality of this Act, *Reno v. Condon*, No. 98-1464, decided on January 12, 2000.

A recent Massachusetts decision could represent indicate that some courts are willing to protect consumers from intrusive marketing schemes, *Weld v. CVS Pharmacy, Inc.*[70] In *Weld*, plaintiffs challenged a marketing scheme between CVS, a drug store chain, and several pharmaceutical manufacturers. CVS maintained a database of customer information that it used to send mailers to remind customers to refill prescriptions, provide information about new drugs, or encourage customers to discuss potential medical conditions with their doctors. CVS claimed that it employed a technical, impersonal means to develop a list of customers who would receive a particular flier. A list of the designated customers' names, addresses and dates of birth would then be compiled on a diskette and given to a manufacturer. CVS customers were never informed of, or asked to provide consent for, this program.

The Massachusetts court denied defendants' motion for summary judgment on plaintiffs'

statutory privacy claim (which the court concluded was likely to be identical to plaintiffs' common law claim for tortious misappropriation of plaintiffs' private information). Significantly, the court rejected defendants' argument that, as a matter of law, the disclosure of plaintiffs' name, address and date of birth could not constitute a violation of plaintiffs' privacy rights.[71]

(b) Public Disclosure of Private Facts

Under this theory, plaintiffs must establish (a) that a defendant publicized private facts about plaintiff to the general public, (b) the facts did not concern a matter of legitimate public concern, and (c) this disclosure would be highly offensive to the reasonable person.[72]

To prevail on this claim, plaintiffs must prove defendants publicized **private** facts. In other words, the facts must not already be in the public domain. The Restatement of Torts specifies that examples of public records for which there can be no liability for publication include birthdate, marital status, military record, professional or occupational licenses, and litigation, unless such information is not open to public inspection (e.g., tax records).[73] In one of the few Supreme Court discussions of this common law tort, the Supreme Court rejected an assertion of this claim by a rape victim whose name was broadcast on the ground that her name was part of the public record because it had been included in a police report inadvertently made available to the media.[74]

To be actionable, defendants' publication of plaintiff's private facts must be highly offensive to a reasonable person. Mundane facts one would rather keep quiet will not give rise to an actionable claim, as explained in comments to the Restatement (Second) of Torts:

> Complete privacy does not exist in this world except in a desert, and anyone who is not a hermit must expect and endure the ordinary incidents of the community life of which he

> is a part. Thus, he must expect the more or less casual observation of his neighbors as to what he does, and that his comings and goings and his ordinary daily activities . . . The ordinary reasonable man does not take offense at a report in a newspaper that he has returned from a visit, gone camping in the woods or given a party at his house for his friends.[75]

For example, in *Grunseth v. Marriott Corp.*, the court rejected plaintiff's claim that a hotel's release of a receipt that corroborated a report that plaintiff had a "liaison" with a woman in that hotel, constituted an invasion of his privacy.[76]

In addition, plaintiffs must prove wide publication of the private facts.[77] Limited disclosure to a small group (or an Internet company's marketing partners) would probably not be actionable.[78]

(c) Intrusion Upon Seclusion

An intrusion upon seclusion claim requires that a plaintiff to prove that a defendant intruded upon the plaintiff's solitude or private affairs and that reasonable people would find this type of intrusion highly offensive.[79] Significantly, this tort does not require that defendant to prove the disclosure of private facts; plaintiff need only prove that defendant intentionally interfered with plaintiff's private affairs.[80]

The intrusion need not be a physical one to be actionable; plaintiffs may recover where defendants use mechanical aids to obtain information about plaintiff's private affairs.[81] Actionable conduct, for example, can include tapping telephone wires, opening private mail, searching a wallet, examining a bank account.[82] Courts have prevented plaintiffs from recovering under this theory if the underlying information is contained in a public record.[83] Although, as a general rule, there can be no

liability under this doctrine if plaintiff is observed (or otherwise intruded upon) in a public place, this general rule is not without exceptions. The Restatement gives the following example: "[T]here may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze and there may still be an invasion of privacy when there is intrusion in these matters."[84]

Since this claim requires intrusion into matters that are private, success in an Internet privacy situation may depend upon whether a plaintiff or class of plaintiffs can establish that a defendant's activities intruded on Internet usage that in some way relates to confidential matters, *e.g.*, health issues. Plaintiffs bringing such claims must not only establish that the intrusion involved matters that are not already those of public record, but also that the defendant used private, not public or employer-owned computers.

