In this chapter we explore the law and policy of the protection of information privacy in a networked world. One widely quoted work on informational privacy defines it as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). The commercialization of the Internet, which is awash with personal information of all types and which allows this information to be collected, manipulated, and transmitted cheaply and easily, predictably has raised a multitude of novel information privacy issues.

Some of the key issues we will address in this chapter are: Will the market take care of online privacy, or is legislation needed? Do the economic benefits of a less-restrictive online privacy policy justify the resulting privacy intrusions? Should privacy in the online world be treated differently from privacy in the offline world?

A. Introduction

1. Legal protection of information privacy in the United States

Perhaps the most salient characteristic of the legal protection of information privacy in the United States is its ad hoc nature. Some types of information transfers are heavily regulated, while other types, seemingly of no less significance to individual privacy interests, are unregulated and left to the mercies of the marketplace. There is no grand scheme that rationalizes the patchwork of legal protections applying to personal information, but only a series of historical accidents and political outcomes that explain them.

For example, the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710, limits disclosure of records of videotape rentals. It was enacted in response to outrage over the disclosure of the video rental records of Judge Robert Bork during the Senate’s consideration of his nomination to the Supreme Court. Information about an individual’s book purchases, however, is unregulated.

Other laws protect the privacy of information transmitted via telecommunications systems. The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22, 2701-11, prohibits the unauthorized interception of electronic communications, including email, and unauthorized access of stored electronic communications. The Telecommunications Act of 1996 includes a provision that protects transactional information concerning telephone calls, including amount of usage and the destination of calls. 47 U.S.C. § 222. The Cable Communications Policy Act of 1984 requires cable operators to disclose to their customers what types of personally identifiable information (“PII”) they collect, and how they use and disclose such information; limits the permissible purposes for collection of PII from subscribers; limits disclosures of subscribers’ PII; gives subscribers the right to access and correct PII concerning them that a cable operator holds; and requires cable operators to destroy PII that is no longer needed for its original purpose. 47 U.S.C. § 551.

The Family Education Rights and Privacy Act of 1974 regulates the handling of student records by educational institutions that receive public funds. The statute limits the disclosure of student records absent parental consent, and gives parents a right to access their children’s records and correct inaccuracies. 20 U.S.C. § 1232g.

Other constitutional and statutory provisions affect the government’s handling of personal information. The Fourth Amendment limits the government’s ability to search for and seize information in which a person holds a reasonable expectation of privacy. The Privacy Act places some, not very stringent, limitations on the government’s use and disclosure of personal information that it holds, and gives individuals a right to access information pertaining to them and to challenge inaccuracies. 5 U.S.C. § 552a. The Driver’s Privacy Protection Act of 1974 places limitations, also not very stringent, on the disclosure of personal information by a state department of motor vehicles. 18 U.S.C. § 2721. It was enacted partly in response to the murder of actress Rebecca Schaeffer, whose killer reportedly obtained her address from records made publicly available for a two dollar fee by the California Department of Motor Vehicles.

The only federal statute that specifically addresses the collection of information online is the Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6501-05, which regulates the collection of personal information from children, as well as the disclosure and use of such information. COPPA is discussed below at —.

To the extent that online transfers of personal information are within the scope of laws designed for the offline world, they are likewise subject to this hodgepodge of legal and marketplace controls. As we shall see, many types of online collection of information have no
easy offline analogue, and in the absence of new legal rules are regulated only by the marketplace.

2. What’s new about the online environment?

Is there anything about online communications that gives rise to fundamentally new issues relating to informational privacy? On the one hand, the digitization of transactional information, and the use of automatic data processing, was a well-established trend long before the Internet became widely available as a medium for commercial transactions. For decades, digitized data on consumer buying habits and credit usage have been collected in databases and used to target marketing and to make decisions on extension of credit. As long ago as 1967, Alan Westin noted that “general information gathering and the dossier have been radically accelerated by the advent of the electronic digital computer, with its capacity to store more records and manipulate them more effectively and rapidly than was ever possible before.” ALAN F. WESTIN, PRIVACY AND FREEDOM 160 (1967). Moreover, vast quantities of transactional information in digitized, personally identifiable form are collected in offline transactions, through the widespread use of payment mechanisms like credit and debit cards and pay-per-call, in sales conducted at as distance through catalogue and telemarketing sales, and using merchant affinity cards.

On the other hand, the use of the Internet for business-to-consumer transactions has introduced some novelties that may have an important bearing on informational privacy issues. First, the widespread use of computers and open-standard networks has made the process of collecting, storing, correlating, transferring, accessing, and otherwise manipulating data much faster and cheaper. The low cost of collecting personal information means that more of it is collected. The low cost of manipulating data means that more value can be mined from it, which raises the incentives both to collect and to disclose it.

Second, the online medium allows pre-transactional data to be captured. When you are browsing at a website, it is a simple matter for the site owner to capture your clickstream information. This includes the identity of every page you have viewed, and any text you enter into web pages, such as search strings. For example, if you research a particular medical problem, the subject of your research can be recorded. If your read an online magazine, the publisher can know which articles you read, and how long you spent on each. If you browse at an online bookstore, the store can get an idea of your reading interests. If you browse at a travel site, the site owner learns something about the travel destinations that interest you. The nature of the online medium makes it economic to store and manipulate such data. By contrast, in realspace shopping it is infeasible and uneconomic for merchants to follow you around as you shop, take notes on what items you look at, and record this information in digital form.

Third, anonymous online payment mechanisms are not widely available online. In realspace shopping you can pay with cash if you want to leave no record of a purchase. When you make a purchase online, your use of a payment mechanism — usually a credit card — generates data that connect you to the purchase.
Fourth, most items that you purchase online must be shipped to you, requiring you to disclose your home address to the merchant. This is also true of other distance selling techniques such as catalogue sales, direct mail, and telemarketing, but not of purchasing in bricks-and-mortar stores.

Fifth, in online transactions the seller is able to capture data surreptitiously, without the knowledge or consent of the data subject. Through the use of cookies, web bugs, and other technologies of surveillance, discussed below at —, a website can gather personally identifiable information about an Internet user who thinks he is browsing anonymously. By contrast, in a telephone conversation the seller gathers only the information that the consumer chooses to provide — with the possible exception of his telephone number, which can be surreptitiously collected using caller ID. When shopping in person, it is possible for the seller to collect information through spying techniques, but this is unlikely to be feasible or cost effective.

Sixth, the Internet makes it easier to gather personal information from children without a parent’s authorization. In realspace shopping settings a child is more likely to be accompanied by an adult, or at least to be recognized as a child.

Seventh, because the network connects us more tightly to each other than other communications technologies, individuals cloaked in anonymity can do greater harm, such as through hacking, fraud, defamation, and revealing private information. There is a correspondingly greater societal interest in being able to ascertain the identity of online speakers.


Recognition of the privacy concerns specific to e-commerce should not obscure the fact that in significant respects online privacy concerns are identical to those raised by offline commerce. The same technology that facilitates the efficient compilation and dissemination of personal information by online companies also allows offline companies to amass, analyze and transfer vast amounts of consumers’ personal information. Offline companies collect and compile information about consumers’ purchases from grocery stores, pharmacies, retailers, and mail order companies, in particular.

It is also not possible to distinguish offline and online privacy concerns on the basis of the nature of the information collected. With the exception of online profiling, it is the same information. The Report’s recommendation would require Amazon.com to comply with the fair information practice principles but not the local bookstore which can compile and disseminate the same information about the reading habits of its customers. The consumer polls, upon which the Report places such significant reliance, demonstrate that consumer concerns about the disclosure of personal information are not dependent on how the data has been collected.

Moreover, it is impractical to maintain such a distinction. Businesses are likely to have a strong incentive to consolidate personal information collected, regardless of the mode of collection, in order to provide potential customers with the most personalized message possible.
Already, companies are seeking to merge data collected offline with data collected online. In light of this reality, the majority’s recommendation would result in perverse and arbitrary enforcement. Enforcement actions would depend on the source of and method used to collect a particular piece of consumer data rather than on whether there was a clear-cut violation of a company’s announced privacy policy or mandated standards.


In the 1960s and early 1970s, computing and telecommunications were generally controlled by the federal government and large corporations. The emergence of personal computers and networking in the mid-1980s, however, contributed to a shift in power to the commercial sector. Smaller private-sector organizations gained access to sophisticated information-processing capabilities through inexpensive equipment. Individuals and small, private organizations obtained access to vast information resources through services such as Prodigy, CompuServe, and America Online. In essence, the Internet and private networks gave globalized access to information to both individuals and small organizations. Globalized access to information and real-time interactivity multiply the options available to users of information, both individuals and businesses. Interactive communications produce numerous transaction records, thereby multiplying choices regarding the use of information as well.

At the beginning of the 1990s, information processing was decentralizing even within large corporations as networks replaced mainframe computers. Today, in the mid-1990s, the decentralization of information processing has made omnipresent surveillance possible by organizations and even individuals. This decentralization enables any network participant to centralize data, for although bits of information are scattered throughout the network, they are accessible from any place on the network. This, however, is not the extent of decentralization’s effects. Sophisticated information providers and intelligent networks already enable combinations of audiovisual images and sounds with other interactive services. Further, decentralization of information processing in the United States dramatically broadened the role of private-sector data processing and shifted power from the federal government to private-sector organizations. These private organizations now have exclusive control over the decisions regarding the collection and use of personal information.

Query

Are the privacy issues presented by the online medium sufficiently different from offline privacy issues to merit independent legislative treatment? Is it feasible to disentangle the two realms and apply different rules to each? Would application of different rules to the two realms result in harmful distortion of business or consumer economic incentives?

