Indecent Exposures in an Electronic Regime

Natalie L. Regoli*

* B.A., The University of Washington, 1996; Candidate for J.D., The University of Texas School of Law, 2002. I would like to thank Professor Stuart M. Benjamin for his thoughtful comments on an earlier draft of this essay.

I. INTRODUCTION

"The privacy that any computer user would and should and is justified in expecting is illusory; Big Brother shrunk to a miniature cyber spy always looms and never sleeps."[1] This is because an Internet user's online activity leaves electronic footprints, commonly called a "clickstream," that businesses routinely use to collect and create user profiles of personally identifiable data that they later use and sell. As the Internet is now a part of virtually every aspect of our lives, this process introduces wide-ranging dangers regarding personal autonomy and dignity. Professor Lawrence Lessig explains that "[t]he system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins again."[2] This constant surveillance shifts power over one's identity from the user to the commercial entity, absorbing individuality and self-determined independence. It destroys the feeling of freedom brought by anonymity and the ability to be free from unsanctioned intrusion. And, it is pervasive. In fact, in a recent lawsuit, Universal Image accused Yahoo! of watching, spying, conducting surveillance, and analyzing "the habits, inclinations, preferences, and tastes, and otherwise . . . follow[ing] and stalk[ing] those who visit the . . . site."[3] Without recourse to an effective privacy law, Universal Image has resorted to suing Yahoo! for violations of the criminal and civil theft laws, criminal stalking laws, civil conversion laws, and civil trespass laws.[4] Indeed, in the largely unregulated cyber realm, the applications of computer technology have introduced new possibilities for marketers, insurance companies, employers, and other interested parties to profit from users' personal information in a variety of ways. Given the ubiquity of unauthorized online profiling, what changes should be made to safeguard privacy?

As the topic of data privacy is vast and the subject of much scrutiny, this Comment focuses narrowly on commercial cyber-activities relating to the nonconsensual Internet acquisition of personally identifiable user data. This Comment begins with a brief examination of the technology that has exacerbated privacy law's inadequacies. It briefly discusses failed attempts to safeguard privacy rights through the market and federal agency

1. Plaintiff's Second Amended Verified Original Petition, Application for Temporary Restraining Order and Temporary Injunction, at 34, Universal Image Inc. v. Yahoo, Inc., (Dallas County Ct. Tex. filed Jan. 18, 2000) (No. 99-13839-A), *at* http://legal.web.aol.com/decisions/dlpriv/univtro2.pdf [hereinafter *Plaintiff's Second Amended Petition*].

2. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 154 (1999).

3. *Plaintiff's Second Amended Petition*, *supra* note 1, at 36.

4. *Id.* at 16-21, 34-39.

management. It then addresses current U.S. privacy legislation and the 1995 European Privacy Directive. Finally, this Comment proposes the creation of a new legislative system to effectively combat the surreptitious collection, storage, use, and sale of personal data.

II. THE NEW FRONTIER OF WOE

Cyberspace introduces new privacy concerns. Its lack of physical boundaries enables abusers to invade privacy with greater ease, efficiency, and power than has been experienced in the offline world. What once required extraneous methods of snooping, such as the manual planting of listening devices or the tapping of phones, can now be done universally and inexpensively through the online monitoring of clickstream data and built-in computer hardware. This invasion of privacy can also be done in much greater detail. Unlike a transaction receipt in the physical world that simply evidences a completed transaction, clickstream data is a record of a user's every online keystroke.[5] Realizing its value, many online businesses, including Yahoo!, RealNetworks, DoubleClick, and Amazon.com, actively accumulate personally identifiable visitor information while an individual visits their sites.[6] Yahoo! President Jeffrey Mallet even publicly stated that the information Yahoo! surreptitiously collects from users is its "single greatest asset."[7] Internet Service Providers ("ISPs") possess even greater collection abilities, as they can record a user's entire clickstream because the ISP is the user's gateway to the Internet. Further, the decentralized nature of the Internet guarantees the ability easily and instantaneously to transfer accumulated data to any party, anywhere in the world, at any time.

Most browsers make information collection easy by disclosing the referring page to a subsequent site every time a person clicks on a link, along with their name or e-mail address, if it has been entered in the browser's software.[8] This feature cannot be turned off.[9] Although users can purchase software to disguise themselves while online, they may encounter situations where they have to disclose personal information in order to get a desired benefit, such as making purchases, registering for free services, or filling out surveys.[10] By default, most browsers also enable Web sites to

5. WEBOPEDIA, *at* http://www.webopedia.com/TERM/c/clickstream.html (last visited Jan. 25, 2002).

6. *See, e.g.*, *Plaintiff's Second Amended Petition*, *supra* note 1, at 4.

7. *Id*.

8. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1486 (2000).

9. *Id*.