D. State Constitutional Protections (California)

California provides a specifically strong form of privacy protection that may play a role in future Internet privacy cases. California's constitution protects individuals against intrusions on their privacy whether such intrusions are committed by governmental entities or private businesses.[85] Cal. Const. Art I, sec. 1. An express right to privacy was added to California's constitution for the express purpose of protecting individuals from "the overbroad collection and retention of unnecessary personal information by government and business interests."[86]

In a 1994 opinion, the California Supreme Court set forth the standard for asserting a claim for invasion of privacy. *Hill v. National Collegiate Athletic Ass'n.*[87] To bring a claim for violation of the California constitutional right of privacy, plaintiffs must establish: (1) a legally protected privacy interest; (2) reasonable expectation of privacy in the circumstances; and (3) conduct by defendant that

constituted a serious invasion of privacy.

In California, an individual's interest in preventing a defendant from disseminating or misusing sensitive and confidential information is a legally protectable interest.[88]

Evaluation of whether a plaintiff has a reasonable expectation of privacy involves an examination of "customs, practices, and physical settings surrounding particular activities." These factors may tend to create or inhibit reasonable expectations of privacy. [89] Whether an individual had an opportunity to consent voluntarily to activities impacting privacy also affects a court's evaluation of this factor.[90]

Plaintiffs must also prove that a defendant's invasion was serious. "No community could function if every intrusion into the realm of private action, no matter how slight or trivial gave rise to a cause of action for invasion of privacy. . . Actionable invasions must be sufficiently serious in nature, scope and actual or potential impact to constitute an egregious breach of social norms underlying the privacy right."[91]

IV. FOREIGN DEVELOPMENTS

Note should be taken as to how the American legal structure differs from that in other countries. The European Union and Canada have both done more to protect Internet users' privacy than the United States. In 1995, the European Union adopted a directive requiring member countries to collect personal data only for a "specified, explicit and legitimate purpose" and only if the person to whom the information refers "has unambiguously given his consent."[92] Similarly, in April 2000, the Canadian House of Commons passed an act that will prohibit organizations from collecting, using, or disclosing personal information without the consent of the individual.[93]

ENDNOTES

1. *See, e.g., Battling Cookie Monsters*, NY Times, February 24, 2000; *Privacy: Outrage on the Web*, Business Week, February 14, 2000.

2. Yahoo and Doubleclick are reportedly being investigated by the FTC.

3. The author of this article is counsel for plaintiffs in three cases challenging covert online data collection practices, *Supnick v. Amazon*, Inc., No C00-0221P (W.D. Wash.), *Healy v. Doubleclick, Inc.*, Civ 0641 (S.D.N.Y.), and *Bell v. RealNetworks, Inc.* (W.D. Washin., MDL, N.D. Ill.)

4. On November 23, 1999, Doubleclick completed its merger with Abacus Direct Corporation ("Abacus"). According to Doubleclick's privacy policy (4/13/00), Abacus is now a division of Doubleclick and it is developing an online division that will maintain a database of personally-identifiable information about Internet users.

5. In its Form 10-K/A (Amendment 2), December 31, 1998, Doubleclick made the following concession under the heading "Privacy Concerns": "Web sites usually place certain information ("cookies") on a user's hard drive usually without the user's knowledge or consent. Web sites use cookies for a variety of reasons. Our DART technology uses cookies to limit the frequency with which the browser is shown a particular ad. Certain currently available Internet browsers allow users to modify their browser settings to remove cookies at any time or to prevent cookies from being stored on their hard drive. In addition, some Internet commentators, privacy advocates and governmental bodies have suggested limiting or eliminating the use of cookies. The effectiveness of our DART technology could be limited by any reduction or limitation in the use of cookies."

6. Tamara Chung, "*Privacy on the Web Rising Concern*," Wilmington News Journal, March 3, 2000 (reporting that attorney generals in New York and Michigan have instituted investigations of Doubleclick's practices).