3. Tensions within the idea of privacy

Like nearly all other interests that the law recognizes, the interest in privacy is not absolute. Privacy serves a number of valuable functions. Most generally, the ability to control
what other people can know about you provides a sphere of free action that is a basic human necessity. The right to keep your identity information secret can help to protect you from stalkers, abusive ex-spouses, and other sociopaths, and makes identity theft less likely. Anonymity enables people to blow the whistle on wrongdoing without fear of retribution.2

But there are also competing societal interests that may be harmed by the protection of privacy. One way to address these competing interests is to ask “how do we balance the need to use information (by government, commerce, and individuals) with the natural desire of individuals to decide what information about themselves will be exposed to others?” Information Infrastructure Task Force, Information Policy Committee, Options for Promoting Privacy on the National Information Infrastructure 7 (1997). These competing interests may be organized under the headings of accountability, free circulation of ideas, and efficiency.

Accountability. Privacy, when it takes the form of anonymity, enables speakers to avoid being held accountable for the consequences of their speech. Although the First Amendment broadly protects the right to free expression, limits the government’s authority to impose sanctions on a person based on his speech, and even guarantees anonymity in certain circumstances,3 there are recognized exceptions. For example, the First Amendment does not prevent the government from imposing liability based on defamation, unauthorized disclosure of trade secrets, false advertising, threats of violence, blackmail, obscenity, advocacy of imminent lawless action, and other speech acts. Anonymity interferes with the law’s ability to protect the interests represented by these derogations from an absolute right of freedom of expression. Laws, norms, and self-regulatory practices that protect privacy must take these same competing interests into account.

Privacy as invisibility — a person’s ability to control who may learn her whereabouts or how she may be contacted — may also interfere with legitimate societal interests. Invisibility makes it harder for single mothers to track down deadbeat dads, for litigants to locate witnesses, and for law enforcement authorities to collar criminal suspects.

Free circulation of ideas. The First Amendment’s free speech clause serves several interests, among them encouraging the free flow of information within what is frequently referred to as the “marketplace of ideas.” The Supreme Court has held that this interest is weighty enough to overcome substantial opposing interests, in view of our “profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials.”4 The protection of privacy, when it takes the form of limiting the disclosure of information that is considered personal, interferes with this goal. Thus, the publication of personal information that touches on matters of public concern, and that is true

---

2 For an extended discussion of the functions of individual privacy, under the rubrics of “personal autonomy, emotional release, self-evaluation, and limited and protected communication,” see ALAN F. WESTIN, PRIVACY AND FREEDOM 32-39 (1967).


and was legally obtained, is almost always protected.\(^5\) However, when the First Amendment right to free association — the right to nondisclosure of the identity of those with whom one chooses to associate — is opposed to society’s interest in the free flow of information, the former may sometimes prevail. Thus, compelled disclosure of membership lists has been held to violate the First Amendment.\(^6\) In addition, in the context of reproductive rights the Supreme Court has recognized a constitutionally protected privacy interest “in avoiding disclosure of personal matters.”\(^7\)

Limiting disclosure of personal information can interfere with the ability of researchers and investigative journalists to do their work. Protected private information may be newsworthy itself, or may lead to other newsworthy information.\(^8\)

\textit{Efficiency}. Privacy is also sometimes opposed to the societal interest in facilitating efficient commercial transactions. Data collected from commercial transactions involving individual consumers are used to create profiles of prospective customers that enable marketers to target promotional solicitations to consumers who are more likely to find them of interest. This results in a higher return rate, and therefore reduces the cost of marketing. Giving individuals a right to prevent the use of their transactional data for these purposes interferes with the creation of lists that permit such targeting. In addition to making marketing more expensive, it may also be contrary to the individual’s own interests in minimizing the quantity of junk mail and telemarketing that she receives, since a lower return rate means that more solicitations must be sent out. Limiting businesses’ use of transactional information can make it harder for new entrants to compete:

\begin{quote}
Because trade in consumer information serves an important economic function, regulatory obstacles to collecting this information can have hidden economic costs. . . . The mandatory opt-in rule would favor larger and older companies at the expense of newer, smaller ones. Established companies could afford more costly lists more easily than could small companies. And established companies would also have less need for lists, since they would have been in business long enough to collect information on their own. The \textit{brunt of an opt-in law would thus be borne by small, new businesses or nonprofits struggling to establish a customer base. . . .} Under mandatory opt-in, firms that could afford to send direct mail would no longer be able to target it effectively. That would lead to fewer, more expensive options for those who shop at home—the elderly,
\end{quote}

\(^5\) See Florida Star v. B.J.F., 491 U.S. 524 (1989) (First Amendment trumps state law forbidding publication of the name of a victim of a sexual offense); Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978) (First Amendment overcomes law prohibiting publication of names of judges who are under investigation for misconduct).


\(^8\) For a criticism from a First Amendment perspective of proposals to protect information privacy through legal restrictions on the disclosure of information, see Eugene Volokh, \textit{Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You}, 52 STAN. L. REV. 1049 (2000).
the disabled, rural residents, and anyone without a car—because their mobility is restricted. In a world without readily available, cheap marketing lists, it is doubtful that another company like Lands’ End would ever be born. Mandatory opt-in could preclude, not only the development of new businesses, but the development of whole new business models and product lines designed to serve groups of customers that could never before be identified. Had mandatory opt-in rules been in place a hundred years ago, for example, consumer credit reporting might never have developed.


The ability to conceal information that reflects badly on yourself, in the name of privacy, can interfere with the ability of others to make rational decisions concerning you; as for example if the fact of your criminal record is unavailable to a potential employer, business associate, or spouse, if your poor credit history is unavailable to a prospective lender, or if your medical information is not readily available in an emergency situation.

Notes

1. **Balancing competing values.** Evaluate the following argument: Expressing the problem of privacy protection as one of “balancing” competing values is a bureaucratic turn that leads to no solution. We are better off thinking of it as an optimization problem, which we can approach either from a utilitarian or a moral rights perspective. Under the former, we extend the right of privacy only as far as it will yield benefits exceeding its costs. Under the latter, we may sometimes protect privacy for its own sake, regardless of the costs entailed.

2. **A communitarian perspective.** Amitai Etzioni urges a “communitarian” approach that explicitly recognizes the claims of societal interests that conflict with privacy interests. He argues that there is no basis for privileging privacy above all other societal interests: where individual interests conflict with communal interests, in some circumstances the individual interests must yield. He proposes a methodology for ascertaining whether a particular invasion of privacy, in the service of some societal goal, is justified:

   First, a well-balanced, communitarian society will take steps to limit privacy only if it faces a well-documented and macroscopic threat to the public good, not a merely hypothetical danger. . . . [For example, w]hen many thousands of lives are lost and many millions more are at risk, as with HIV, we face a clear and major threat. The effects of abusing marijuana are real but of a much lower magnitude, and hence do not justify the same kind of response. . . . The second criterion is to look at how carefully a society acts to counter a tangible and macroscopic danger without first resorting to measures that might restrict privacy. . . . Third, to the extent that privacy-curbing measures must be introduced, a communitarian society makes them as minimally intrusive as possible. . . . Lastly, measures that treat undesirable side effects of needed privacy-diminishing measures are to be preferred over those that ignore these effects.

Do you agree that there is no aspect of informational privacy that we should regard as absolute, indefeasible regardless of the countervailing interests?

B. Fair Information Practices Principles

One widely followed approach to information privacy issues is to implement privacy protections that correspond to a set of principles defining what are fair information practices. Statements of these principles have had an important impact on policy discussions concerning information privacy on the Internet.

FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7-11 (2000)

III. Fair Information Practice Principles

A. Fair Information Practice Principles Generally

Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information — their “information practices” — and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.

Common to all of these documents [hereinafter referred to as “fair information practice codes”] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

1. Notice/Awareness

The most fundamental principle is notice. Consumers should be given notice of an entity’s information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below — choice/consent, access/participation, and enforcement/redress — are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.

While the scope and content of notice will depend on the entity’s substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- identification of the entity collecting the data;
- identification of the uses to which the data will be put;
- identification of any potential recipients of the data;
- the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
• whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
• the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data; whether the consumer has been given a right of access to the data; the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised.

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity’s information practices on a company’s site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site’s home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent. At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company’s mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer. Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put. Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company’s general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user’s decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.
3. Access/Participation

Access is the third core principle. It refers to an individual’s ability both to access data about him or herself — i.e., to view the data in an entity’s files — and to contest that data’s accuracy and completeness. Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

4. Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.

5. Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.

a. Self-Regulation

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress). Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association; external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue. A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.
Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (e.g., correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer. Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

b. Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity’s unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation. The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, e.g., the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages; and the elements of any such cause of action.

c. Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers. Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.

Notes

1. A widely recognized formulation. This formulation of the fair information practice principles underpins several self-regulatory efforts aimed at online privacy. See, for example, the principles implemented by the TRUSTe privacy seal program, discussed below at —, the guidelines adopted by the Online Privacy Alliance, discussed below at —, and the content of website privacy notices created by the Direct Marketing Association’s privacy policy generator, discussed below at —.

2. Substantive content of notice. Should the “notice” principle extend to the content of a website’s privacy practices, or only to whether those practices are disclosed in a clear and conspicuous manner? Consider the following privacy notice: “We collect and retain all of the personally identifiable information we can extract from your online activities, including all of your clickstream activity. Using a cookie, we associate this information with your online identity. We also make every effort to link this information to your real-world identity, and are usually successful. We will use the information we have gathered to target-market you to whatever extent we find profitable. We will also avail ourselves of every opportunity to sell, rent, share, or trade your personal information with any other commercial entity if by doing so we can turn a buck.” Is this privacy statement objectionable from the standpoint of the fair information practice principles?

