Footprints in Cyberspace: Using Transactional Data to Target Advertising

by Laura D. Ravine

I. Introduction

{1}The growing number of internet users presents an irresistible opportunity for marketers. Advertisers are increasingly seeking ways to reach this pool of potential customers. Current trends are towards sytems that tailor advertisements to individual users, sometimes using information gathered without the users' knowledge or consent. The collection and use of such a large volume of data regarding the activities of individuals naturally raises concerns about privacy. This paper addresses those concerns and examines the legal barriers(1) that may stand in the way of a system using detailed user information to target advertising on the internet.

II. Advertising on the Internet

A. Problems

{2}The advertising techniques used in traditional mass media do not make sense in internet advertising. Mass advertising aims at familiarizing as many viewers or readers as possible with the product, service, or brand name. This kind of shotgun approach is not cost effective when the audience for each advertisement is small. Despite the large number of internet users, the number of visitors to any individual Web site is very small compared to the number of viewers a television commercial or magazine advertisement will reach. This will probably continue to be true even as the

number of Web users grows. The Web is large and diverse, and users are not currently channeled through particular sites that serve to concentrate the viewing audience the way that television networks do. It therefore makes far more sense to use a direct marketing approach in advertising on the internet, which is likely to yield more purchasers per viewer.(2)

{3}Targeting advertisements to the consumer on the internet has proven problematic. Some Web sites use variables passed by the user's Web browsing software, but these variables provide little information beyond the type of computer and software being used.(3) A Web site may ask the user for information in exchange for access, but the wary user might refuse.(4) A software package called Adfinity has recently been released by Intelligent Interactions that will ask the user for minimal data, such as name and address, then use existing consumer databases compiled by credit bureaus to gain a great deal of detailed information.(5) While this strategy will probably discourage fewer users, many people concerned about privacy will be reluctant to participate.

B. A Potential Solution

{4}Advertisers are now moving towards systems that take advantage of information gathered without the user's direct participation.(6) Internet browsing software can be modified to track the users' activities on the internet, collecting information such as which sites are visited, how much time is spent viewing any

particular page of information, and what files are downloaded. This transactional data,[7] combined with any information provided by the user, can be used to develop consumer profiles, which allow advertisers to target or tailor advertisements to the user. These systems also provide valuable data to the advertisers about the number and type of users exposed to their advertisements.

{5}A system that tracks this type of information can be beneficial to the user, as well as to advertisers. The user will be exposed to advertisements in any case, so most would prefer to be exposed to the advertisements that are most likely to be of interest to them. More importantly, these systems can be designed to use gathered information to provide the user with benefits unrelated to advertising, such as tailored Web pages, links to information likely to be of interest to the user, and faster access to data made possible by downloading frequently accessed information in anticipation of the user's request.

III. Privacy Concerns

{6}The accumulation of large amounts of personal data about individuals is nothing new. Credit bureaus, mailing list merchants, and health insurers maintain extensive databases containing minute details of our lives: financial histories, magazine subscription information, and medical records are collected, stored, and sometimes sold.[8] Many Americans are increasingly concerned about the lack of control they have over the collection and dissemination of their personal data.[9] The

collection of data regarding internet activities prompts similar discomfort. These concerns are heightened somewhat by the fact that many internet users do not know enough about the technology to ascertain just what is and is not kept private. Discussions of information privacy have focused on concerns over accuracy and timeliness of data, disclosure to inappropriate persons, and the chilling effects of surveillance.(10) These analyses were directed at information gathering by governments and by private economic entities such as credit bureaus and insurance companies. In the advertising context many of these issues are far less vital. Inaccurate or outdated information presents a real danger when used by a financial institution or health insurer to deny services to the individual. If the information is to be used only to target advertisements or to personalize or improve services, inaccuracies cause little, if any, problem to the individual. Similarly, if the user is confident that the information gathered will be used only as a marketing tool, she is unlikely to modify her behavior in light of the surveillance. There will only be a serious threat to privacy if there is a danger of inappropriate disclosure of personal information.