7. Jeffrey S. Klein and Nicholas J. Pappas, *Monitoring Internet Use in the Workplace*, New York Law Journal, February 7, 2000; *Watchdog Oversees Employee Web Use*, Law Technology Product News, Vol. 5, No. 4, April 1998 (announcing release of Internet Watchdog, software that allows employers providing networked work environments to monitor and record all Internet activities by their employees).

8. The ACLU challenged the use of filtering software by a Virginia public library in *Mainstream Loudoun v. Bd. of Trustees of Loudoun County Library*, 24 F. Supp.2d 552 (E.D. Va. 1998) (granting plaintiffs' motion for summary judgment because library's policy of using filtering software to block access to certain sites was a content-based restriction on speech that was not narrowly tailored to

serve library's interest in restricting children's access to "obscene material").

9. ABA, Facts About Privacy and Cyberspace (2000).

10. ABA Standing Committee on Ethics and Prof. Responsibility, Formal Op. 99-413 (March 10, 1999).

11. *See, e.g.*, Alaska Bar Ass'n, Op. 98-2 (Jan. 1998); Mass. Op. 2000-1 (Jan. 2000).

12. *Credit Card Files Turn Up on the Internet*, Toronto Star, April 11, 2000.

13. *ACLU v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997).

14. The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, A Report of the President's Working Group on Unlawful Conduct on the Internet, March 2000; Self-Regulation and Privacy Online, A Report to Congress, Federal Trade Commission, July 1999; Privacy Online: A Report to Congress, Federal Trade Commission, June 1998.

15. The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, A Report of the President's Working Group on Unlawful Conduct on the Internet, March 2000.

16. Privacy Online: A Report to Congress, Federal Trade Commissioner, June 1998 ("1998 Report")

17. Self Regulation and Privacy Online: A Report to Congress, Federal Trade Commission, July 1999 ("1999 Report")

18. U.S. Dep't of Commerce and Federal Trade Commission, Public Workshop on Online Profiling, November 8, 1999.

19. *See* Report of President's Working Group.

20. *See* As *FTC Rides Herd on the Web, Marketers Begin to Circle the Wagons*, Wall St. J., February 29, 2000; Rick Whiting, *Mind Your Business*, Information Week, March 6, 2000.

21. 47 U.S.C. § 551(1)(A).

22. 47 U.S.C. § 551.

23. 47 U.S.C. 551 (f)(2).

24. *See U.S. v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000) (subscriber information divulged by a cable/Internet service company would not be suppressed because neither the Cable Act nor the ECPA authorize suppression); *In re Application U.S.*, 36 F. Supp. 2d 430 (D. Mass. 1999) (government

application for disclosure of information regarding cable/Internet company's customer would be granted despite conflicting obligations imposed under the Cable Act and ECPA).

25. Va. St. Ann. 18.2-152.5 ("A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person"); Ga-St. 16-9-93(c) (same); W.Va. St. Ann. 61-3C-12 (same).

26. *American Ass'n v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997); *Cyberspace Communications v. Engler*, No. 99-73150 (E.D.Mich. 1999) (preliminarily enjoining law banning the distribution of sexually explicit materials to minors over the Internet as a violation of the Commerce Clause and the First Amendment); *ACLU v. Johnson*, 4 F. Supp.2d 1029 (D. N.M. 1998), *aff'd*, 194 F.3d 1149 (10th Cir. 1999). *But see Hatch v. Superior Ct.*, 2000 WL 337527 (Cal. Ct. App. March 31, 2000) (concluding California statute did not violate Commerce Clause because statute, which does not impose punishment for conduct outside of California, would not result in extraterritorial enforcement that could burden interstate commerce).

27. 969 F. Supp. at 169.

28. S. Rep. 101-544 (1990).

29. S. Rep. 101-544.

30. 18 U.S.C. §1030(a)(2) (C).

31. 18 U.S.C. §1030 (e)(2).

32. *AOL v. LCGM, Inc.*, (E.D. Va. 1998) (granting summary judgment for AOL on CFAA claim).

33. 18 U.S.C. 1030(e)(8).

34. 18 U.S.C. §§ 2511, 2701.