3. Comprehensibility of notice. Website privacy notices tend to be long, rambling, full of legalese, diluted with extraneous material, and generally incomprehensible to most people. One analysis of the privacy policies posted at some of the most heavily trafficked sites on the Web found that they were all written at a college reading level or higher, while most people in the United States read at a tenth-grade level or below. One of these policies was eight pages long, containing 3,405 words and 167 sentences. How easy must a privacy notice be for it to be considered adequate notice? Is this subject of online privacy inherently too complex to allow a website to disclose its practices in a brief and understandable manner?

4. Choice: Opt-in vs. Opt-out. The question whether the exercise of choice should be through an opt-in or an opt-out mechanism has provoked heated debate. Since few Internet users exercise any choice they are offered, the default option is the one that is “selected” in the vast majority of cases. Marketers therefore strongly prefer opt-out. Privacy advocates are critical of opt-out, on the ground that it does not represent the exercise of informed consent on the part of the user. Consider the following viewpoint:

[Opt-out] puts the burden of protecting privacy on the consumer. Most people have neither the time, know-how, or gumption to examine closely the uses to which their data will be put; they are unlikely to take the initiative to direct dozens of Web sites to not shadow and share.

“Opt out” is the marketer’s public relations trick to provide the pretense of choice. . . . The only genuine online privacy protection is informed, written consent. That is when the burden of getting permission to pass around personal data falls where it

---

belongs, on the seller, who must explain the deal and persuade or offer inducements to
the buyer to choose to give permission.


In another context, the U.S. Court of Appeals has held that an FCC regulation requiring
opt-in consent to the disclosure of customer information by telecommunications carriers is an
unconstitutional regulation of speech, in violation of the First Amendment. See U.S. West, Inc.
v. Federal Communications Commission, 182 F.3d 1224 (10th Cir. 1999).

5. Access. The question of appropriate access has been a thorny issue for U.S. policy-
makers. A blue-ribbon advisory committee assembled by the FTC was able to do little more
than agree to disagree on such issues as what access consists of, what information should be
subject to access, how to implement access when information is shared among various third
parties, and who should bear the cost of access. See Final Report of the Federal Trade
Commission Advisory Committee on Online Access and Security (2000),
an access right that is in some respects equivocal, but does give the data subject a right to
“communication to him in an intelligible form of the data undergoing processing and of any
available information as to their source,” and also “as appropriate the rectification, erasure or
blocking of data the processing of which does not comply with the provisions of this Directive,
in particular because of the incomplete or inaccurate nature of the data.” EC Directive, Art. 12,
discussed below at —.

6. Supplemental fair information practice principles. The European Commission’s Data
Protection Directive goes beyond this formulation of the fair information practice principles in
several respects. First, it places a substantive limitation on the quantity of personal data that is
collected, requiring that it be “not excessive in relation to the purposes for which they are
collected and/or further processed.” Art. 6(1)(c). Second, personal data must be “kept in a form
which permits identification of data subjects for no longer than is necessary for the purposes for
which the data were collected or for which they are further processed.” Art. 6(1)(e). Third, the
processing of certain sensitive types of data is off limits: with certain exceptions, it is
impermissible to process “personal data revealing racial or ethnic origin, political opinions,
religious or philosophical beliefs, trade-union membership, and . . . data concerning health or sex
life.” Art. 8(1). Fourth, the onward transfer of personal data is subject to the limitation that in
the hands of the transferee the data retains “an adequate level of protection.” Art. 25(1). These
might be formulated as four additional principles: “Minimal Collection,” “Minimal Retention,”
“Sensitivity,” and “Onward Transfer Protection.” If you were devising a list of the cardinal
privacy protection principles, would you include any of these additional principles?

C. Online Privacy Issues

1. Surreptitious collection of information from Internet users

When accessing the Internet from your personal computer it is natural to assume that,
unless you choose to identify yourself, your activities are anonymous. This is an illusion.
Network technology has spawned mechanisms that allow a website operator to learn the identity
and track the online activities of website visitors, and enable senders of email to receive notification when the recipient opens the message. Cookies brand an Internet user’s computer with a unique identifying number that facilitates tracking, and web bugs allow a web page or an email message to “call home” and report the information they have gathered. This surveillance is carried out in a manner that is invisible to most Internet users, and that may be difficult to prevent. Privacy advocates view this surveillance as one of the most serious and intrusive threats to the privacy interests of Internet users.

a. Technologies of surveillance

i. Cookies

When you use your computer to access a website, your computer transmits certain information to the website, including the URL of the web page you are seeking to access (which tells the website what data you want it to send to you), the IP address of your computer (which tells the website where to send the data so that you can receive it), the URL of the web page you are viewing at the time you access the site, and certain configuration information about your computer. This information is usually not sufficient to allow the website to recognize you, the next time you access the site, as someone who has previously visited the site. Nor does it generally allow the website to ascertain your real-world identity.

Cookies were designed to overcome this identity gap. A cookie is a unique identification code that a website causes to be placed on a computer as it accesses the site. The next time you visit the website, it reads the cookie it left behind, and is able to recognize you — or at least the computer you are using — as one that has previously visited the site. Cookies can also contain additional information, such as a password or user preferences, that can be read by the server that placed it on your computer.

This rather simple capability has profound implications for the privacy of website visitors. Each time you access a website, you transmit “clickstream” information to the site, consisting at a minimum of the URL of each page you visit at the site. Once a site has assigned your computer a unique identification code, it can collect all of the clickstream data created by visits using your computer and associate that data with your identification code. Thus, a website can create a dossier of information that is associated with your computer, and can use this information to personalize its interaction with you. For example, if you visit a sporting goods

---

10 With the dial-up connections that most people use to access the Internet from their home computers, the IP address is “dynamic”: it may change each time the computer dials in and makes a new connection to the Internet. Since this identifier is not persistent, it does not allow a website to identify a visiting browser. Some types of broadband connections, such as DSL and cable, use “static” IP addresses: the address of the computer is always the same, giving the computer a persistent identity. The same is true of most connections to the Internet through a local area network.

11 Cookies come in different flavors. “Session” cookies are maintained in your computer’s memory while your computer is connected to the Internet, and disappear as soon as you close your browser. “Persistent” cookies are written to a file on the hard drive of your computer — usually either into a file named “cookies.txt,” or into a file directory named “cookies.” It is only persistent cookies that allow a website to recognize your computer through multiple visits to the site.
site on several occasions, and view a number of web pages showing tennis racquets, the next time you visit the site it can serve you a personalized home page that features special offers on tennis racquets. Although the site does not know your real-world identity — your name, address, age, gender, or anything else — it does recognize you as somebody who has manifested an interest in tennis racquets.

Now suppose that in one visit to the website you provide some personal information about yourself. The unique identifier contained in the cookie the site has dropped onto your hard drive allows the website to associate this information with all the other data it has stuffed into your dossier. If, for example, you give the website your email address to subscribe to a free newsletter or to enter a contest, the site will know that all the clickstream data it has previously collected from you belongs to a person with a particular email address. It can then use the information in its dossier to send you email messages containing promotional material tailored to your interests. Or the website might want to know more. Before it sends you the free newsletter, or enters you in a contest to win a vacation for two to the Bahamas, it may ask for your age, gender, and income range. Then it has more to go on: it can tailor its promotional messages taking into account this demographic information as well. It may also be able to make some money by renting your email address and demographic information to another company, so that it too can send you targeted direct marketing material.

Finally you break down and decide to buy yourself that tennis racquet you have been coveting each time you visit the site. You order it via the website, necessarily providing your name, address, and telephone number so that the seller can have the racquet delivered to you. Now the website knows exactly who you are, and all the information in its dossier becomes associated with your real-world identity. The website can now use all of the information it has about you to tailor special offers it conveys to you by direct mail and telemarketing, as well as via email. Your dossier becomes a more valuable commodity, which can be rented to a broader range of other sellers. Your activities in visiting that website, past and future, are no longer anonymous.

ii. Globally unique hardware identifiers

As described above, dropping cookies is a way of branding a computer with a persistent, globally unique identifier that allows the computer to be identified from across the network. A cookie is software — it is a data file that is written to a computer’s hard drive. Another type of persistent GUID is one that is embedded in the computer’s hardware. Like a cookie, hardware GUID’s can be read remotely from across the network.

One common type of hardware GUID is the identifier that is inscribed on Ethernet cards. An Ethernet card is a device installed in a personal computer that allows it to interconnect with other computers through a local area network. The protocol that is used for routing communications within a LAN requires each of the computers belonging to the LAN to have a unique address. This address is derived from the unique serial number of each computer’s Ethernet card.
Within the context of a LAN, the existence of a unique identifier on the Ethernet card raises no privacy concerns, since nobody who uses a LAN’ed computer has any expectation that his communications across the LAN will be anonymous. But in early 1999, a privacy advocate named Robert M. Smith announced his discovery of a peculiar feature of the online registration program for Windows 98. If the computer whose copy of Windows 98 was being registered contained an Ethernet card, the registration program would extract the card’s unique identification number, place it on the computer’s hard drive as a cookie, and transmit the number to Microsoft. When a user of the computer created a document using certain Microsoft application programs, including Word 98 and Excel 98, this GUID would be inserted into the document in a manner that made it invisible to the average user but easily available to the cognoscenti. This gave Microsoft the ability to identify the author of any such document, by looking up the document’s GUID in the GUID database created by the Windows 98 registration process. It would also give anybody with access to a computer the ability to identify documents as having originated with that computer, and would make it possible to prove that two particular documents originated from the same computer.