10. *See* Freedom Privacy & Security Tools *at* http://www.freedom.net (last visited Oct. 2, 2001); Anonymizer Privacy Button *at* http://www.Anonymizer.com (last visited Oct. 2, 2001).

read "cookies," which allow the information a user gives to the Web site to be stored and used to create a user profile. Cookies may be used to silently track and record search terms, visited sites, and articles read in order to build a detailed profile from information given to other Web sites; this data can be shared between Web sites.[11] Moreover, software makers like Microsoft routinely exploit their collection abilities by embedding unique identification numbers into documents so that documents transmitted through Ethernet cards can be traced back to the sender's computer.[12] Additionally, computer hardware makers, like Intel, have stealthily built tracking features into their systems, making electronic anonymity nearly impossible.[13] More drastically, the upcoming Internet protocol version most likely will use a computer's Ethernet card to establish a permanent globally unique identifier ("GUID"), creating unalterable fingerprints for each computer.[14]

III. LAW IN AN ELECTRONIC REGIME

A. Failed Avenues

Internet threats to individual privacy abound, and many agree that it is necessary to end the clandestine private sector invasion of individuals' cherished ability to control the uses of their personal information.[15] Internet users should be empowered to make informed decisions about explicitly trading their personal dossiers for desired benefits. Various approaches exist to facilitate this end—among them self-regulation and legislation—and it is important to examine each to understand why the creation of new legislation for protecting online privacy is now necessary.

1. The Market Approach

Studying online privacy issues since 1995, the Federal Trade Commission ("FTC" or "Commission") found through its first online survey in 1998 that 92% of Web sites collected personal information from

11. Froomkin, *supra* note 8, at 1486. According to Webopedia, an online data source, cookies are defined as messages given to a Web browser by a Web server to store and then send back to the server each time the browser requests a page from the server. *Cookie*, WEBOPEDIA *at* http://webopedia.Internet.com/TERM/c/cookie.html (last visited Sept. 18, 2001). The main purpose of cookies is to identify visitors and to customize Web sites for them. *Id.*

12. Froomkin, *supra* note 8, at 1492.

13. *Id*. at 1490.

14. *Id*. at 1525.

15. *See, e.g.*, Froomkin, *supra* note 8, at 1461.

online visitors, but only 14% disclosed their collection practices.[16] The FTC advocated industry use of "the widely-accepted fair information practice principles of *notice*, *choice*, *access*, and *security*."[17] Despite its efforts, in 1999 the Commission reported "that only 10% of the sites posted disclosures that even touched on all four fair information practice principles."[18] Still, the Commission recommended that self-regulatory efforts be given a chance to work.[19] The FTC's attitude changed in 2000, however, when it found that despite its recommendations, 97% of Web sites collected an e-mail address or some other type of personally identifying information while only 20% even partially implemented the four fair information practice principles.[20] Moreover the Commission found that only 8% of Web sites participated in the industry's self-regulatory enforcement initiative—online privacy seal programs—and concluded that reliance on industry efforts was futile.[21]

This is a classic case of self-regulatory failure. Businesses, given ample time to get things right, have chosen to steal information aggressively and secretly from citizens while maintaining a façade of effort to self-regulate and to comply with governmental requests to take action. While the government has patiently encouraged industry to act, harvesting personal data has become a $1.5 billion market.[22] This market is comprised of "data warehousing" businesses like Acxiom and First Data that collect and sell information such as ethnic and religious affiliations, property purchases and loan data, travel destinations, and even pet ownership on 165 million Americans.[23]

These covert undertakings are further disguised by companies such as TRUSTe.com, which licenses online merchants with "trustmarks" and provides users with a false sense of security.[24] Although TRUSTe.com is currently the most successful self-regulatory program, it does not assess the

16. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, at i (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf [hereinafter *FTC Privacy Report*].

17. *Id*. (emphasis in original).

18. *Id*. (quoting Georgetown Internet Privacy Policy Survey).

19. *Id*.

20. *Id*. at ii.

21. *Id*.

22. Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 776 (1999).

23. *Id*. These statistics may be verified at http://www.acxiom.com (last visited Nov. 30, 2001).

24. Froomkin, *supra* note 8, at 1525. *See also* Reidenberg, *supra* note 22, at 778 (discussing the similar failure of BBBOnline, the project of the Better Business Bureau).

quality of the privacy policy, conduct an audit, or revoke certification if the online licensee violates its own privacy policy. Licensees only need to pay a licensing fee and have a privacy policy in existence to obtain a trustmark.[25] To illustrate the falseness of this supposed privacy protection system, TRUSTe.com declined to revoke GeoCities' trustmark even after the FTC brought charges against GeoCities for collecting and disclosing detailed consumer information to marketers—including e-mail addresses, postal addresses, income, education, gender, marital status, and occupation—despite GeoCities' promise that customer registration information would not be released without the customer's permission.[26] Another trustmark holder, RealNetworks RealJukebox Software, created and transmitted GUIDs through the Internet to catalog an individual's listening habits whenever the individual used the software.[27] Even though RealNetworks' privacy policy concealed this practice, TRUSTe.com again declined to revoke RealNetworks' trustmark.[28] Nor did TRUSTe.com revoke Microsoft's trustmark after discovering that Microsoft routinely sent GUIDs during Windows 98 registrations when users expressly denied Microsoft permission to do so.[29]

The fraudulent nature of this system is not surprising, as TRUSTe.com and other certification programs have no incentive to strangle their sole revenue sources.[30] Considering that the vast majority of the public may be unaware of this misrepresentation and believes in the illusion of safety created by the placement of a trustmark on a Web site, this misplaced trust may lower users' personal guards, leading them to reveal more information than they would in situations without the appearance of the privacy-ensuring mechanisms. These user perceptions may ultimately result in a situation more detrimental to users than the absence of privacy policies or trustmarks altogether.