35. 18 U.S.C. § 2511(1)(a).

36. 18 U.S.C. §2511(2)(d).

37. 18 U.S.C. §2520(b).

38. 18 U.S.C. §2520(c)(2).

39. 18 U.S.C. §2701(a).

40. 18 U.S.C. §2510(15).

41. 18 U.S.C. §2707(b)(1), (3) and (c).

42. *See, e.g.*, Fla. Stat. §934.03 (mirrors 18 U.S.C. 2511); Tex. Penal Code §16.02 (same); Il. St. Ch. 720, 6/16D-3 (criminalizing computer tampering).

43. *See, e.g.*, N.Y. Gen. Bus. Law §349 *et seq*.

44.*See, e.g*, Ala. Code 8-19-1; Cal. Civ. Code §1750; N.M. Stat. Ann. §57-12-1; Va. Code §59.-196; Wash. Rev. Code 19.86 *et seq*.

45. *See, e.g.*, N.M. Stat. Ann. §57-12-1 ($100 minimum damages; $300 minium damages or treble damages for willful violations; mandatory attorneys' fees to prevailing consumer); Va. Code 59.196 (actual damages or $500, whichever is greater; treble damages for willful violations or $1000, whichever is greater; attorneys' fees); Wash. Rev. Code Ann. §19.86 *et seq.* (attorneys' fees, treble damages at court's discretion).

46. *Dwyer v. Amer. Express, Inc.*, 652 N.E.2d 1351 (Ill. App. Ct. 1995).

47. National Consumer Law Center, *Unfair and Deceptive Acts and Practices* (hereinafter "*Unfair and Deceptive Acts*") § 8.4.1.1 (4th Ed. 1997); *see also*, N.M. Stat. Ann. 57-12-1 ($100 minimum damages; $300 minium damages or treble damages for willful violations; mandatory attorneys' fees to prevailing consumer); Va. Code 59.196 (actual damages or $500, whichever is greater; treble damages for willful violations or $1000, whichever is greater; attorneys' fees); Wash. Rev. Code Ann. 19.86 *et seq.* (attorneys' fees, treble damages at court's discretion).

48. Cal. Bus. & Prof. Code §17200 *et seq*.

49. *See, e.g., Hinchliffe v. Amer. Motors Corp.*, 440 A.2d 810 (Ct. 1981).

50. *Id.* at 814.

51. *Unfair and Deceptive Acts* § 8.4.3.2.

52. *Unfair and Deceptive Acts* §8.6.1.

53. *Unfair and Deceptive Acts* §8.8.2.1; *see, e.g.*, N.M. Stat. Ann. §57-12-1 ($100 minimum damages; $300 minium damages or treble damages for willful violations; mandatory attorneys' fees to prevailing consumer); Va. Code 59.196 (actual damages or $500, whichever is greater; treble damages for willful violations or $1000, whichever is greater; attorneys' fees); Wash. Rev. Code Ann. §19.86 *et seq.* (attorneys' fees, treble damages at court's discretion).

54. Vernon's TX. Civ. Prac. and Remedies, Liability for Stalking, §85.001.

55. *Id.* at 85.003.

56. *America Online, Inc. v. IMS*, 24 F. Supp.2d 548 (E.D. Va. 1998) (concluding that a marketing company which sent 60 million unauthorized electronic mail advertisements committed trespass to chattel against AOL's computer network); *Compuserve v. Cyber Promotions*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (collecting cases)

57. *See, e.g.*, Rest. (Second) of Torts 217(b).

58. *Compuserve v. Cyber Promotions*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (collecting cases); *Thrifty Tel v. Bezenek*, 46 Cal. App. 4th 1559, 1567 (1996) (parents of teen who gained access to long distance companies' computers and confidential codes and then made calls without paying for them could be found liable for trespass to chattel).

59. *AOL*, 24 F. Supp.2d at 550 (spam injured AOL diminishing its "reservoir of goodwill and its possessory interest in its computer network"); *Compuserve*, 962 F. Supp. at 1022-23 (by intruding into Compuserve's computer systems to send unwanted email to Compuserve's customers, defendants harmed Compuserve's business reputation).