Microsoft received a good deal of criticism after this practice was revealed, and it sought to make amends by announcing it would stop collecting GUIDs in the registration process, delete the GUID database it had assembled from Windows 98 registrations, and make available a program to delete the GUID from an individual computer’s Windows registry. It also pledged to remove from its Office 2000 suite of applications the ability to insert GUIDs in documents. See Letter from Yusuf Mehdi (Mar. 8, 1999), www.microsoft.com/PressPass/features/1999/03-08custletter2.asp.

iii. Web bugs

A web bug is an instruction in the code that constitutes an HTML page that causes your computer to transmit information across the network to some other computer. The functionality that a web bug exploits was designed to allow web pages to display graphic images. The HTML code of a page with a graphic image contains an instruction that tells your browser to fetch the image from a particular location on the server hosting the website, or on any other server connected to the Internet, and to place it on the web page it is displaying at a particular location and as a specified size. The HTML protocol allow your browser to append a string of text to the fetch request it sends to the server, and the server is able to read this text. A web bug is an instruction that pretends to be fetching an image to display on your web page, but in fact has the sole purpose of transmitting information from your computer to the server computer. The image it fetches generally consists of a single pixel that is the same color as the pixel of the web page over which it is placed, and that therefore has no visible effect on the site visitor’s computer. For this reason web bugs are sometimes euphemistically referred to as “clear GIFs” or “1 x 1 GIFs.”

A web bug can transmit a variety of information to the server it is pointed at, including the visiting computer’s IP address, the URL of the page on which the bug is placed, the time the

12 An instruction that is placed in the code of a web page for the bona fide purpose of fetching a graphic image may have a dual character, functioning also as a web bug.
page containing bug was displayed, and the identification code contained in any cookie that was placed by that server. What makes a web bug so much more powerful than a cookie alone is its ability to transmit information to a server other than the one that holds the web page the visitor is viewing. Suppose, for example, that the sporting goods website you are visiting displays a banner advertisement from an online bookseller. In order to display the ad, the code making up the page of the sporting goods site you are viewing contains an instruction telling your browser to fetch the image constituting the banner ad from a server maintained by the bookseller. The instruction causes your browser to transmit to the bookseller’s server the URL of the page you are visiting — the one featuring the tennis racquet of your dreams. The bookseller’s server is then able to place on the web page you are about to view a banner ad that it thinks will interest you, say one featuring a book on the history of racquet sports. The bookseller’s server is also able to place a cookie on your computer, so that it can begin to assemble a dossier on you. Note that this transmission of information to the bookseller occurs even though you have not clicked on its banner ad or taken any other action expressing any interest in the bookseller.

Now imagine that some company managed to place web bugs on thousands of web sites, including the most popular sites on the web. This company would be in a position to assemble quite a detailed profile of your online activities. Every time you viewed a page at any one of those websites, that fact would be transmitted to the company and added to your dossier. If you ever divulged your real-world identity at any of those websites, the company would be able to associate your identity with all of the data it had assembled about you. If the company were able to link this dossier with other collections of information about your offline activities, quite a lot of information about you would be available in one easily sortable, searchable, transmissible digital package, and various commercial entities might find such a package highly valuable.

As discussed below, this is the method that network advertising servers use to gather information they use in targeting online advertising.

iv. Email and document bugs

Web bugs can also be used in email messages, and in electronic documents. Email messages that display graphics and styled text are constructed out of the same HTML code that constitutes web pages, and are equally capable of harboring web bugs. Such a bug might consist of an instruction to fetch an invisible graphic from the email-sender’s server, and while doing so to transmit information back to the server. For example, when you open the message the web bug can “call home” and report the time and date you opened it. The sender thereby learns that you do in fact read your email, and through sending a series of messages may discern the time of day you typically check your email. A job applicant could use this technique to determine whether companies to which he emailed his resume opened it.

A more advanced type of bug, which works only in email readers with JavaScript enabled, can transmit back to the original sender any comments you add to the email when you forward it to somebody else. This technique, which is known as “email wiretapping,” would allow the original sender to eavesdrop on an entire email conversation between two people who converse by using the “Reply” button to send messages back and forth. (Does email wiretapping
violate the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq.? Does it violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030?)

An email bug can be used in conjunction with a network advertising server’s cookies to link personally identified information to a previously anonymous online profile. Suppose that DoubleClick, which is one of the leading network ad servers, has dropped a cookie on your hard drive, and has collected clickstream information from you that is associated with your cookie’s identification code, but does not know your real-world identity. Now you register to receive a free email newsletter from another company that uses DoubleClick as its ad server. When you open the newsletter in your mail reader, a bug in the newsletter set by DoubleClick checks your hard drive to see whether it holds a DoubleClick cookie. If it does, then DoubleClick is able to link your cookie identification code — and all of the clickstream information it has associated with that code — to your email address. If in registering to receive the newsletter you supplied your real name, address, or other personal details, DoubleClick now knows exactly who you are and can associate its entire dossier with your real-world identity.

Bugs can also be inserted into documents produced by word processing, spreadsheet, presentation, and other software applications. These documents can include code that fetches a graphical image from a remote server, via the Internet. If the instruction is coded to retrieve an invisible 1 x 1 pixel dummy graphic, it can be used just like any other web bug. This sort of instruction will routinely transfer to the server the host name and IP address of the computer holding the document, and has the ability to set and read cookies. The bug would report back to the document’s creator each time it is accessed on a computer with a live Internet connection. The document creator could therefore be alerted whenever the document was forwarded to and opened by somebody else. If it was a confidential document, and the bug reported that it had been opened on a computer with a different host name, the creator would know it had been leaked and might be able to determine from the host name the organization that received it. If the document was copyrighted, the creator could determine whether it has been distributed in violation of the copyright.

v. Application-based spyware

Some software developers have included within their application software code that causes the user’s computer to transmit information back to the developer via the Internet. One use of this technology is to deliver advertising content to the user that is tailored to the information that the spyware gathers. It could also be used to scan the user’s hard drive to see what other software he has installed, adding this information to a profile of the user that will be used for marketing purposes. Several developers have been caught using this technology surreptitiously, without informing the user or seeking his consent. In one widely publicized incident, security experts discovered that RealJukebox, free downloadable software that organizes and plays music files, was surreptitiously transmitting to RealNetworks, the maker of the software, information on users’ listening habits, including the number of songs stored on the user’s hard drive, the file formats in which they are stored, and the user’s preferred music genre. Unless the user changed the software’s default settings, it also transmitted the title of each CD inserted into the user’s CD-ROM drive. All of this information was combined with a GUID assigned to each user, allowing dossiers to be compiled. All of this occurred without notice to

Notes

1. GUID’s. Is the proliferation of software- and hardware-based GUID’s something to be feared and fought, or is it an inevitable and largely beneficent consequence of the growing importance of network communications in all facets of life and the consequent necessity to privilege security and easy identification over privacy and anonymity?

2. Online profiling

Commercial websites frequently feature banner advertisements, which are rectangular panels appearing on website pages that contain promotional material and are usually hyperlinked to the website of the company placing the ad. As with print and broadcast media, these advertisements may be placed through a contractual arrangement between the website owner and the advertiser, according to which the advertiser pays the website owner to insert its ad into the code making up the website.

Advertisements can also be placed on websites through a third-party intermediary known as a network advertising server. The ad server contracts with advertisers who want their banner ads placed on websites, and contracts with website owners for the right to place ads on their sites. When a user pulls up a web page on a site that belongs to an ad server’s network, the ad server determines what banner advertisement to display on the page based on the information that the server has obtained about the user (more accurately, about whoever uses that computer to browse the Web). The collection of information generated when Internet users browse the Web, and association of that information with a particular web-browsing computer or individual, is known as online profiling.


II. WHAT IS ONLINE PROFILING?

A. Overview

Over the past few years, online advertising has grown exponentially in tandem with the World Wide Web. Online advertising revenues in the U.S. grew from $301 million in 1996 to $4.62 billion in 1999, and were projected to reach $11.5 billion by 2003. A large portion of that online advertising is in the form of “banner ads” displayed on Web pages — small graphic advertisements that appear in boxes above or to the side of the primary site content. Currently, tens of billions of banner ads are delivered to consumers each month as they surf the World Wide Web. Often, these ads are not selected and delivered by the Web site visited by a consumer, but by a network advertising company that manages and provides advertising for numerous unrelated Web sites. DoubleClick, Engage, and 24/7 Media, three of the largest
Internet advertising networks, all estimate that over half of all online consumers have seen an ad that they delivered.

In general, these network advertising companies do not merely supply banner ads; they also gather data about the consumers who view their ads. This is accomplished primarily by the use of “cookies” and “Web bugs” which track the individual’s actions on the Web. Among the types of information that can be collected by network advertisers are: information on the Web sites and pages within those sites visited by consumers; the time and duration of the visits; query terms entered into search engines; purchases; “click-through” responses to advertisements; and the Web page a consumer came from before landing on the site monitored by the particular ad network (the referring page). All of this information is gathered even if the consumer never clicks on a single ad.

The information gathered by network advertisers is often, but not always, anonymous, i.e., the profiles are frequently linked to the identification number of the advertising network’s cookie on the consumer’s computer rather than the name of a specific person. This data is generally referred to as non-personally identifiable information (“non-PII”). In some circumstances, however, the profiles derived from tracking consumers’ activities on the Web are linked or merged with personally identifiable information (“PII”). This generally occurs in one of two ways when consumers identify themselves to a Web site on which the network advertiser places banner ads. First, the Web site to whom personal information is provided may, in turn, provide that information to the network advertiser. Second, depending upon how the personal information is retrieved and processed by the Web site, the personally identifying information may be incorporated into a URL string that is automatically transmitted to the network advertiser through its cookie.

Once collected, consumer data can be analyzed and combined with demographic and “psychographic” data from third-party sources, data on the consumer’s offline purchases, or information collected directly from consumers through surveys and registration forms. This enhanced data allows the advertising networks to make a variety of inferences about each consumer’s interests and preferences. The result is a detailed profile that attempts to predict the individual consumer’s tastes, needs, and purchasing habits and enables the advertising companies’ computers to make split-second decisions about how to deliver ads directly targeted to the consumer’s specific interests.