2. The Agency Approach

In May 2000, the FTC recommended legislative standards for online data acquisition activities and the creation of an agency to implement these standards and to promulgate further legislation.[31] The proposed legislation would explicitly require all consumer-oriented commercial Web sites to

25. Froomkin, *supra* note 8, at 1525.
26. *Id*. at 1526.
27. *Id*. at 1525.
28. *Id*.
29. *Id*.
30. *Id*. at 1527.
31. *FTC Privacy Report*, *supra* note 16, at 36.

comply with the four widely accepted fair information practice principles: notice, choice, access, and security.[32]

At the outset, it is unclear why the FTC observed an industry secretly profiting from users' stolen personal information for five years before making any legislative recommendation. Public choice theory would explain this behavior by arguing that administrative officials are strategic actors, using the regulatory processes to showcase their career talents and to gain the favor of prospective industry employers by changing policies in subtle ways.[33] The consequence of such behavior is that agencies are "captured" by the entities that they are supposed to be regulating.[34] This may elucidate why the FTC allowed online industries to profit for such an extended period before proposing regulation. Public choice theorists argue that bureaucrats, like other rational economic actors, seek to maximize their influence on public policy, their discretionary budget, their power, and their utility.[35] By prolonging its involvement in the online privacy debacle, the FTC might have been attempting to secure its position and power over future Internet-related policies.

Another problem with the FTC's approach is that it lacks a coherent understanding of information technology. This problem has led to a proposal that fails to protect individual privacy rights adequately. For example, although the FTC recommended that Web sites be required to provide users access to collected information, it could not define "access," admitting that the term could mean total access, partial access, or access only when the Web site "uses the personal information to grant or deny significant benefits to an individual, and where granting access would improve the accuracy of the data in a way that justifies the costs."[36] Depending on the definition, the proposed level of required "access" could actually become "no access." The Commission's other proposed principles provide equally scarce guidance regarding how online entities are to comply with the fair information practice principles.[37] This attempt to avoid defining key terms that serve as foundations of proposed regulation and to jump straight into structuring the regulation is perplexing.

32. *Id*.

33. Roger G. Noll, *Economic Perspective on the Politics of Regulation, in* II HANDBOOK OF INDUSTRIAL ORGANIZATION 1277, 1278 (1989).

34. *Id*.

35. Ronald Wintrobe, *Modern Bureaucratic Theory, in* PERSPECTIVES ON PUBLIC CHOICE 429, 431 (Dennis C. Mueller ed., 1997).

36. *FTC Privacy Report*, *supra* note 16, at 31.

37. *Id*.

Indeterminate definitions amplify risks of capture.[38] In deciding the appropriate parameters of proposed privacy regulations, bureaucrats may yield to the well-explicated concerns of business lobbyists to the detriment of unorganized and unheard individuals.[39] But concrete statutory definitions also pose risks. Static structures are ill-suited for the governance of an extremely dynamic system, are complicated by the burden of designing detailed regulations to address different data acquirers (i.e., online merchants, employers), and at some point eventually render the legislation inapplicable or inadequate to deal with the latest state of technology.[40]

Neither industry self-regulation nor federal agency protection hold much promise for improving cyberspace privacy. In light of this deficiency, legislation that builds universal privacy rights into the foundation of the system without mandating the need for a victim to undergo costly and uncertain *ex post facto* litigation is the most viable route.

B. Qualified Legislative Success

The United States' track record is rife with piecemeal approaches to patch up privacy leaks after they have sprung. Congress has attempted to fix targeted areas with narrow privacy legislation: the Privacy Act of 1974, to provide individuals more control over the data the government collects about them;[41] the Freedom of Information Act, to increase governmental agency information disclosures;[42] the Fair Credit Reporting Act, to protect consumers against inaccurate credit information;[43] and the Video Privacy Protection Act, to prevent the disclosure of video tape rental or sale records.[44] Only the Electronic Communications Privacy Act addresses the interception and disclosure of cyberspace data by nongovernmental actors, but it is of little use for profiling activities because it exempts data that is

38. Terry Moe, *The Positive Theory of Public Bureaucracy*, *in* PERSPECTIVES ON PUBLIC CHOICE 455, 462 (Dennis C. Mueller ed., 1997). According to George Stigler, the capture theory asserts that special business interests organize for political action more than taxpayers and other large groups do. This is the case because the small number of companies in each industry makes possible an increase in the concentration of benefits each company receives from rules designed on its behalf. *Id.*

39. Noll, *supra* note 33, at 1277.

40. Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1424 (1987).