{7}Subscribers will want some assurance that the information collected will be used only for the purposes stated, and that the information will not be shared with unauthorized persons. But beyond these practical concerns, many people are simply uncomfortable with the idea of any person or entity having so much detailed information about them. People dislike being followed or feeling that they are

watched when going about their daily activities in public. Many will also dislike the idea of being "followed" on the internet. These people will need more than assurances of confidentiality. To contract for such a service, they will need to believe that they are gaining an enhancement in services sufficient to offset their discomfort, and that they will have some recourse if confidentiality is breached.

IV. Legal Barriers and Protections

{8}This section examines both the potential legal barriers to the system described above and the recourse a subscriber might have for abuse of their personal information. This is a fairly new area of the law, and very little case law exists. This makes it rather difficult to advise either the company seeking to develop a new system or the individual concerned about their privacy rights.

{9}Legal protections for personal information vary greatly with the type of information being collected and the manner in which it is collected. There is no comprehensive protection or recognition of privacy rights in the American legal system.(11) Federal and most state constitutions do not provide information privacy rights for private transactions.(12) There is also no comprehensive statutory scheme for privacy protection. Statutes have been enacted only to address specific problems, such as the Video Privacy Protection Act(13), prohibiting the disclosure of personal data by videotape service providers. State common law provides some recourse when privacy rights are violated, but only in fairly extreme cases. Given the patchwork nature of

current law, it may be that contractual agreements are the simplest way for individuals to protect their information privacy.

A. Constitutional Protections

1. The U.S. Constitution

{10}The Supreme Court has recognized constitutional protection of the contents of communications where there is a reasonable expectation of privacy.(14) However, the Supreme Court withheld constitutional protection from pen register information(15) (transactional data) in *Smith v. Maryland*.(16) Thus the content of telephone conversations were protected under the Fourth Amendment, but not the information regarding the numbers dialed and the duration of the call. In *Whalen v. Roe*,(17) a majority of the Court found that a right to information privacy "arguably has its roots in the Constitution",(18) specifically in the Fourteenth Amendment's right to liberty. But non-governmental actors are immune from Fourteenth Amendment restrictions,(19) so any rights recognized would not be enforceable against a private internet service provider.

2. State Constitutions

{11}Several state constitutions expressly protect privacy rights.(20) The Arizona constitutional provision for privacy only restricts governmental actions.(21) In California, however, the State Supreme Court has ruled that "the Privacy Initiative in

article I, section 1 of the California Constitution creates a right of action against private as well as government entities."[(22)] The court goes on to lay out the elements of this right of action:

i) A legally protected privacy interest,

ii) A reasonable expectation of privacy,

iii) Conduct by the defendant that amounts to a serious invasion of a privacy interest.

{12}The defendant may offer an affirmative defense that the invasion of privacy was justified by competing interests. This defense may be rebutted by a plaintiff's proof that feasible and effective alternatives exist.[(23)]

i. A Legally Protected Privacy Interest,

{13}The California Supreme Court expressly recognizes that the right to privacy includes the right to information privacy. One of the purposes of the initiative by which the California Constitution was amended was to "prevent government and business interests from (1) collecting and stockpiling information about us and (2) misusing information gathered for one purpose in order to serve other purposes or to embarrass us."[(24)] Depending on how courts decide to interpret and weigh this language, this provision could cause problems for internet providers who collect transactional data. It certainly seems that tracking of internet activities to produce consumer profiles would amount to "collecting and stockpiling information". It could be argued that if this were enough to constitute an invasion of privacy, credit bureaus, which exist primarily to collect consumer credit information, would be liable.

However, credit bureaus might be immune because the value of free-flowing financial and credit information to the economy is well recognized.[25] Consumer profiling for efficient advertising would not enjoy the same privilege.

ii. A Reasonable Expectation of Privacy,

{14}An internet user might have difficulty in establishing a reasonable expectation of privacy. The California Supreme Court said that a reasonable expectation of privacy should be founded on broadly based and widely accepted community norms.[26] Some internet providers already keep logs of all electronic movements of their subscribers.[27] When a user visits a Web site, he leaves behind information indicating he was there. It can be argued that the "information superhighway" is as public as a city street or shopping mall, so there is no reasonable expectation of privacy.[28]

{15}On the other hand, one is more likely to be aware of the possibility of being watched on a city street than when logged onto the internet from one's private home.