The profiles created by the advertising networks can be extremely detailed. A cookie placed by a network advertising company can track a consumer on any Web site served by that company, thereby allowing data collection across disparate and unrelated sites on the Web. Also, because the cookies used by ad networks are generally persistent, their tracking occurs over an extended period of time, resuming each time the individual logs on to the Internet. When this “clickstream” information is combined with third-party data, these profiles can include hundreds of distinct data fields.

Although network advertisers and their profiling activities are nearly ubiquitous, they are most often invisible to consumers. All that consumers see are the Web sites they visit; banner ads appear as a seamless, integral part of the Web page on which they appear and cookies are placed without any notice to consumers. Unless the Web sites visited by consumers provide
notice of the ad network’s presence and data collection, consumers may be totally unaware that their activities online are being monitored.

**B. An Illustration of How Network Profiling Works**

*Online consumer Joe Smith goes to a Web site that sells sporting goods. He clicks on the page for golf bags. While there, he sees a banner ad, which he ignores as it does not interest him. The ad was placed by USAad Network. He then goes to a travel site and enters a search on “Hawaii.” USAad Network also serves ads on this site, and Joe sees an ad for rental cars there. Joe then visits an online bookstore and browses through books about the world’s best golf courses. USAad Network serves ads there, as well. A week later, Joe visits his favorite online news site, and notices an ad for golf vacation packages in Hawaii. Delighted, he clicks on the ad, which was served by the USAad Network. Later, Joe begins to wonder whether it was a coincidence that this particular ad appeared and, if not, how it happened.*

At Joe’s first stop on the Web, the sporting goods site, his browser will automatically send certain information to the site that the site needs in order to communicate with Joe’s computer: his browser type and operating system; the language(s) accepted by the browser; and the computer’s Internet address. The server hosting the sporting goods site answers by transmitting the HTTP header and HTML source code for the site’s home page, which allows Joe’s computer to display the page.

Embedded in the HTML code that Joe’s browser receives from the sporting goods site is an invisible link to the USAad Network site which delivers ads in the banner space on the sporting goods Web site. Joe’s browser is automatically triggered to send an HTTP request to USAad which reveals the following information: his browser type and operating system; the language(s) accepted by the browser; the address of the referring Web page (in this case, the home page of the sporting goods site); and the identification number and information stored in any USAad cookies already on Joe’s computer. Based on this information, USAad will place an ad in the pre-set banner space on the sporting goods site’s home page. The ad will appear as an integral part of the page. If an USAad cookie is not already present on Joe’s computer, USAad will place a cookie with a unique identifier on Joe’s hard drive. Unless he has set his browser to notify him before accepting cookies, Joe has no way to know that a cookie is being placed on his computer. When Joe clicks on the page for golf bags, the URL address of that page, which discloses its content, is also transmitted to USAad by its cookie.

When Joe leaves the sporting goods site and goes to the travel site, also serviced by USAad, a similar process occurs. The HTML source code for the travel site will contain an invisible link to USAad that requests delivery of an ad as part of the travel site’s page. Because the request reveals that the referring site is travel related, USAad sends an advertisement for rental cars. USAad will also know the identification number of its cookie on Joe’s machine. As Joe moves around the travel site, USAad checks his cookie and modifies the profile associated with it, adding elements based on Joe’s activities. When Joe enters a search for “Hawaii,” his search term is transmitted to USAad through the URL used by the travel site to locate the information Joe wants and the search term is associated with the other data collected by the
cookie on Joe’s machine. USAad will also record what advertisements it has shown Joe and whether he has clicked on them.

This process is repeated when Joe goes to the online bookstore. Because USAad serves banner ads on this site as well, it will recognize Joe by his cookie identification number. USAad can track what books Joe looks at, even though he does not buy anything. The fact that Joe browsed for books about golf courses around the world is added to his profile.

Based on Joe’s activities, USAad infers that Joe is a golfer, that he is interested in traveling to Hawaii someday, and that he might be interested in a golf vacation. Thus, a week later, when Joe goes to his favorite online news site, also served by USAad, the cookie on his computer is recognized and he is presented with an ad for golf vacation packages in Hawaii. The ad grabs his attention and appeals to his interests, so he clicks on it.

A previously anonymous profile can also be linked to personally identifiable information in other ways. For example, a network advertising company could operate its own Web site at which consumers are asked to provide personal information. When consumers do so, their personal information could be linked to the identification number of the cookie placed on their computer by that company, thereby making all of the data collected through that cookie personally identifiable.

Psychographic data links objective demographic characteristics like age and gender with more abstract characteristics related to ideas, opinions and interests. Data mining specialists analyze demographic, media, survey, purchasing and psychographic data to determine the exact groups that are most likely to buy specific products and services. . . . Psychographic profiling is also referred to in the industry as “behavioral profiling.”

DoubleClick, Inc., a leading network advertising server, raised the hackles of privacy advocates when it announced, in June 1999, that it was merging with Abacus Direct Corp., a direct marketing research firm that held in its databases information about catalogue purchases of about 90 million U.S. households. Thereafter, in a revision to its website privacy notice, DoubleClick announced, in obfuscated language indecipherable to the great majority of Internet users, that it intended to link information acquired from websites within its network with data in the Abacus databases. This would allow it to associate previously anonymous clickstream data with the real-world identities of Internet users, and to combine information about consumers’ offline purchases with data about their online activities. The Electronic Privacy Information Center filed a complaint against DoubleClick based on these actions, accusing the company of deceptive and unfair practices in violation of the FTC Act. See In the Matter of DoubleClick, Inc. (Complaint and Request for Injunction, Request for Investigation and for Other Relief, filed with FTC Feb. 10, 2000), www.epic.org/privacy/internet/FTC/DCLK_complaint.pdf. The FTC opened an investigation of DoubleClick, but closed it without taking any further action, finding that DoubleClick had not in fact combined clickstream data with information from Abacus databases. See Letter from Joel Winston to Christine Varney dated Jan. 22, 2001, www.ftc.gov/os/closings/staff/doubleclick.pdf.

In March 2000, facing a barrage of criticism from privacy advocates and a round of bad publicity, DoubleClick reversed course and announced that it would not go forward with the
planned information merger “until there is agreement between government and industry on privacy standards.”

Notes

1. Benefits of network advertising. Network advertising servers describe the benefits of the services they provide as follows:

   Effective Internet advertising is fundamental to the accessibility and dynamism of this revolutionary medium. Advertising underwrites the rich variety of online content choices available to consumers at no cost or at a far lower cost than would otherwise be possible. By delivering customized advertising, network advertisers offer substantial benefits for consumers and the advertiser. In addition, many small and emerging Web companies depend on network advertisers to compete against more well-established companies and their Web sites. Effective Internet advertising thus helps to maintain the low barriers to entry that have played a crucial role in the robust competition and innovation that have fueled this medium.


   In view of these benefits, how would you balance the privacy interests of Internet users against the asserted benefits of information collection by network advertisers? Are Internet users entitled to meaningful notice about the practices of network advertising servers, and true choice about whether to allow their clickstream data to be collected for purposes of online profiling? Can you think of any mechanism that would provide Internet users with such notice and choice?

2. Opting out of online profiling. The major network advertising servers allow individual Internet users to opt out of their tracking systems. How likely is it that users will avail themselves of this option? To do so, a user must be aware that this sort of tracking is conducted, locate the website for each of the ad server companies, and follow each company’s procedure for opting out. The whole procedure must be repeated if the user switches to another computer, or if she deletes her cookies file. Would it be preferable from the standpoint of fair information practices if the website that is harboring the web bug — the one that the user is actually visiting — provided the disclosure?

   In its Privacy Policy, Yahoo! discloses that it allows network advertisers to collect information about visitors to its website. It advises visitors: “If you want to prevent a third-party ad server from sending and reading cookies on your computer, currently you must visit each ad network’s web site individually and opt out (if they offer this capability).” Yahoo!, “Network

---


Advertisers and Third-Party Ad Servers,” privacy.yahoo.com/privacy/us/adservers/details.html. It continues with a list of links to no fewer than 33 network advertisers’ websites!


4. Surreptitious collection of video rental information. Advertising servers are capable of collecting an Internet user’s clickstream information. Suppose a website that rents videotapes uses an ad server. When a visitor selects a video to rent, that information is collected by the ad server. In so doing, has the ad server violated the Video Privacy Protection Act, 18 U.S.C. § 2710, which, with certain exceptions, makes it illegal to knowingly disclose personally identifiable information about an individual’s rental or purchase of videos. Has the video rental website violated the Act? Does it matter whether the video rental information is maintained in a personally identifiable manner?

5. Application of anti-surveillance laws to ad servers. DoubleClick creates profiles of Internet users by tapping into the clickstream information that users exchange with the websites they visit. For this to happen, the websites with which DoubleClick has contractual arrangements must modify the code that constitutes their web pages by inserting statements that direct clickstream information to DoubleClick. In collecting this information, does DoubleClick violate the Electronic Communication Privacy Act, 18 U.S.C. § 2511, which makes it unlawful to “intentionally intercept[] . . . any . . . electronic communication”? Does it violate another provision of ECPA, 18 U.S.C. § 2701, which prescribes penalties for anyone who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.”? See Bruce v. DoubleClick, Inc. (N.D. Cal. filed Jan. 28, 2000); Healy v. DoubleClick, Civil Action No. 00 Civ. 0641 (S.D.N.Y. filed Jan. 31, 2000); Judnick v. DoubleClick, Inc., No. CV 000421 (Cal. Super. Ct., Marin Cty. filed Jan. 27, 2000). Does the website that hosts the code that allows DoubleClick to collect clickstream information violate these provisions? See Rubin v. Intuit Inc., No. 00 CIV. 1778 (S.D.N.Y. filed Mar. 8, 2000).