41. *See* 5 U.S.C. § 552a (2000).

42. *See id.* § 552. Parenthetically, as written, the Freedom of Information Act raises the concern that it grants third parties increased access to information that would have been private before the Act. *Id.* § 552 note (Supp. V 1999)

43. *See* 15 U.S.C. §§ 1681a-1681u (1994 & Supp. V 1999).

44. *See* 18 U.S.C. § 2710 (1994).

readily available to the public.[45] Despite its acknowledgment of the need for greater Internet privacy, Congress has not been receptive to proposed legislation addressing online profiling, partly because of intense lobbying by industry[46] and partly because previous administrations were reluctant to regulate Internet-specific concerns.[47] Not surprisingly, today, the FTC's proposal languishes unpassed.

1. Multinational Consensus

Contrary to the U.S. government's position, what is needed is a structure that recognizes a fundamental, but alienable, right to data privacy and that strictly controls entities that profile Internet users on a worldwide basis. The European Directive guarantees a broad floor of basic rights for individual control of personal data collection, storage, use, disclosure, and access to stored data for error correction.[48] Under this omnibus legislation, Member States are required to enact national laws that conform to the Directive's comprehensive standards and maintain an independent data controller to oversee and enforce the standards.[49] The Directive is a "comprehensive endorsement of 'First Principles,'" a set of fair information practices that assure individuals' participation in the acquisition and use of their personal data.[50]

The First Principles have gained wide acceptance, as the United States, Europe, the United Nations, the Organisation for Economic Co-Operation and Development ("OECD"), and New Zealand have committed to these practices in the course of their establishment over the last thirty years.[51] The First Principles concern four main categories of standards: "(1) data quality; (2) transparency or openness of processing; (3) treatment of particularly sensitive data, often defined as data about health, race, religious beliefs, and sexual life, among other attributes; and (4)

45. *See id.* § 2510 (1994 & Supp. V 1999). *See supra* text accompanying notes 13-14 discussing that "public" includes information that people consider private.

46. Graham, *supra* note 40, at 1428 n.165.

47. *Internet Privacy and Electronic Communications: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 25-26 (1998) (statement of David L. Aaron, Under Secretary, International Trade Administration, Department of Commerce) (explaining that enforcement of Internet regulations would be difficult, would demand extensive governmental resources, and would give users a false sense of security).

48. Council Directive 95/46, art. 1, 1995 O.J. (L 281/38) 31, *available at* http://www.europa.eu.int/eurlex/en/search/search-oj.html.

49. *Id*. art. 6.

50. Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1326-29 (2000).

51. *Id*. at 1327-29.

enforcement mechanisms."[52] More exactly, the analysis of Colin Bennett and Rebecca Grant regarding national data privacy legislation reveals First Principle policy convergence into ten main standards for commercial entities:

> [1] Must be *accountable* for all personal information in its possession;
>
> [2] Should *identify the purposes* for which the information is processed at or before the time of collection;
>
> [3] Should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances);
>
> [4] Should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes;
>
> [5] Should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the *finality principle*);
>
> [6] Should *retain* information only as long as necessary;
>
> [7] Should ensure that personal information is kept *accurate*, *complete*, and *up to date*;
>
> [8] Should protect personal information with appropriate *security safeguards*;
>
> [9] Should be *open* about its policies and practices and maintain no secret information systems;
>
> [10] Should allow data subjects *access* to their personal information, with an ability to amend it if necessary.[53]

Although developed for privacy protection generally, these guidelines are applicable to regulating online activities, as demonstrated by the European Directive.

2. Lessons Learned

Admittedly, the European Directive is an accomplishment far ahead of anything the United States has achieved for privacy rights. Nevertheless, the Directive has its problems. Critics have criticized it for failing to adequately enforce compliance with its requirement that all people processing personal information notify the data controller of their activities.[54] Critics also charge that the Directive fails to harmonize the differences in national interpretation and implementation of the laws applying it.[55] These challenges are mitigated, however, by a working group composed of the Member States' data-protection controllers that creates a

52. *Id*. at 1326.

53. *Id.* at 1326-27 (quoting Colin J. Bennett & Rebecca Grant, *Introduction*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 6 (Colin J. Bennett & Rebecca Grant, eds. 1999)) (emphasis in original).

54. Reidenberg, *supra* note 22, at 784.

55. *Id*.

formal channel through which Member States can consult and reach consensus on the interpretation of different Directive provisions.[56] In addition, to combat divergences in the execution of the standards, the Directive includes a provision for consensus on industry codes of conduct that can be used to certify privacy-assuring technologies.[57]

Notable difficulties remain, however, as the European Directive strains global business relations. The Directive creates tension for global information networks by including provisions that ensure European personal information will be handled according to European standards. These provisions also provide the authority to restrict transborder data flows to countries that do not have the appropriate level of privacy protection.[58] Moreover, these statutory attributes pressure non-Member States to enact Europe's subjective determination of appropriate privacy protections in order to continue information-related business transactions with them.

