20:3 BERKELEY TECHNOLOGY LAW JOURNAL

Pages
1269
to
1475

Summer
2005

Production: Produced by members of the *Berkeley Technology Law Journal* on PC computers. All editing and layout is done using Microsoft Word.

Printer: Joe Christensen, Inc., Lincoln, Nebraska.
Printed in the U.S.A.
The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Library Materials, ANSI Z39.48—1984.

Berkeley Technology Law Journal
University of California, Berkeley
Boalt Hall School of Law
587 Simon Hall
Berkeley, California 94720-7200
(510) 643-6454 (Phone)
(510) 643-6816 (Fax)
btlj@law.berkeley.edu
www.btlj.org

BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 20 NUMBER 3 SUMMER 2005

TABLE OF CONTENTS

SYMPOSIUM: SPYWARE: THE LATEST CYBER-REGULATORY CHALLENGE

DONORS

The *Berkeley Technology Law Journal* acknowledges the following generous donors to Boalt Hall's Law and Technology Program:

Benefactors

COOLEY GODWARD LLP

DLA PIPER RUDNICK GRAY CARY US LLP

FARELLA BRAUN + MARTEL LLP

FENWICK & WEST LLP

LATHAM & WATKINS LLP

ORRICK, HERRINGTON & SUTCLIFFE LLP

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

WEIL, GOTSHAL & MANGES LLP

WILSON SONSINI GOODRICH & ROSATI PC

Members

ALSCHULER GROSSMAN STEIN & KAHAN LLP

BAKER BOTTS LLP

BINGHAM MCCUTCHEN LLP

COVINGTON & BURLING

DAVIS POLK & WARDWELL

DAY CASEBEER MADRID & BATCHELDER LLP

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER L.L.P.

FISH & RICHARDSON P.C.

HELLER EHRMAN LLP

HOWREY LLP

KIRKLAND & ELLIS

KNOBBE MARTENS OLSON & BEAR LLP

MARGER JOHNSON & MCCOLLOM PC

MCDERMOTT, WILL & EMERY

MORGAN, LEWIS & BOCKIUS LLP

MORRISON & FOERSTER LLP

O'MELVENY & MYERS LLP

PILLSBURY WINTHROP SHAW PITTMAN LLP

TOWNSEND AND TOWNSEND AND CREW LLP

WHITE & CASE LLP

VAN PELT, YI & JAMES LLP

Patrons

BAKER & MCKENZIE

DEWEY BALLANTINE LLP

GREENBERG TRAURIG LLP

GUNDERSON DETTMER STOUGH VILLENEUVE FRANKLIN & HACHIGIAN, LLP

KEKER & VAN NEST LLP

KENYON & KENYON

MILBANK, TWEED, HADLEY & MCCLOY LLP

ROPES & GRAY LLP

The *Berkeley Technology Law Journal* is a nonprofit organization and welcomes donations. Donors are recognized appropriately for their contributions. For more information, e-mail btlj@law.berkeley.edu, or contact the *Berkeley Technology Law Journal*, 587 Simon Hall, Boalt Hall School of Law, University of California, Berkeley, California 94720, (510) 643-6454.

ADVISORY BOARD

SUBSCRIBER INFORMATION

The *Berkeley Technology Law Journal* (ISSN 1086-3818), a continuation of the *High Technology Law Journal* effective Volume 11, is edited and published four times each year (Spring, Summer, Fall, and Annual Review of Law and Technology) by the students of Boalt Hall School of Law, University of California, Berkeley. Application to Mail at Periodicals Postage Rate is Pending at Berkeley, California, and at additional mailing offices. POSTMASTER: Send address changes to Journal Publications Coordinator, Boalt Hall School of Law, 421 North Addition, University of California, Berkeley, CA 94720-7200.

Correspondence. Address all correspondence regarding subscriptions, address changes, claims for nonreceipt, single copies, advertising, and permission to reprint to Journal Publications Coordinator, Boalt Hall School of Law, 421 North Addition, Berkeley, CA 94720-7200; (510) 643-6600; journalpublications@law.berkeley.edu. Authors: see section entitled Information for Authors.

Subscriptions. Annual subscriptions are $65.00 for individuals, and $85.00 for organizations. Single issues are $27.00. Please allow two months for receipt of the first issue. Payment may be made by check, international money order, or credit card (MasterCard/Visa). Domestic claims for nonreceipt of issues should be made within 90 days of the month of publication; overseas claims should be made within 180 days. Thereafter, the regular back issue rate ($27.00) will be charged for replacement. Overseas delivery is not guaranteed.

Form. The text and citations in the *Journal* conform generally to the UNITED STATES GOVERNMENT PRINTING OFFICE STYLE MANUAL (29th ed. 2000) and to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 18th ed. 2005). Please cite this issue of the *Berkeley Technology Law Journal* as 20 BERKELEY TECH. L.J. ___ (2005).