6. Application of consumer protection laws. The Attorney General of Michigan took enforcement action against several websites that harbored web bugs set by DoubleClick and other network advertising servers, explaining:

    Surreptitious tracking of consumers’ browsing behavior is not legal under Michigan law. The Michigan Consumer Protection Act generally applies to a wide range of transactions and practices affecting consumers. While there are over 30 different unfair practices that are prohibited under the Act, the central theme is that businesses are
required to deal fairly and honestly with consumers. This includes a duty on the part of businesses to disclose important aspects of a transaction that are not reasonably obvious to consumers.

In the context of online privacy, the fact that consumers’ browsing behavior is being monitored by unfamiliar third parties for unknown reasons to be a material fact to consumers. Furthermore, this fact is not something that a consumer could reasonably be expected to know. For this reason, web sites that interact with Michigan consumers are required to disclose tracking of consumers’ online activity.

The Attorney General’s office has issued Notices of Intended Action to a number of companies that operate commercial web sites warning these companies that lawsuits may follow unless the web sites take steps to tell consumers that they are being tracked by third parties.


7. Profiling not limited to ad servers. The same surveillance techniques that network advertising servers use to target marketing can be used for other purposes as well. For example, a trade association could use a combination of web bugs and cookies to track people who visit its members’ websites, and could share that information with its members.

Amazon.com has implemented a mechanism by which Internet users can make a donation to a website they visit by clicking on a “Click to Give” icon that appears on the site’s home page. The graphic file that constitutes the icon is fetched from Amazon’s server; the instruction that causes the fetching therefore functions like a web bug. In fact, the instruction checks for an Amazon cookie on the visitor’s hard driver, and if it finds one, looks up the name that Amazon has associated with that cookie, and customizes the “Click to Give” icon with a greeting that includes the visitor’s name! But Amazon explains that it has configured its servers so that it does not retain any personal information that is collected during this procedure. See Amazon.com, “About the Amazon Honor System,” s1.amazon.com/exec/varzea/subst/fx/help/how-we-know.html.

3. Failure to honor a website privacy policy

a. Saying one thing, doing another

Not all online privacy issues are novel. Existing laws that forbid deceptive marketing practices can be applied when a website makes representations in its privacy policy concerning its handling of site visitors’ personal information, and then fails to honor its promises.

One such law is the Federal Trade Commission Act, which forbids “unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. § 45(a)(1). In GeoCities, FTC Docket No. C-3850 (Feb. 5, 1999), the FTC charged GeoCities with failing to observe its privacy promise. GeoCities offered free website hosting services, with sites organized thematically into “virtual communities.” GeoCities — which was subsequently acquired by Yahoo!, and continued operating under the name Yahoo!GeoCities — provided its members (which it dubbed
“homesteaders”) with space on its web server, accessed through a URL of the form “www.geocities.com/member_name/...”. At the time the FTC filed its complaint, GeoCities had over 1.8 million homesteaders, including 50,000 under the age of 13. To become a member, users had to provide GeoCities with certain types of personal information, including first and last name, zip code, email address, gender, and date of birth. In its privacy notice, GeoCities stated: “We will not share this information with anyone without your permission . . . .”

In its complaint, the FTC alleged that, contrary to this privacy statement, GeoCities “sold, rented, or otherwise marketed or disclosed this [personal identifying] information, including information collected from children, to third parties who have used this information for purposes other than those for which members have given permission. For example, third parties have targeted unrequested e-mail advertising offers to individual members based on their chosen GeoCities neighborhoods.” The FTC also alleged that GeoCities represented that it collected certain personal identifying information from children, when in fact this information was collected by undisclosed third parties operating through GeoCities’ website. The FTC alleged that these were deceptive misrepresentations, in violation of the FTC Act. GeoCities consented to entry of an order that prohibited future misrepresentations, required it to post a website privacy policy containing specified categories of information, and required it to obtain “express parental consent” before collecting personal identifying information from children.

**Query**

Does an undertaking in a website privacy policy give rise to an enforceable contract? If GeoCities discloses a member’s personal information in contravention of its privacy policy, can the member sue GeoCities for breach of contract?

**b. The special case of bankruptcy: Toysmart**

Suppose the owner of a website that has operated under a policy of never disclosing its personal customer data files for bankruptcy. Does the company’s customer list, with its associated transactional data, become an asset of the bankruptcy estate, subject to sale for the benefit of the company’s creditors?

The issue arose in the case of Toysmart.com, an online toy retailer that went bankrupt. Toysmart’s privacy policy stated: “Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party.” The policy also stated: “When you register with toysmart.com, you can rest assured that your information will never be shared with a third party.”<sup>15</sup> Toysmart was a licensee of TRUSTe, and its website displayed the TRUSTe trustmark. The company announced that it was going out of business, and offered to sell its assets, including its customer lists, to the highest bidder. Toysmart’s creditors subsequently filed a petition against it for involuntary bankruptcy.

---

The FTC filed a lawsuit against Toysmart to prevent the sale of the customer information, alleging that to do so in the face of its privacy promise would be a deceptive practice in violation of the FTC Act. The FTC reached a settlement with Toysmart, under which the customer information could only be sold as part of a package including the entire website, and only to a purchaser that agreed to abide by the terms of Toysmart’s privacy notice. But the Attorneys General of 38 states, and TRUSTe as well, objected to the settlement as being insufficiently protective of consumers, reasoning that when a company says it will “never” disclose personal information, it should be held to its word. The controversy was ultimately resolved when Walt Disney Co., the majority owner of Toysmart, agreed to pay $50,000 for the customer information and immediately to destroy the information.

Notes

1. **What constitutes disclosure?** It is not always easy to determine whether a particular event constitutes disclosure of information to another party. Suppose Company A operates a website that provides free information about medical problems, with a privacy policy that states: “We will never sell, share, rent, trade, or otherwise disclose your personal information to anyone, ever.” Is there a violation of the privacy policy if (1) Company A is sold, as a going concern, to Company B, which is also a provider of free medical information? (2) Company A is sold, as a going concern, to Company C, which is a pharmaceutical marketing company? (3) Company A acquires Company D, a pharmaceutical marketing company, as a subsidiary, and transfers the information to Company’s D’s marketing department? (4) Company A expands its business by beginning to sell pharmaceuticals, and uses its customer data for marketing? (5) Company A’s stockholders sell a majority of the company’s stock to new stockholders? (6) Company A goes out of business, and sells its database of personal information together with the rights to its trademark?

2. **Online vs. offline.** Toysmart got into trouble because its website operated under a highly protective privacy policy. If Toysmart had been a bricks-and-mortar toy store that went bankrupt, it would most likely not have stated any privacy policy, and there would be not been any objection to sale of its customer information. Does it make sense for the two situations to be treated differently? Did the FTC and the states overreact to the proposed sale of Toysmart’s customer information?

3. **The lesson of Toysmart.** In view of Toysmart’s difficulties, how would you advise a commercial website to structure its privacy policy? How likely is it that prospective customers would refuse to patronize a website because its privacy policy allowed customer information to be transferred without limitation in case of merger, acquisition, restructuring, or bankruptcy? Will prospective creditors be less willing to lend to an e-commerce business if its privacy policy makes customer information unavailable as an asset to satisfy debts?

c. **Modification of a website privacy policy**

In the aftermath of the Toysmart controversy, Amazon.com implemented a change in its privacy policy. In September 2000 it sent email messages to its 23 million customers announcing the change. The emails (with some non-substantive variations) read:
Dear Customer,

We’re sorry for this intrusion. We know that you’ve asked not to receive certain types of e-mail from Amazon.com. From that request, it’s clear that privacy issues are important to you. As we’ve recently updated our privacy policy, we did think it very important to contact you by e-mail to inform you of these changes.

To read the revised Privacy Notice, visit:

http://www.amazon.com/privacy-notice

And again — please accept our apologies for sending you this e-mail. Thanks for shopping with us.

Sincerely,

Amazon.com

The privacy notice had previously stated:

Amazon.com does not sell, trade or rent your personal information to others. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank e-mail message to never@amazon.com.

The revised policy says:

**Business Transfers:** As we continue to develop our business, we might sell or buy stores or assets. In such transactions, customer information generally is one of the transferred business assets. Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.

The revised policy also eliminates the option to direct Amazon not to disclose personal information to third parties.

As a result of this modification, the Electronic Privacy Information Center, a privacy advocacy group, severed its relationship with Amazon, through which Amazon was a favored distributor of EPIC’s publications. In a letter to its subscribers, EPIC explained: “Recently Amazon announced that it could no longer guarantee that it would not disclose customer information to third parties. Because of this decision, and in the absence of legal or technical means to assure privacy for Amazon customers, we have decided that we can no longer continue our relationship with Amazon.” Electronic Privacy Information Center, Letter from Marc Rotenberg (Sept. 13, 2000), [www.epic.org/privacy/internet/amazon/letter.html](http://www.epic.org/privacy/internet/amazon/letter.html).

Notes

1. **Sufficiency of notice of change to a privacy policy.** Note that the Amazon’s email message announcing the modified privacy policy provided a link to the (revised) policy, but gave
no indication what changes were made. How useful is such an announcement to the average Internet user? Should a website that changes its privacy policy have an obligation to explain to its existing customers exactly those changes are? Is it sufficient for a website privacy policy to state: “We may change our privacy policy at any time. Be sure to read it carefully each time you revisit the site.”?

2. **No choice.** Amazon’s revised privacy policy does not offer users any choice as to whether their personal information will be disclosed. Is this aspect of the policy consistent with the FTC’s articulation of the fair information practice principles? Would Amazon’s policy qualify for a TRUSTe seal of approval?