{16}In *United States v. Maxwell*,[29] the United States Air Force Court of Criminal Appeals addressed the expectation of privacy regarding the electronic mail of an America Online (AOL) subscriber. While this decision is not binding regarding an action under the California Constitution, it is illustrative of the analysis applied in expectation of privacy cases. In finding that there was an expectation of privacy in personal electronic mail, the court stated:

{17}We agree that appellant well may have forfeited his right to privacy to any e-mail transmissions that were downloaded from the computer by another subscriber or removed by a private individual from the on-line service. However, we find appellant definitely maintained an objective expectation of privacy in any e-mail transmissions he made so long as they were stored in the America Online computers.

{18}In our view, appellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords.

{19}Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that appellant's computer transmissions would be received by anyone other than the intended recipients. [*citations omitted*]

{20}In the modern age of communications, society must recognize such expectations of privacy as reasonable. We believe such recognition is implicit in the Electronic Communications Privacy Act. We also find support for our determination in the following language by the United States Supreme Court:

{21}"For the Fourth Amendment protects people, not places. 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."[(30)]

{22}There is less of an expectation of privacy when browsing the Web than when sending electronic mail to an individual. Communications on the Web are often made with unknown entities. When moving from one Web site to another, the site the user leaves often knows what site she is moving to, and the new site knows where she previously visited. This is a fairly open circle of communication, not like the end to end transmission of a letter. In addition, the court's argument that the Electronic Communications Privacy Act (ECPA) recognizes the reasonableness of an expectation to privacy in electronic mail does not apply to other internet activities, because the ECPA does not imply an expectation of privacy regarding data other than communication contents.[(31)] It seems likely that a court would not find a reasonable expectation of privacy in this context. In addition, a subscriber who consented to the tracking would have no reasonable expectation of privacy within the scope of that consent.

iii. Conduct Amounting to a Serious Invasion of a Privacy Interest.

{23}The third element of a right of action for violation of privacy is that the invasions be "sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right."[(32)] The seriousness of the invasion of privacy posed by the system under discussion would probably depend on the safeguards imposed to protect information.

A system that allowed raw data traceable to the individual to be accessed by unauthorized persons would seem to constitute an egregious breach. A system that protected raw data and maintained the anonymity of its users would not seem to be a serious threat to privacy. Analysis is likely to be fact specific.

iv. Summary

{24}It seems unlikely that an action would succeed for invasion of privacy under the California Constitution. However, given the uncertainty, it would be wise to design any system to avoid a problem. Gaining the consent of subscribers would ensure that there will be no reasonable expectation of privacy. Maintaining the anonymity of subscribers through the use of anonymous user identification numbers or by other methods would lessen the likelihood that an invasion of privacy would be found.

B. Statutory Protections

{25}There are four federal statutes that may be interpreted as being applicable to a system that tracks user activity on the internet. None directly address the questions at hand, but they may indicate areas where system designers should tread carefully to avoid an inadvertent violation. In each case, problems can be avoided by getting prior authorization from subscribers.

1. The Fair Credit Reporting Act

{26}The Fair Credit Reporting Act of 1970 (FCRA)[33] was enacted to provide some rights and responsibilities in the dissemination of personal information by credit reporting agencies. This act applies only to consumer credit reporting agencies, defined by the FCRA as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[34] This could be read to include a system that tracks consumer internet activities for the purpose of providing consumer profiles to advertisers. Credit information is not being collected, but "other information on consumers" is being assembled and evaluated. However, the term "consumer report" is defined by the act as:

any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance to be used primarily for personal, family, or household purposes, or (2) employment purposes, or (3) other purposes authorized under section 604 [15 USCS §1681b].[35]

{27}Advertising and tailored internet services are not purposes covered by this definition, so information provided solely for those purposes would not be deemed a

consumer report. As quoted above, a person is only a consumer reporting agency if they provide consumer reports, so the act would not cover the system under consideration.