BTLJ ONLINE

Abstracts of all *Berkeley Technology Law Journal* and *High Technology Law Journal* articles as well as the full text of most articles published in previous issues can be found at http://www.btlj.org. Our site also contains subject, author and title indexes, general information about the *Journal*, selected materials related to technology law, and links to other related home pages. Subject, author, and title indexes may also be found in Volume 10, Number 2 (1995) of the *Journal*.

INFORMATION FOR AUTHORS

The Editorial Board of the *Berkeley Technology Law Journal* invites the submission of unsolicited manuscripts. Submissions may include previously unpublished articles, essays, book reviews, case notes, or comments concerning any aspect of the relationship between technology and the law. If any portion of a manuscript has been previously published, the author should so indicate.

Format. Authors should submit double-spaced, single-sided manuscripts with generous margins. We regret that submissions cannot be returned. Authors should retain an exact copy of any material submitted. Authors may submit manuscripts in electronic or hardcopy form, though electronic submissions are strongly encouraged. Electronic submissions should be sent as attachments in Microsoft Word format to btlj@law.berkeley.edu.

Citations. All citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 18th ed. 2005). In addition, the author should include his or her credentials, including full name, degrees earned, academic or professional affiliations, and citations to all previously published legal articles.

Copyrighted Material. If a manuscript contains any copyrighted table, chart, graph, illustration, photograph, or more than eight lines of text, the author must obtain written permission from the copyright holder for use of the material. A photocopy of such written permission should accompany the submission.

Mailing Address. Please submit all hardcopy manuscripts to:

Submissions Editor
Berkeley Technology Law Journal
University of California, Berkeley
Boalt Hall School of Law
587 Simon Hall
Berkeley, California 94720
(510) 643-6454 (Phone)

BOARD OF EDITORS 2005-2006

PRIVACY INALIENABILITY AND THE REGULATION OF SPYWARE

By Paul M. Schwartz

TABLE OF CONTENTS

I. INTRODUCTION

A privacy-sensitive model for personal data trade should respond to five areas: inalienabilities, defaults, a right of exit, damages, and institutions. A key element of such a privacy-promoting model is the employment of use-transferability restrictions in conjunction with an opt-in default. This Article calls this model "hybrid inalienability" because it allows individuals to share, as well as to place limitations on, the future use of their personal information. The proposed hybrid inalienability model follows personal information through downstream transfers and limits the negative effects that result from "one-shot" permission to all personal data trade.

After developing a privacy-sensitive model for personal data trade in Part II, this Article uses it to evaluate a recent federal bill, H.R. 29 (entitled the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)), that seeks to regulate spyware. A controversial application of networked computing, spyware is a program that "install[s] itself without your permission, run[s] without your permission, and use[s] your computer without your permission."[1] Spyware draws on computer resources to create a network that can be used for numerous purposes, including collecting personal and nonpersonal information from computers and deliver-

1. Tracy Baker, *Here's Looking at You, Kid: How To Avoid Spyware*, SMART COMPUTING, Sept. 2003, at 68.

ing adware or targeted advertisements to individuals surfing the Web.[2] This Article finds some strengths, but also numerous weaknesses in the proposed legislation.

II. THE FIVE ELEMENTS OF PROPERTY IN PERSONAL INFORMATION

In this Part, I develop an approach to data trade that responds to weaknesses in the current "privacy market."[3] Currently, the existing market for exchanges of personal information does not promote data trades capable of responding to different privacy preferences. In this Article, I largely focus on a strategy for transformation of the existing privacy market to match each individual's preferred privacy characteristics. It is important to note, however, that the value of information privacy also accrues beyond the individual. A privacy commons can function as an important type of public good, like clean air or national defense.

A. Inalienabilities

Propertized personal information requires the creation of inalienabilities to respond to the problem of market failure. According to Susan Rose-Ackerman's definition, an "inalienability" is "any restriction on the transferability, ownership, or use of an entitlement."[4] As this definition makes clear, inalienabilities may consist of separate kinds of limitations on a single entitlement. In the context of personal data trade, a single combination of these inalienabilities proves to be of greatest significance—namely, a restriction on the use of personal data combined with a limitation on their transferability. This Section first analyzes this combination and then discusses why this hybrid inalienability should include a recourse to defaults.

The current privacy market fails—in part—by providing, at best, only one opportunity to refuse an information collector's overtures. Both downstream data use and subsequent transfers of personal information may exacerbate market shortcomings. Indeed, a variety of devices and systems that commodify information lead to downstream uses and onward trans-

2. *Id.* Adware performs much the same function as some spyware by delivering targeted advertising content to computer users. The definitional line between the two depends on whether the computer user receives adequate notice of the program's installation.