The five-year period over which the European Directive was negotiated, and the additional three years that it took to implement the Directive into law,[59] amounted to a substantial delay severely misaligned with the fast pace of the Internet. By the time the Directive was finally implemented, much abuse had already been allowed to pass unchallenged.[60]

These problems, and those known to be inherent in legislation generally, present opportunities from which the United States could learn in the construction of a superior privacy protection system. The U.S. government must overcome its reluctance to regulate the Internet and act to protect its citizens from commercial exploitation. Internet-facilitated commercial exploitation of personally identifiable information has given bricks-and-mortar marketers an inexpensive way to accumulate extensive information on consumers and prospective consumers at a level of detail not possible in the physical world. Clickstream data can be used to create permanent and easily disseminated records of a user's every online keystroke. Users are powerless to control this practice. This scenario is analogous to being incessantly stalked through a random walk in a mall, down a street while window-shopping, or while purchasing a cup of coffee with cash, with the stalker's intricate observations sold and used to target

56. *Id*. at 785.

57. *Id*.

58. *Id*. at 786.

59. *Id*. at 787.

60. Council Directive 95/46, *supra* note 48, 31-50 ("Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier . . . .").

the stalked victim. Perhaps falling behind Europe in this important area will spark the United States' competitive spirit and give it the impetus to fulfill its duty to protect its citizens.

C. Making Legislation Work

1. Proposing New Legislation: The Federal Umbrella Statute

A potential solution to the current privacy disaster is a legislative umbrella structure consisting of both the federal government and the state governments. Under this scheme, the federal government would promulgate a statutory mandate that all states appoint independent quasi-governmental agencies to enact laws in line with the objectives of the First Principles to protect Internet users against online commercial profiling. For the purposes of this discussion, this federal statute will be called the "Online Commercial Privacy Act" ("OCPA"). State governments would completely control the construction of their own independent agencies, which would have wide latitude in statutory promulgation. The federal government would then appoint its own independent quasi-governmental agency to oversee the states' progress. This structure would continue indefinitely, until the federal agency determined that national alignment was needed, or until the agency determined that the states' progress was insufficient. The OCPA would create the following rudimentary statute:

ONLINE COMMERCIAL PRIVACY ACT

(a) **Establishment of a Federal Agency**. There is established a federal independent quasi-governmental agency to be known as the Agency on Privacy in Commerce (in this title referred to as the "Agency").

(b) **State Agencies**. Each state must establish an independent quasi-governmental agency to create default-rule privacy protections for Internet users clearly consistent with the First Principles of the European Directive. Each state will be responsible for protecting Internet users accessing the Internet through Internet Service Providers located in its state. State agencies must establish auditing and enforcement procedures that provide remedies to individual victims, create consequences for violators, and ensure the operational effectiveness of their legislative enactments. No other provisions of this Act will apply to the state agencies.

(c) **Membership in Federal Agency**.

(1) *In General*. The Agency members shall serve for the life of the Agency. The membership of the Agency shall be as follows:

(A) Two (2) representatives from the federal government, one appointed by the Majority Leader of the Senate, and one appointed by the Minority

Leader of the Senate.

(B) Two (2) representatives from state and local governments, one appointed by the Speaker of the House of Representatives, and one appointed by the Minority Leader of the House of Representatives.

(C) Two (2) representatives from the electronic commerce industry, comprised of:

(i) One (1) representative from a large business in the electronic commerce industry, who does not have the same political party affiliation as that of the small business representative. This representative shall be appointed by the Majority Leader of the Senate.

(ii) One (1) representative from a small business in the electronic commerce industry, who does not have the same political party affiliation as that of the large business representative. This representative shall be appointed by the Minority Leader of the Senate.

(D) Two (2) representatives from consumer advocacy groups, one appointed by the Speaker of the House of Representatives, and one appointed by the Minority Leader of the House of Representatives.

(E) One (1) representative from education or academia, elected through a Congressional vote.

(2) *Vacancies*. Any vacancy shall be filled in the same manner as the original position.

(d) **Acceptance of Gifts and Grants**. Agency members may only accept gifts or grants for the exclusive and complete purpose of promoting the goals of the Agency. Gifts or grants shall become the property of the Agency. The amounts of all gifts or grants, the name of the donor party, any corporate or entity affiliation of the donor party, and a detailed description of the gift or grant must be disclosed in the public record.

(e) **Other Resources**. The Agency shall have reasonable access to the resources of the federal government.

(f) **Agency Rules**.

(1) *Quorum*. Eight members of the Agency shall constitute a quorum.

(2) *Meetings*. All meetings shall be closed to the public.

(3) *Records*. Complete and accurate records shall be kept at all meetings. Records of aggregate committee decisions shall be open to the public. Records open to the public will not disclose the individual votes of the members.

(4) *Actions*. Decisions to act by the Agency must be unanimous.

(g) **Duties of the Agency**.