{28}Courts do occasionally try to fit a square statute to a round problem, particularly when dealing with new technology, so it would be worthwhile to consider the limitations that would flow from application of the act to such a system. The FCRA does not limit the collection of consumer information; it is primarily concerned with accuracy and disclosure. Credit reporting agencies must follow reasonable procedures to assure accuracy of personal information, including a dispute process to investigate and correct errors.(36) Individuals have a right to obtain copies of their reports for a "reasonable charge".(37) Credit reporting agencies have broad discretion to disseminate information without permission from the consumer for a "legitimate business need".(38) It is an open question of law whether advertising would be deemed a legitimate business purpose in this context. Courts have ruled in other contexts that information on a particular consumer may only be provided to a third party who requires it in connection with a specific transaction between that party and that particular consumer.(39) Targeted advertising would not appear to meet that test, because most advertisements are a general invitation to transact. Permission from the consumer may be required prior to disseminating information for that purpose. Providing tailored or enhanced services, however, might well qualify as a legitimate business purpose under the act.

2. The Video Privacy Protection Act

{29}The Video Act prohibits video tape service providers from knowingly disclosing personal information without the individual's consent.(40) Internet entities may have to tread carefully when dealing with data collected through interactions with the Web sites of video providers, lest they collect or disseminate information protected by the act. However, the Act prohibits disclosures by video tape service providers only. It is not clear that a third party observer of a transaction, such as an internet service provider or browsing software system, would be covered by the Act. Furthermore, the Video Act may not apply to video services provided directly over the internet.(41) The statute was intended to cover the rental, sale or delivery of video cassette tapes or similar material from a video store. It may be argued that the Video Act does not apply to video programming transmitted without the delivery of a physical tape or similar material.

3. The Cable Communications Policy Act

{30}The Cable Communications Policy Act of 1984 is unusual in that it places limits on the information that may be collected. Without a subscriber's express consent, the Act allows a cable operator to collect personal information only if it is necessary to render the requested services or to detect unauthorized reception or cable communications.(42) Personal information must be destroyed if it is no longer necessary for the purpose for which it was collected.(43) In addition, disclosure of

personal information is generally prohibited unless the disclosure is necessary to render the services requested or to a legitimate business activity related to the service.(44) The Cable Act applies only to cable operators. To be a cable operator, an entity must engage in the "transmission" of video programming.(45) The FCC has stated that "transmission" requires "active participation in the selection and distribution of video programming".(46) Current internet service providers are unlikely to meet this definition, but a cable company that provides both video programming and internet access to its clients will be severely limited by this act.

4. The Electronic Communications Privacy Act

{31}In protecting the privacy of transmitted communications, federal laws distinguish between the contents of communications and the communication attributes.(47) The Electronic Communications Privacy Act (ECPA)(48) prohibits a provider of "electronic communication service to the public" from disclosing the contents of communications, except under certain limited circumstances.(49) The communication attributes, which include all information except the contents themselves, enjoy far less protection. The ECPA allows providers to "disclose a record or other information pertaining to a subscriber not including the contents of communications" to any non-governmental entity.(50) The distinction between communication and communication attributes is simple to make in the context of telephone voice communications: the conversation is the content, and information

regarding the parties, numbers dialed, and duration are communication attributes. It is not so clear which aspects of internet activities will constitute communication contents and which will constitute communication attributes.(51) If a file is downloaded, is the name of the file an attribute? Susan Friewald predicts that judges would likely deem all or almost all of the information concerning a download to be communication attributes.(52)

{32}On the other hand, a 1995 White Paper by the NTIA stated that:

[a] strong argument can be made that by transaction records, Congress meant nothing more than information that reveals the origin, destination, and existence of a communication. Based on this interpretation, from a privacy point-of-view, there may be no meaningful difference between, for example, the contents of a communication and transactional data that identifies the title or the specific nature of the communication.(53)

{33}Thus, descriptive information like the name of a file or the subject line of an electronic mail message may deserve as much protection as the contents of the communications. This remains an open question of law.

{34}An internet provider monitoring internet activities would have to be careful to avoid gathering information that would be deemed communication contents. For example, the system might record when a purchase was made by an internet user at a commercial Web site, but not record what was purchased (the "contents" of the "order form"). This may be problematic, given the uncertainty of the distinction

between contents and attributes described above. Alternatively, the internet provider might obtain the consent of the user to disclose the information for the limited purpose of consumer profiling. Note that the individual user's permission may not be required: the ECPA allows a provider to divulge the contents of a communication "with the lawful consent of the originator *or any addressee or intended recipient* of such communication."(54) Thus the operator of the Web site offering goods for purchase could authorize disclosure.