3. **Retroactive application of a modified privacy policy?** If a website changes its privacy policy, which policy applies to information collected before the change is announced. Consider the following statement, which appears at the end of Amazon.com’s revised privacy policy:

   Our business changes constantly. This Notice and the Conditions of Use will change also, and use of information that we gather now is subject to the Privacy Notice in effect at the time of use. We may e-mail periodic reminders of our notices and conditions, unless you have instructed us not to, but you should check our Web site frequently to see recent changes.

(Emphasis added.) What is the meaning of the phrase in italics? Is there anything wrong with this?

4. **Piercing the veil of online anonymity**

   Many Internet users engage in online speech under a pseudonym, on the assumption that the speech cannot be associated with their real-world identity. This assumption has frequently turned out to be unwarranted. If a user furnishes her true identity when acquiring online access from an Internet service provider, when registering a domain name, or when registering at a website that offers a bulletin board or other forum for public communication, then the institution holding that identity information frequently has the capability of associating an online pseudonym, such as an email address, user name, screen name, or handle, with the speaker’s real-world identity.

   a. **Discovering via subpoena the identity of anonymous online speakers**

   In a number of cases, companies have brought defamation actions against individuals who have posted anonymous comments online that are critical of the company. After initiating the lawsuit, the company issues a subpoena to an ISP, online portal, or other entity that know the online speaker’s real-world identity, seeking disclosure of that identifying information. If the entity complies with the subpoena, the company learns the identity of its critic, and can proceed with the lawsuit, or pursue various other avenues of retaliation. Revelation of the critic’s identity can have severe consequences if he happens to be an employee of the company, or involved in some business relationship with it. In some of these cases, the company has dropped the defamation lawsuit after learning the identity of its critic. Privacy advocates have branded this a
misuse of the judicial system, claiming that the lawsuits were frivolous and were filed for the sole purpose of unmasking the critic.

In many of these cases, the subpoena recipient complies with the subpoena by divulging the speaker’s identity, without giving the speaker prior notice or an opportunity to contest the subpoena. However, in a few cases the propriety of such discovery has been challenged.

Columbia Insurance Co. v. Seescandy.com
United States District Court, N.D. California, 1999.
185 F.R.D. 573.

JENSEN, District Judge.

On February 22, 1999, plaintiff Columbia Insurance Company filed an motion for a temporary restraining order and an order to show cause why a preliminary injunction should not issue. On March 4, 1999, plaintiff withdrew the motion with respect to defendants the Web Service Provider, Sidney Trayham, and Peter Jackson. The Court hereby denies the motion without prejudice to refiling and orders plaintiff to submit a brief with the Court within 14 days addressing the issue of whether the Court should authorize discovery to establish defendant's identity sufficiently such that he may be served in compliance with the Federal Rules of Civil Procedure.

I. BACKGROUND

A. Factual-Background and Procedural History

On February 22, 1999, plaintiff Columbia Insurance Company ("Columbia") filed this action seeking injunctive relief, damages, and an accounting of profits. Columbia is the assignee of various trademarks related to the operation of See's Candy Shops, Inc. ("See's"). See's is the predecessor in interest to the trademarks at issue in this case and holds a license from Columbia to use the marks.

The domain names "seescandy.com" and "seecandys.com" have been registered with Network Solutions, Inc. ("NSI") by someone other than plaintiff.

* * *

As of September 24, 1998, the seescandy domain name was registered to seescandy.com. The address was given only as "CA, 90706," which is for Bellflower, California. The administrative and billing contacts were listed as Salu Kalu, who could be contacted by e-mail at hostmaster@fluctuate.com. The telephone number given, 408-555-1212, is the local number for information in the San Jose area. The fluctuate.com domain, as of February 21, 1999 is registered to a Ravi Kumar of Artesia, California.

On December 22, 1998, the record was changed to show the owner as R, L of Artesia, California; however, the zip code given, 90706 is for Cerritos, California. The phone number was again given as the number for information, but the area code had been changed from 408 to
The contact e-mail address had been changed to RL@fluctuate.com. In addition, the domain was now shown as being hosted by websp.com.

On February 13, 1999, the record was modified again to list the address as P.O. Box 1300, Artesia, California, with the zip code changed from 90706 to 90702, which is an actual zip code for Artesia, California. The telephone number was also changed to (562) 807-0297.

As of January 22, 1999, the domain name seecandys.com was registered to Sees Candys and had the contact listed as Robby Kumar. The address was given as Tustin, California 92782; the e-mail address as dns@fluctuate.com; and the telephone number as (310) 860-0229.

On February 25, 1999, both the seescandy.com and seescandys.com domains were changed from the web host of websp.com to simplenet.net. Simplenet.net is a San Diego, California company.

Plaintiff has sued defendants for (1) infringement of federally registered service and trademarks, in particular "SEE'S," "SEE'S CANDIES," and "FAMOUS OLD TIME"; (2) federal unfair competition; (3) federal trademark dilution; (4) California State dilution under California Business and Professions Code § 14330; (5) unfair and deceptive trade practices under California Business and Professions Code § 17200; (6) California common law trade name, trademark, and service mark infringement and unfair competition; and (7) unjust enrichment.

Plaintiff seeks as relief a temporary, preliminary, and thereafter permanent injunction enjoining defendants from using any of See's marks, for goods or services or as metatags, directory names, other computer addresses, metatags, invisible data, or otherwise engaging in acts or conduct that would cause confusion to the source, sponsorship or affiliation of See's Candies with defendants.

* * *

II. DISCUSSION

The Court will not grant a temporary restraining order against defendants at this time because such a ruling would be futile. Plaintiff has not been able to collect the information necessary to serve the complaint on defendants. As a result any temporary restraining order issued could only be in effect for a limited time and would be unlikely to have any effect on defendant whom plaintiff has not yet located. Once the order expired plaintiff would be unable to obtain a preliminary injunction because such relief cannot be imposed ex parte.

Service of process can pose a special dilemma for plaintiffs in cases like this in which the tortious activity occurred entirely on-line. The dilemma arises because the defendant may have used a fictitious name and address in the commission of the tortious acts. Traditionally, the default requirement in federal court is that the plaintiff must be able to identify the defendant sufficiently that a summons can be served on the defendant. See Fed.R.Civ.P. 4. This requires that the plaintiff be able to ascertain the defendant's name and address.
As a general rule, discovery proceedings take place only after the defendant has been served; however, in rare cases, courts have made exceptions, permitting limited discovery to ensue after filing of the complaint to permit the plaintiff to learn the identifying facts necessary to permit service on the defendant. See e.g., Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir.1980) (finding the district court abused its discretion in dismissing the case with respect to the John Doe defendants without requiring the named defendants to answer interrogatories seeking the names and addresses of the supervisors in charge of the relevant facilities during the relevant time period); Estate of Rosenberg by Rosenberg v. Crandell, 56 F.3d 35, 37 (8th Cir.1995) (permitting a suit naming fictitious parties as defendants to go forward because the allegations in the complaint were "specific enough to permit the identity of the party to be ascertained after reasonable discovery"); Maclin v. Paulson, 627 F.2d 83, 87 (7th Cir.1980) (approving of fictitious name pleadings until such time as the identity of the plaintiffs "can be learned through discovery or through the aid of the trial court"). In the even rarer case, a district court has sua sponte issued an order directing revelation of facts necessary to determine the true name of a John Doe defendant. See Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 390 n. 2, 91 S.Ct. 1999, 29 L.Ed.2d 619 (1971) (noting that the trial court had ordered the United States attorney to identify "those federal agents who it is indicated by the records of the United States Attorney participated in the ... arrest of the [petitioner]") (quoting the district court's order).

In the Ninth Circuit such exceptions to the general rule have been generally disfavored. See Gillespie, 629 F.2d at 642. However, a district court does have jurisdiction to determine the facts relevant to whether or not it has in personam jurisdiction in a given case. See Wells Fargo & Co. v. Wells Fargo Express Co., 556 F.2d 406, 430 n. 24 (9th Cir.1977). A district court's decision to grant discovery to determine jurisdictional facts is a matter of discretion. See id.

With the rise of the Internet has come the ability to commit certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely on-line. The tortfeasor can act pseudonymously or anonymously and may give fictitious or incomplete identifying information. Parties who have been injured by these acts are likely to find themselves chasing the tortfeasor from Internet Service Provider (ISP) to ISP, with little or no hope of actually discovering the identity of the tortfeasor.

In such cases the traditional reluctance for permitting filings against John Doe defendants or fictitious names and the traditional enforcement of strict compliance with service requirements should be tempered by the need to provide injured parties with an forum in which they may seek redress for grievances. However, this need must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously. People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity.
Thus some limiting principals should apply to the determination of whether discovery to uncover the identity of a defendant is warranted. The following safeguards will ensure that this unusual procedure will only be employed in cases where the plaintiff has in good faith exhausted traditional avenues for identifying a civil defendant pre-service, and will prevent use of this method to harass or intimidate.

First, the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court. See e.g., Wells Fargo, 556 F.2d at 430 n. 24 (stating that plaintiffs bear the burden of establishing jurisdictional facts). This requirement is necessary to ensure that federal requirements of jurisdiction and justiciability can be satisfied. See Plant v. Does, 19 F.Supp.2d 1316 (S.D.Fla.1998) (refusing to issue a temporary restraining order against unnamed and unserved bootleggers who had not yet committed an offense on the theory that plaintiffs have failed to establish that the Court had jurisdiction over defendants, to provide defendants with due process, and to demonstrate that an actual controversy existed).