(1) *In General*. The purpose of the Agency is the evaluation and recordation of state progress. To achieve these purposes, the Agency shall

conduct thorough and extensive studies of all state treatment of online privacy protections from Web organizations. The Agency shall review the states' progress, determine if progress has been sufficient, and administer changes as needed based on existing state infrastructures. Although the Agency will have the authority to align states' privacy systems with the goals of the First Principles, its primary objective is to monitor systems created and administered by the states themselves.

(2) *Issues To Be Studied*. The Agency shall conduct thorough and extensive studies annually to monitor states' progress and the corresponding effects on the individual user, the industry, and the economy. Such studies may include tracking of user-contracting and default-rule usage, types of data collection by commercial entities, revenue trends for online companies, revenue trends for the data trade generally, Internet commerce trends, Internet usage trends, Internet activity trends, and related activities.

(3) *Authority For Action*. The Agency shall have the authority to exchange legislation adopted in one state with that of another state, or with that from a combination of states, if the Agency determines that a state or states are substantially misaligned with the First Principle goals of privacy protection. The Agency will give deference to states' actions when it is in doubt as to whether the degree of misalignment justifies federal agency intervention.

(4) *Reporting*. The Agency will compile a comprehensive official report on an annual basis that details its findings and its current position. This report will be made available to the public.

a. State Responsibilities

Each state would create an independent body to develop default rule protections for Internet users in accordance with the First Principles. States would then govern online profiling issues locally unless the federal agency, through its annual study and review process, concluded that state efforts were not adequately ameliorative. In this case, the federal agency would have the authority to harmonize state laws based on one or more of the empirically tested privacy systems established by the states. In this way, states would function as miniature think tanks, which would resume local control after harmonization to continue adjusting their legislation to the changing needs of the online world.

The default rules would set laws by which profiling entities would have to abide, unless those entities contracted alternate agreements with individual users. The structure of the default rule would be very important because it would allocate the burden of attaining the visitor's personal data. Adherence to the First Principles mandates that commercial entities obtain

knowledge and consent before collecting personal data; however, what constitutes "knowledge" and "consent" is arguably ambiguous, and would profoundly affect overall privacy protection. For instance, a default rule structured for enhanced user protection might interpret "knowledge" as a completely informed understanding for specified levels of profiling activity (i.e., collection, use, sale) after the Web site has disclosed the purposes of the activities and the third parties involved (i.e., sale to X.com for the purpose of soliciting visitors).

The rule might interpret "consent" as stringently: explicit permission granted by the user after being directly approached by the Web site on the user's first visit. In contrast, a default rule lenient to businesses might interpret "knowledge" as the awareness that online profiling is widespread, and "consent" as merely placing oneself in cyberspace. In essence, definitional distinctions could create state conditions that span the spectrum from opt-in to opt-out clauses. Clearly, these implementations would have starkly opposite consequences, perhaps resulting in no statute at all in some states as a practical matter. Even with protection disparities across states, although impossible to quantify, this system would probably still result in greater overall privacy protection. This is likely because a decentralized structure would help to mitigate the risk of special interest groups dominating the process while federal oversight keeps outliers in check.

This statute would require businesses to comply with the state regulations in which their visitors' ISPs resided. Logistically, commercial entities would be able to code for automatic identification of a visitor's Internet Protocol address and the subsequent tracking of the ISP server location, linking that entity's profiling procedures to the resultant state's statutes. This linking of compliance to the location of visitors' ISPs acts as a disincentive for state agency officials to structure business-friendly state legislation in an attempt to procure favors or attract lucrative business to the state.

Admittedly, such a system would place a disproportionate cost burden on smaller companies, who would have to allocate a larger percentage of their operating budgets than would larger companies in order to comply with the various state regulations. With the advent of a federal umbrella statute, an enterprising computer engineer or software company would logically create a software package to automate this task for businesses across the nation, complete with software patches to upgrade the software for changes in regulations as necessary. The availability of such commercial software would presumably decrease the total cost for

businesses to comply with the federal umbrella statute,[61] though not alleviate the disparate cost between large and small businesses as a percentage of their operating budgets. Ultimately, the additional cost for such software would not seem to be a problem that would outweigh the benefits of the federal umbrella statute.

Moreover, the federal umbrella statute would most likely protect state citizens against actions of offshore businesses and the tax system against businesses relocating offshore to circumvent the profiling statutes. New Internet jurisdictional issues are already beginning to be settled, for example, in the area of Internet gambling. Internet gambling through servers licensed and located offshore has been held illegal under the Federal Interstate Wire Act, the Travel Act, and the Interstate Transportation of Wagering Paraphernalia Act, if the person who is gambling is physically present within the United States.[62] Courts have held that personal jurisdiction may be established even though the gambling businesses are physically located offshore.[63] Courts have also held that operators of Internet gambling enterprises cannot move their computer servers offshore to divest a state of its jurisdiction and escape liability. [64] More specifically, if an individual logs onto the gambling site from a given state and places a bet, the gambling is deemed to have taken place there, in violation of both federal and state law, and is prosecutable in that state.[65]

61. According to David L. Randall, a computer software engineer located in Austin, Texas, design of such software would not be prohibitively difficult, and would take approximately one "man-year" to develop. If the cost for the creation of such software were estimated at approximately a one-year salary for a software engineer capable to design such a system, the design cost for the software could be estimated at $75,000. As most business software is sold for over $100, and as there are well over 750 businesses that would have to comply with the federal umbrella statute, the profit on such software would be substantial. This potential for substantial profit by the developer of such software makes it extremely likely that it would be made available on a commercial basis at a price that is less than the cost of the total initial development and somewhat on par with other commercial software. Interview with David L. Randall, Computer Software Engineer, Sculpted Systems. (Mar. 2001).