C. Common Law Remedies

{35}There are four commonly recognized privacy torts categorized as follows by the Restatement (Second) of Torts:

1) unreasonable intrusion upon the seclusion of another,

2) appropriation of another's name or likeness,

3) unreasonable publicity given to the other's private life, and

4) publicity that unreasonably places another in a false light before the public.(55) These torts provide some recourse to the abuse of information by an internet service provider, but do not pose any real barrier to the use of transactional data, particularly if subscriber consent is obtained.

1. Intrusion upon seclusion

{36}"One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."(56) Adjudication of a case where an individual claimed his privacy had been invaded by a system that recorded his movements on the internet would likely turn on whether he had a reasonable expectation of privacy in that context.(57) As discussed in Section III.A, it seems likely that a court would not find a reasonable expectation of privacy in this context.

2. Appropriation of name or likeness

{37}"One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."(58) Although one could argue that selling a consumer profile is an appropriation of one's name, it has generally been held that defendants who sell customer or subscriber lists for advertising purposes are not liable. For example, in *Shibley v. Time*, an Ohio court found that the practice of selling magazine subscriber lists does not amount to an appropriation or exploitation of one's personality.(59) The appropriation contemplated by this tort refers to "those situations where the plaintiff's name or likeness is *displayed* to the public to indicate that the plaintiff indorses the defendant's product or business."(60)

3. Publicity given to private life

{38}"One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that:

(a) would be highly offensive to a reasonable person, and

(b) is not of legitimate concern to the public."(61)

{39}This tort would provide recourse to an individual in the event that personal information collected by their internet provider or software system was made public: that is, communicated to the public at large.(62)

{40}This cause of action appears to provide more protection than it actually does. First, it only applies to information that most people would find highly embarrassing or offensive. Any "mildly offensive" publication would go unpunished. In addition, public figures generally receive almost no protection. First Amendment law has evolved to a point where most information about public figures is considered to be of legitimate interest to the public.(63)

4. False light publicity

{41}"One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if

(a) the false light in which the other was placed would be highly offensive to a reasonable person, and

(b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."(64)

{42}Like the previous tort, this cause of action would only arise if information was made public, and if the publicity would be highly offensive to a reasonable person. This is similar to an action for defamation, but the information does not have to be false: it can be true but misleading. The intent requirement means that the defendant could not be held liable for an inadvertent leak of information.

5. Summary

{43}These privacy torts provide recourse to the individual only in cases of fairly extreme abuse of information. Given the uncertainty regarding the invasion tort, it would be wise to obtain the consent of the subscriber to any tracking system. Consent creates an absolute privilege within the scope of that consent.(65)

D. Contractual Solutions

{44}Contractual agreements may be the simplest way for individuals to protect their information privacy. Contracts have the advantage of flexibility: parties can determine for themselves the value of various risks, costs and benefits. This is particularly useful in the area of privacy, because there is no consensus on the

importance of privacy or on what information is considered private.(66) Also, this flexibility makes contracts more adaptable to the uncertainties inherent in dealing with new, emerging technologies.

{45}There are few concerns about market inefficiencies at present. The market for internet services is currently fairly diverse. Subscribers can choose between services, selecting the one that provides the level of privacy that best suits them. Making an informed choice should not be problematic, as there are many sources for information on privacy available. Private groups such as the Electronic Frontier Foundation (EFF) and government groups such as the Information Infrastructure Task Force provide reports and develop voluntary guidelines for information privacy. Internet users concerned about privacy should be able to select a system that meets their needs.

{46}Market demands are often the best motivation for providers to solve problems. When America Online users experienced problems connecting to the service, their competitors highlighted those problems in their advertisements. AOL had to correct the problem or risk losing their customers. Now, the growing concern over information privacy is prompting interactive providers to find ways to protect user privacy.(67)

{47}For example, subscribers of the system being designed by Andromedia and VeriSign will have Digital ID's. Detailed information will be gathered and stored, but attributed to a digital identity: the user can remain anonymous.(68) Subscribers who

provide supplemental information, such as country, zip code, age and gender, will have increased control over when and where the Digital ID is presented. In addition, each subscriber will be notified as to how the information is to be used.(69) This sort of "digital personality" can actually enhance the privacy of internet users.