Plaintiff’s papers establish that the listed defendants who remain in the case after March 4, 1999 appear to be aliases for a person known as Ravi or Robby Kumar of Artesia, California ("the Kumar defendants"). Most of the addresses listed by aliases associated with the Kumar defendants show a California domicile, which indicates that the Court likely has jurisdiction over defendants. Plaintiffs are suing the following aliases, all of which are alleged to be owners or operators of the domain names seescandy.com and seescandys.com: Seescandy.com, Sees Candys, hostmaster dns, fluctuate, foolio, x2, ticker talk, RL, and Salu Kalu. Salu Kalu was listed as the contact for seescandy.com in September of 1998. RL is a person who was listed as the contact person for seescandy.com as of January 16, 1999. Hostmaster DNS is the name of the contact person listed for seescandy.com as of February 8, 1999. It is important to note that Hostmaster DNS is a common generic term used to describe the system operator in charge of running a domain name server. It is thus highly problematic as an identifier of a defendant. However, Hostmaster's e-mail address is dns@foolio.com, which ties this alias to the Kumar defendants. Fluctuate is the second level domain of fluctuate.com, which is listed in the WHOIS as registered to tickertalk, for whom the contact is Robby Kumar. Fluctuate.com is the domain that provides all the mailboxes for the e-mail addresses listed as contacts for the seescandy.com and seescandys.com domains. X2 is the listed registrant of the domain name x2.org, for whom the contact is listed as Ticker Talk with the E-mail address of dns@foolio.com. Foolio is the listed registrant for foolio.com, for whom the contact is Salu Kalu, and which is the domain hosting the E-mail address of the contact, Ticker Talk, for the x2.org domain. Most convincing of all, See's has been in contact by e-mail with a person who goes by the name "Ravi." In his e-mail message, Ravi has indicated a desire to sell the subject domain names to See's and has provided See's with evidence that consumers have been actually confused by these web sites, for which Ravi claims to hold registration rights. The Court finds that there appears to be only one person behind all these registrations, a Ravi or Robby Kumar, who may also be known as Salu Kalu. The Court finds that plaintiff has made a satisfactory showing that there is an actual person behind these acts who would be amenable to suit in federal court.

Second, the party should identify all previous steps taken to locate the elusive defendant. This element is aimed at ensuring that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants. See Plant, 19
F.Supp.2d at 1320 (noting that plaintiffs had failed to explain why they were unable to identify the defendants). Plaintiff's counsel has certified that the following efforts were made to contact defendants: (1) calls were made to the two non-directory information services telephone numbers. One was a non-working number and nobody answered the other one. Simultaneous with the filing of the motion for a temporary restraining order and preliminary injunction plaintiff served its complaint, brief, and all accompanying papers to the official addresses provided to NSI, only one of which was a complete mailing address. Plaintiff also served these documents, sans exhibits, by electronic mail to the e-mail addresses associated with the domains registered by Ravi Kumar, Robby Kumar, RL, Salu Kalu, and Hostmaster DNS. Although such service is not sufficient to comply with the Federal Rules of Civil Procedure, the Court finds that such acts do show that plaintiff has made a good faith effort to specifically identify defendant and to serve notice on defendant.

Third, plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss. See Gillespie, 629 F.2d at 642. A conclusory pleading will never be sufficient to satisfy this element. Pre-service discovery is akin to the process used during criminal investigations to obtain warrants. The requirement that the government show probable cause is, in part, a protection against the misuse of ex parte procedures to invade the privacy of one who has done no wrong. A similar requirement is necessary here to prevent abuse of this extraordinary application of the discovery process and to ensure that plaintiff has standing to pursue an action against defendant. See e.g., Plant, 19 F.Supp.2d at 1321 n. 2 (commenting that standing was likely absent because defendants were alleging only future acts of infringement, not past acts or patterns of infringement). Thus, plaintiff must make some showing that an act giving rise to civil liability actually occurred and that the discovery is aimed at revealing specific identifying features of the person or entity who committed that act.

Plaintiff has demonstrated that their trademark infringement claim could survive a motion to dismiss and therefore have satisfied this element. The test for infringement of a federally registered trademark (Count I) and for false designation of origin (Count II) under the Lanham Act is whether the alleged infringing act creates a likelihood of confusion. [The Court reviewed the evidence, and concluded:] Plaintiffs showing is sufficient to demonstrate that the Kumar defendants have committed an unlawful act for which a federal cause of action can subsist.

Lastly, the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible. See Gillespie, 629 F.2d at 642 (stating that discovery should not be permitted if it is not likely to uncover the identity of the defendant). As ordered below, plaintiff has 14 days to make a filing with the Court with respect to the process the Court should consider ordering.

II. CONCLUSION AND ORDER

Plaintiff shall have 14 days from the date of this order to submit a brief with the Court setting forth specifically the forms of discovery process, the justification for such process, and
the persons or entities on whom they are to be served that plaintiff expects will achieve the end of providing the missing identifying information necessary for service of process. If plaintiff does not yet have sufficient information to satisfy the Court that such process should be ordered, plaintiff may so indicate and later reapply for such discovery once the facts necessary to make the required showing have been uncovered.

IT IS SO ORDERED.

Notes

1. The Internet connection. In Seescandy.com, was there any danger that allowing discovery of the defendant’s would chill the online speech of defendant or others similarly situated? Was the involvement of the Internet in that case anything more than incidental? Is the standard that the courtarticulates one that appropriately balances the interests of tort victims in obtaining redress and the interests of anonymous online speakers in remaining anonymous?

2. A different standard. In Melvin v. Doe, No. GDD99-10264 (Ct. of Common Pleas of Allegheny County, Pennsylvania, Nov. 15, 2000), the plaintiff was a state judge who brought a defamation action against a person who had anonymously posted a message on an America Online bulletin board that accused her of official misconduct. Plaintiff made a discovery request, seeking the defendant’s identity. Defendant objected to the discovery request on the ground that anonymous political speech is protected by the First Amendment. While recognizing that the First Amendment prevents states from barring anonymous political speech entirely, and that allowing litigants to unmask anonymous speakers has a tendency to chill speech that is at the core of First Amendment protections, the court rejected the argument that the First Amendment places an absolute bar on discovering the identity of an anonymous online speaker. Instead, the court held that discovery would be allowed unless defendant showed that plaintiff could not make out a prima facie case, and stayed discovery to give defendant a chance to do so. The court explained that plaintiff could defeat defendant’s effort to make such a showing “(1) if the plaintiff establishes that the publication appeared on the Internet and that the statements within the publication, if false, support a defamation recovery, and (2) if the plaintiff testifies that the statements are untrue and that she has experienced emotional distress as the result of the statements.” The court held that plaintiff had met this threshold, and that discovery into defendant’s identity would be allowed. However, to limit the exposure of defendant’s identity in case defendant should ultimately prevail, the court issued a protective order preventing disclosure of defendant’s identity other than to the parties and their counsel.

When the issue is whether to allow discovery of the identity of an anonymous online speaker, is the burden of proof more appropriately placed on the plaintiff or defendant? Should a higher standard apply in cases where the speech in question is core First Amendment speech, such as speech relating to the conduct of government officials?

3. John Doe fights back. In Doe a/k/a Aquacool_2000 v. Yahoo! Inc., Case No. CV 00-04993 WMB (RZx) (C.D. Cal. filed May 11, 2000), the plaintiff was an individual who had posted comments on a Yahoo! message board that were critical of its former employer, a company named AnswerThink Consulting Group, Inc. The comments were posted
pseudonymously, attributed to “Aquacool_2000.” AnswerThink filed a defamation action against Aquacool_2000 and several other unnamed defendants, and served a subpoena on Yahoo! seeking the disclosure of their identities. Yahoo! complied with the subpoena, disclosing Aquacool_2000’s real-world identity, without notifying him or seeking his consent. Upon learning Aquacool_2000’s identity, AnswerThink fired him and took other punitive action against him.

Aquacool_2000 then filed this action against Yahoo!, alleging that the disclosure of his identity violated his free speech rights under the U.S. and California Constitutions, and that it constituted unfair competition and false advertising under California law. He also alleged that Yahoo! was in breach of contract, and had committed negligent misrepresentation, by failing to abide by its website privacy policy. The policy stated: “We will notify you at the time of data collection or transfer if your data will be shared with a third party and you will always have the option of not permitting the transfer.” It also stated that Yahoo! would disclose a member’s personal information “when we believe in good faith that the law requires it.”

How would you interpret the quoted provisions of Yahoo!’s Privacy Policy? Do you think Yahoo! violated the policy when it revealed Aquacool_2000’s identity in response to the subpoena? Is this policy an enforceable contract? Yahoo! later modified its Privacy Policy so that it states: “We respond to subpoenas, court orders or legal process,” and does not promise any notification that it is doing so.

4. Anonymous plaintiffs? In America Online, Inc. v. Anonymous Publicly Traded Company, 542 S.E.2d 377 (Va. 2001), plaintiff brought a defamation action against defendants who had anonymously posted disparaging comments concerning plaintiff. Plaintiff sought to protect its own anonymity in the litigation, arguing that disclosure of its identity would cause irreparable harm. Plaintiff caused a subpoena to be issued to America Online requiring it to identify the John Doe defendants. AOL resisted the subpoena, “arguing that APTC should not be permitted to proceed until it revealed its identity.” The trial court ruled that the plaintiff could proceed anonymously, but the Virginia Supreme Court disagreed. The court began by observing that “courts must balance the need for anonymity against the general presumption that parties’ identities are public information and the risk of unfairness to the opposing party.” It held that the plaintiff had not made the required showing. “In the case before us, the sole reason APTC has offered in support of its request to proceed anonymously is fear of economic harm. While reasonable concern over potential economic harm is not excluded from factors to consider, APTC has not borne its burden to show special circumstances justifying anonymity.” The court was not impressed by the plaintiff’s conclusory assertion that “the filing of this lawsuit under the proper and correct legal name for the Plaintiff, where Plaintiff at this time is unable to identify the Defendants, will trigger publicity about this lawsuit, which Plaintiff believes will damage the value of the corporation.”