60. *Hotmail Corp. v. Vans Money Pie, Inc.*, 1998 WL 388389, *7 (N.D. Cal. 1998) (granting plaintiff's motion for preliminary injunction on trespass to chattel and CFAA claims, among others).

61. *See, e.g.*, Mass. G.L. c. 214, 1B ("a person shall have a right against unreasonable, substantial or serious interference with privacy.").

62. Restatement (Second) of Torts 652A.

63. Restatement (Second) of Torts, 652C.

64. Restatement (Second) of Torts 652C, comment a.

65. *See, e.g., Reeves v. Fox Television Network*, 983 F. Supp. 703 (N.D. Ohio) (prohibiting recovery on misappropriation claim by plaintiff whose arrest was broadcast because there was no evidence that plaintiff's name or likeness had any intrinsic value).

66. *See, e.g., Staruski v. Continental Telephone Co.*, 581 A.2d 266 (Vt. 1990).

67. *See, e.g., Shibley v. Time, Inc.*, 341 N.E.2d 337 (Ohio Ct. App. 1975) (concluding that a magazine publisher which sold subscription lists to direct mail advertisers without the consent of individual subscribers did not violate the subscribers' rights of privacy) and *Dwyer v. Amer. Express*, 652 N.E.2d 1351 (Ill. App. Ct. 1995) (credit card companies disclosure of lists of card holder names, categorized by purchasing patterns, did not violate card holders' privacy rights).

68. *Shibley*, 341 N.E.2d at 339; *Dwyer*, 652 N.E.2d at 1355 (citing *Shibley*).

69. 18 U.S.C. §§2721-2725.

70. 1999 WL 494114 (Mass. Superior Ct. June 29, 1999).

71. *Weld*, 1999 WL 494114 at *3-4, n. 13. In denying defendants' motion for summary judgment, the court did not repudiate the rationale of *Shibley v. Time* and *Dwyer v. American Express*. Instead, the court distinguished the CVS case by noting that "[i]ndividuals arguably posses a greater expectation of privacy as to the use of their names in connection with their prescription and medical information than in connection with an individual's spending and reading habits." *Weld*, 1999 WL 494114 at *6 n. 18.

72. Restatement of Torts 652D

73. Restatement (Second) of Torts 652D, comment b.

74. *Cox Broadcasting v. Cohn*, 420 U.S. 469 (1975).

75. Restatement (Second) of Torts 652D, comments.

76. *Grunseth v. Marriott Corp., d/b/a J.W. Marriott Hotel*, 79 F.3d 169 (D.C. Cir. 1996) (unpublished opinion).

77. Restatement (Second) of Torts, 652D., cmt. a.

78. Restatement (Second) of Torts 652B, comment a; *see also, Tureen v. Equifax, Inc.*, 571 F.2d 411 (8th Cir. 1978) (consumer reporting firm's disclosure of plaintiff's past insurance history to one of its clients did not constitute sufficient disclosure to general public to support an invasion of privacy claim).

79. *See* Restatement (Second) of Torts 652B.

80. Restatement (Second) of Torts 652B, comment a; *see also, Medical Lab. Management Consultants v. ABC*, 30 F. Supp. 1182 (plaintiffs can recover on intrusion claim only if expectation of seclusion in the place, conversation or data source is reasonable).

81. Restatement (Second) of Torts 652B, comment b.

82. Restatement (Second) of Torts 652B, comment b.

83. Restatement (Second) of Torts 652B, cmt. b; *Dwyer*, 652 N.E.2d at 1354 ("We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation").

84. Restatement (Second) of Torts 652B, comment c.

85. States with constitutional protections for privacy rights tend to protect such rights against government, not private, intrusions. *See, e.g., Hart v. Seven Resorts, Inc.*, 947 P.2d 846 (1997) (Arizona's constitutional right to privacy does not restrict private individual actors); *Roe v. Quality Transp. Services*, 838 P.2d 128 (Wash. App. Div. 1992) (same).

86. *Hill*, 7 Cal.4th 1, 17-18 (1994).

87. *Id.*

88. *Id*. at 35.

89. *Id*. at 36.

90. *Id*. at 37.

91. *Id.* at 37.

92. Directive 94/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

93. AP Online, Canada's News Briefs, April 4, 2000.