{48}Creative solutions to privacy problems are more likely to emerge when financial incentives are paired with a lack of government interference. In a highly fluid situation where technology will continue to move in directions we do not foresee, market based solutions provide a flexibility that makes them clearly preferable in this case.

V. A Note on Government Requests for Information

{49}This paper has not addressed requirements placed on internet providers to turn over information to the government. Both the ECPA and the Digital Telephony Act(70) require disclosure of personal information under certain circumstances. When deciding what information to store on a long term basis, it is important for providers to consider that they might be forced to disclose some or all of that information to the authorities.

VI. Conclusions

{50}The law in both the area of privacy rights and in the area of the internet is very unsettled. At present, there are no real barriers to a system that uses transactional

data to target advertisements, as long as that data does not constitute communications contents. The barriers that do exist can be circumvented.

{51}The only potential limitations to collection and use of information come from the California State Constitution and from the Cable Act. A system that collected and used the data, but did not disclose the information to third parties, would face few obstacles.

{52}The easiest way to protect any system from liability for disclosure of information is to gain meaningful consent from subscribers. Subscribers are far more likely to grant that consent if they feel they are gaining a significant advantage. Enhanced protection of privacy through anonymity is one possible selling point, faster or more tailored internet interactions are another.

{53}In the event that a subscriber's privacy is violated through inappropriate disclosure, the subscriber has limited rights in the absence of a contractual provision. Federal statutes and common law provide causes of action only in the event of a severe breach of privacy, such as publication of the contents of an electronic mail message or publication of a list of videos rented by an individual. It is therefore important that agreements regarding the collection and use of personal information be specifically laid out in contracts, along with the penalties for breach of those agreements.

1. This paper does not attempt to address the problems which may arise under international agreements or the laws of jurisdictions outside of the United States. The implications of international law are no doubt important given the supranational nature of the internet, but they are beyond the scope of this effort.

2. *See* Andy Kessler, *Tracking Mouse Droppings*, Forbes, Aug. 29, 1995.

3. Thomas E. Weber, *Software Lets Marketers Target Web Ads*, Wall Street Journal, Monday, Apr. 21, 1997, at B1.

4. In a 1994 survey, 70% of respondents said they had refused requests from businesses for information because they thought it was not really needed or too personal. Jeff Ubios, *Keep it Under Your Hat*; *Privacy Gets Airtime*, Digital Media, November 7, 1994.

5. Weber, *supra* note 3.

6. *See, e.g., Andromedia, Inc. and VeriSign, Inc. Announce Strategic Partnership*, Business Wire, April 14, 1997 (describing a new system for organizing profile and preference information for Web site visitors).

7. Terminology for this type of information has not yet converged. The National Telecommunications and Information Administration (NTIA) used the term "telecommunications-related personal information" (TRPI) to refer to "personal information that is created in the course of an individual's subscription to a telecommunications or information service or as a result of his or her use of that service." U.S. Dep't of Commerce, Privacy and the NII: Safeguarding

Telecommunications-Related Personal Information (1995) [*hereinafter* Safeguarding TRPI]. Andy Kessler more colorfully referred to the data collected from tracking internet activities as "mouse droppings". Kessler, *supra* note 2. I've chosen to use the term "transactional data", which draws on a comparison to the data collected by consumer credit bureaus and to the records traditionally kept by telephone service providers.

8. *See* Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 Computer & High Technology Law Journal 431, 432 (1993).

9. *See, e.g* ., Ubios, *supra* note 4; *What Price Privacy?* Consumer Reports, May 1991, at 356.

10. *See, e.g*., Roger Clarke, *Information Technology and Dataveillance*, Commun. ACM 31,5 (May 1988); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 Hastings L.J. 1321.

11. Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?* 44 Fed. Com. L. J. 195, 208 (1992).

12. *Id*.

13. 18 U.S.C. § 2710 (1997).

14. Katz v. United States, 389 U.S. 347 (1967).

15. The Court described the pen register as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released." Smith v. Maryland, 442 U.S. 735, 736 n.1.