62. Joel Michael Schwarz, *The Internet Gambling Fallacy Craps Out*, 14 BERKELEY TECH. L.J. 1021, 1069-70 (1999).

63. State v. Granite Gate Resorts, Inc., 568 N.W.2d 715 (Minn. Ct. App. 1997), *aff'd by an equally divided court*, 576 N.W.2d 747 (1998) (finding personal jurisdiction over a non-resident Internet gambling business based on Internet and physical-world contacts). *See also* Thompson v. Handa-Lopez, Inc., 998 F. Supp. 738 (W.D. Tex. 1998) (finding personal jurisdiction over a nonresident Internet gambling business based on the defendant's advertising in Texas, permitting the Texas plaintiff to log in and gamble from Texas, and sending prize money to the Texas plaintiff).

64. People v. World Interactive Gaming Corp., 714 N.Y.S.2d 844 (N.Y. Sup. Ct. 1999). *See also* L.E. Servs, Inc. v. State Lottery Comm'n, 646 N.E.2d 334 (Ind. Ct. App. 1995) (holding that gambling takes place in the state from which the transmission originated).

65. *See generally World Interactive Gaming*, 714 N.Y.S.2d 844; *L.E. Servs*, 646 N.E.2d

Similar applications of jurisdiction to Internet privacy violations would help protect state citizens and discourage businesses from relocating in an attempt to evade privacy legislation.

The federal umbrella statute would also require state independent agencies to enact auditing mechanisms to ensure business compliance with state statutes and enforcement mechanisms that provide remedies to individual victims and appropriate consequences to violators. Although state independent bodies would have complete control of the creation of their auditing and enforcement mechanisms, one approach for enforcement could be to provide Web-based complaint forms at the state level that could initiate an investigation into the practices of the named entity.

b. Federal Supervision

The federal independent quasi-governmental agency would have extensive powers and be small, consisting of delegates from different groups to represent a diversity of viewpoints. The agency's role would be to annually review states' progress and conduct studies to determine if progress had been sufficient. It would have the authority to transplant legislation adopted in one state with that of another state if the agency determined that a state was substantially misaligned with the privacy protection goals of the First Principles.

This decentralized umbrella structure is potentially, but not necessarily, a final solution. After a few years of evaluation, the independent federal agency could determine that some states have created substantially more attractive infrastructures than other states, and decide to implement one state's or a combination of states' infrastructures on a national level. If this implementation were to occur, states would automatically regain full control of their local laws after harmonization, and would be allowed to modify their systems as long as such modification would not result in a decreased level of "clearly consistent"[66] compliance with the goals of the First Principles. Review would repeat indefinitely on an as-needed basis. The federal agency could also determine that the majority of states have developed laudable protections that, while possibly divergent, nonetheless adequately achieved the First Principle goals and did not cause notable economically or socially adverse consequences. In such a case, states would continue to operate their local infrastructures without the federal harmonization process.

334.

66. *See* discussion *supra* Part III.C.1.

If negative externalities arose from substantial disparities, such as business discrimination against citizens of the more heavily protected states or a distortion of interstate competition, the federal agency would rectify the situation by applying one state's or a mixture of states' frameworks on a national level. Additionally, the federal agency would generally defer to state judgment, be sympathetic to local control over federal control, and favor greater privacy protections over more relaxed standards.

2. System Implications

The federal umbrella structure would benefit all parties—users, industry, and government.

a. Users Would Be More Protected

A combined system provides for more user protection than local or federal legislation alone would accomplish. Because the federal agency would be sympathetic to individual privacy, the umbrella structure would embed extra safeguards into the legislative system. In the event that an individual resided in a probusiness state whose independent agency failed to implement adequate default rules, the federal agency would bring that state into line. Although not infallibly prophylactic, this decentralized structure helps prevent successful industry lobbying efforts and agency capture through an exponential increase in and spreading of industry targets, leading to greater privacy protection on average.

The addition of independent state agencies to the regulatory regime permits the establishment of default rules sensitive to local cultural issues, and faster responses to cyberspace change. Local authority also enables more thorough auditing and enforcement coverage than would occur from a more removed federal level.

By adopting objectives based on the First Principles, the federal government guarantees Internet users a baseline of privacy protection. These objectives have been developed over thirty years, have gained multinational consensus, and have been adopted into many laws across the world. Users can accordingly have a higher degree of confidence in these rules than may be the case with a framework quickly assembled solely by our state and federal governments.