16. 442 U.S. 735 (1979).

17. 429 U.S. 589 (1977).

18.

Id. at 605. 19. Jackson v. Metropolitan Edison Co., 419 U.S. 345, 349 (1974).

20. < *See, e.g.*, California Constitution, Article I, §1; Arizona Constitution, Article II, §8; Illinois Constitution, Article I, §6.

21. Hart v. Seven Resorts, Inc., 947 P.2d 846, 849-50 (Ariz. App. 1997.

22. Hill v. National College Athletic Association, 7 Cal. 4th 1, 20 (1994).

23. *Id*. at 39-40.

24. *Id*. at 36 (quoting from a Ballot Argument).

25. *See, e.g.*, Scott Shorr, Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment, 80 Cornell L. Rev. 1756, 1778 (1995).

26. Hill v. National College Athletic Association, 7 Cal. 4th 1, 36 (1994).

27. Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949, 958 (1996).

28. Courts have found that there is no reasonable expectation of privacy in public places. *See, e.g.*, Chico Fem. Women's Hlth. Ct. v. Scully, 208 Cal.App.3d 230, 241-

242 (1989) (no reasonable expectation of privacy on public sidewalks and streets outside of abortion clinic).

29. 42 M.J. 568, 576 (1995), *rev'd in part*, 45 M.J. 406 (1996) (limiting expectation of privacy in e-mail transmissions.)

30. *Id*.

31. *See* 18 U.S.C. § 2703(c)(1)(A) (1997).

32. Hill v. National College Athletic Assoc., 7 Cal. 4th 1, 36 (1994).

33. 15 U.S.C. § 1681 - 1681t (1997).

34. 15 U.S.C. § 1681a(f).

35. 15 U.S.C. § 1681a(d).

36. 15 U.S.C. § 1681e(b), 1681i.

37. 15 U.S.C. § 1681j.

38. 15 U.S.C. § 1681, 1681b.

39. Greenway v. Information Dynamics, Ltd., 399 F. Supp. 1092 (D. Ariz. 1974), *cert denied* (holding that the FCRA was violated where consumer reporting agency sent subscribers a microfiche list containing information about hundreds of prospective customers with many of whom they would never do business).

40. 18 U.S.C. § 2710(b)(1) (1997).

41. Safeguarding TRIP, *supra* note 7, at Sect. II.C

42. 47 U.S.C. § 551(b)(2) (1997).

43. 47 U.S.C. § 551(e) (1997).

44. 47 U.S.C. § 551(c)(2)(A) (1997).

45. 47 U.S.C. § 522(5),(6) (1997).

46. This was upheld by the court in National Cable Television Ass'n., v. FCC, 33 F.3d 66 at 71, 73 (D.C. Cir. 1994).

47. Freiwald, *supra* note 27, at 950.

48. 18 U.S.C. §§ 2510-2521, 2701-2709, 3117-3127 (1997).

49. 18 U.S.C. § 2511(3)(a),(b) (1997).

50. 18 U.S.C. § 2703(c)(1)(A) (1997).

51. Freiwald, *supra* note 27, at 956-957.

52. *Id*. at 957 n.31.

53. Safeguarding TRIP, *supra* note 7, at n.77.

54. 18 U.S.C. § 2511(3)(b)(ii) (emphasis added).

55. Restatement (Second) of Torts § 652 (1976).

56. *Id*. § 652B.

57. *See id*. § 652B cmt. c.

58. Restatement (Second) of Torts § 652C (1976).

59. [59]

Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

60. *Id*. (emphasis added).

61. Restatement (Second) of Torts § 652D (1976).

62. *Id*. § 652D cmt. a.

63. *See id*., Special Note on Relation of § 652D to the First Amendment to the Constitution; cmts. f.

64. *Id*. § 652E.

65. *Id*. § 652F.

66. Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 Harv. J. L. & Pub. Pol'y 591, 598 (1994).

67. Ubios, *supra* note 4.

68. *Andromedia, Inc. and Verisign, Inc. Announce Strategic Partnership, Business Wire, April 14, 1997.*

69. *Id*.

70. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C.A. § 1001-10 (West Supp. 1995) and in scattered sections of 18 U.S.C.).

Date of BLT Publication: September 30, 1998