The default rule system is a fantastic advancement for user privacy protection because it allows a context-specific assessment of the value of personal data to that user. If a user places higher value on her personal data than does the commercial entity, the user's right to retain the confidentiality of her data will be ensured. On the other hand, if the commercial entity places a higher value on the user's data than does the

user, the commercial entity will be able to use that data and the individual will be entitled to whatever enticements are traded for that permission. This arrangement is beneficial for users, because setting a default rule for the way a commercial entity must operate, unless otherwise agreed, corrects the power disparity between the user and the information broker. The arrangement is further beneficial because it mandates that users have all of their personal data completely hidden unless they permit otherwise. The arrangement insists that users be given an actual choice about whether or not their information is gathered and used. Finally, the arrangement structures the relationship such that the business must somehow compensate the normal, nonexhibitionist user for the benefit of profiting from that individual's identity information.

b. Industry Would Benefit from Tested Fundamentals and Clear Cost-Benefit Analysis

Under the umbrella structure, a number of different systems—perhaps even fifty—would be tried and tested, decreasing the risk to industry that an overly onerous standard would be promulgated on a national level. Likewise, structuring default rules around the First Principles infuses the system with an element of safety because these Principles have been developed over time and adopted internationally. Further, this system would force American businesses to comport with global standards, would simplify international business transactions, and would bring new opportunities.

The development of default rules provides industry with clear expectations of required behavior and allows commercial entities to contract around the rules in cases where the benefits of contracting outweigh the transaction costs. Promulgation at the state level helps local businesses by infusing the process with an understanding of local cultural business issues. Although their perspectives would depend on their compositions, state agencies would certainly frame legislation with more of a local understanding than federal authorities that comprehensively promulgate regulations for all fifty states. State agencies would also have more flexibility than the national government, due to their smaller territorial responsibility. The corresponding enhanced agility in initial implementation and response to technological changes would help to minimize business uncertainty over future developments and sunk costs for business strategies involving newly-prohibited activities. At the same time, retaining federal oversight provides a monitoring capacity to check potentially draconian local enactments.

c. Federal and State Governments Would Benefit

By structuring default rules around the First Principles, the federal government achieves a privacy floor for users and increased opportunities for American business. This both accommodates major constituents and simultaneously fosters international appreciation for its steps toward the global harmonization of privacy standards. Further, it avoids the resource-intensive process of developing its own objectives. In addition, the government would presumably realize enhanced tax revenues from the expanded American business opportunities abroad stemming from new international trust in American business activities. Concededly, this may be partially offset by a decrease in tax revenues due to limitations on profiting from surreptitious profiling activities.

The federal government would gain valuable data regarding potential regulatory schemes through empirically-tested privacy systems from its state-composed think tank, using the states as test cases for the development of an appropriate national framework in the event one became necessary. Meanwhile, the federal government would be able to retain ultimate control over the process and deploy fewer resources than would be necessary to maintain such a system under national legislation.

State agency delegation would be faster overall than would be possible in the federal legislature because of the reduced diversity of interests and constituents to appease. This expediency would mitigate the risk of legislation lagging even farther behind an increasingly entrenched Internet architecture. A corollary benefit would be mitigating the risk that online privacy concerns will stunt the proliferation of online commerce if individual privacy interests are unbalanced with the benefits of the Internet. Additionally, the feasibility of speedily implementing protections would minimize the risk of resigning to a hastily-created federal structure that may ultimately prove undesirable.

The umbrella structure also benefits state governments because it gives them more control over the laws that affect their residents. It increases the effective protections for their residents by allowing for faster modification of profiling regulations to adapt to new technological and cultural concerns. At the same time, the prospect that the federal agency will pull outlier states into line with the national norm decreases an individual state's risk of losing local businesses due to its having a more stringent regulatory system than other states.

IV. CONCLUSION

The digital world presents a wholly unique challenge to our regulatory systems. In it, the potential for privacy invasion is universal and

entrenched. Industry self-regulation has not seriously attempted to combat this stampede, and existing legislation is not well-positioned to establish a framework that safeguards Internet users from the commercial amassing of individual dossiers from online information. For these reasons, a new and unique legislative format tailored to address the distinctive harms created by the electronic exploitation of personal information is the best avenue for removing the integrity of personal information from the grip of industry's natural competitive and commercial tendencies.

The federal umbrella structure meets the main objectives of protecting online users from surreptitious identity data collection, with ancillary but distinct benefits to industry and government. With this system, industry would operate within tested and widely-accepted parameters that have a lower likelihood of unforeseen negative consequences than any newly-established regime. Additionally, this system would expand global opportunities to American businesses by forcing their operations to comply with internationally accepted principles, and would allow for clear cost-benefit analysis for contractual arrangements outside of the default rules. Federal and state governments would benefit from reduced cost, increased expediency, enhanced international acceptance, and higher quality laws.

With the rapid speed of technological innovation, delay in the establishment of an appropriate profiling privacy framework raises the costs for all involved to the point where it becomes prohibitively costly to implement. If lawmakers do not act now, American citizens will not be able to safeguard our identities effectively. And then, citizens will have lost not only their privacy, but also a government supposedly created for the people.