3. This Part provides abridged versions of arguments that I have developed at greater length elsewhere. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).

4. Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931, 931 (1985).

fers.[5] Beyond downstream data use and subsequent transfers, free alienability is problematic because information asymmetries about data collection and current processing practices are likely to resist easy fixes. The ongoing difficulties in providing understandable "privacy notices" in both online and offline contexts illustrate the challenges of supplying individuals with adequate information about privacy practices.[6] As a result, there may be real limits to a data trade model under which consumers have only a single chance to negotiate future uses of their information.

To limit the negative results of one-shot permission for data trade, this Article proposes a model that combines limitations on use with limitations on transfer. Under this approach, property rights are an interest that "run[] with the asset"; the use-transferability restrictions follow the personal information through downstream transfers and thus limit the potential third-party interest in such information. Specifically, the ideal alienability restriction on personal data is a hybrid one based partially on the Rose-Ackerman taxonomy. This hybrid consists of a use-transferability restriction plus an opt-in default.

In practice, this model would permit the transfer of personal data for an initial category of use, but only if the customer is granted an opportunity to block further transfer or use by unaffiliated entities. Any further use or transfer would require the customer to opt-in—that is, it would be prohibited unless the customer affirmatively agrees to it. Note that this restriction limits the alienability of individuals' personal information by preventing them from granting one-stop permission for all use or transfer of their information. A data processor's desire to carry out further transfers thus obligates the processor to supply additional information and provides another chance for the individual to bargain with the data collector.

To ensure that the opt-in default leads to meaningful disclosure of additional information, however, two additional elements are needed. First, the government must have a significant role in regulating the way that information transferees provide notice of privacy practices to information owners. A critical issue will be the "frame" in which transferees present information about data processing.[7]

---

5. For expansion of this argument, see Schwartz, *supra* note 3, at 2096-98.

6. *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230-32, 1241-44 (2002).

7. For more details regarding this argument, see Schwartz, *supra* note 3, at 2099.

Second, meaningful disclosure requires addressing what Henry Hansmann and Reinier Kraakman term "verification problems."[8] As they explain, "[a] verification rule sets out the conditions under which a given right in a given asset will run with the asset."[9] Their scholarship points to the critical condition that third parties must be able to verify that a given piece of personal information has, in fact, been propertized and then to identify the specific rules that apply to it. In the context of propertized personal information, the requirement for verification creates a role for non-personal metadata, a tag or kind of barcode, to provide necessary background information and notice.

B. Defaults

As a further safeguard to promote individual choice, this Article advocates the use of defaults. It prefers an opt-in default because it would be information-forcing—that is, this approach places pressure on the better-informed party to disclose material information about how personal data will be used.[10] This default promises to force the disclosure of hidden information about data-processing practices. Furthermore, such a default should generally be mandatory to further encourage disclosure—that is, the law should bar parties from bargaining out of the default rule.[11]

The strengths of the proposed model can be illustrated through a consideration of the design and the effects, both positive and negative, of a recent American statute. In the United States, the Gramm-Leach-Bliley Act (GLB Act) removed legal barriers blocking certain transactions between different kinds of financial institutions and provided new rules for financial privacy. These privacy rules require financial entities to mail annual privacy notices to their customers.[12] Moreover, consistent with the model that I have proposed, the GLB Act incorporates a transferability

---

8. Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights*, 31 J. LEGAL STUD. S373, S384 (2002).

9. *Id.*

10. For a more detailed discussion of the merits of opt-in defaults, see Schwartz, *supra* note 3, at 2103. For the classic discussions of opt-in rules in the context of contract, see Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 93 (1989); Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729, 761 (1992).

11. *Id.*

12. These protections are found in Title V of the GLB Act. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501-527, 113 Stat. 1338, 1436-50 (1999) (codified at 15 U.S.C. §§ 6821-27 (2000)).

restriction.[13] Unlike this Article's proposed default, however, the Act merely compels financial entities to give individuals an opportunity to opt out, or to indicate their refusal, before their personal data can be shared with unaffiliated entities.[14] Thus, the GLB Act does not have a true information-forcing effect because it chooses an opt-out rule over an opt-in rule.

An assessment of the GLB Act supports the proposition that a use-transferability restriction, combined with a default regime, can lead to optimal information-sharing. Consistent with the privacy model proposed by this Article, the GLB Act obligates the relatively better-informed parties—financial institutions—to share information with other parties. Also, it sets this obligation to inform as a mandatory default: the GLB requires financial institutions to supply annual privacy notices to their customers.[15] A client cannot trade the notice away for more products and services or even opt not to receive the notices because she does not want to receive more paper. Even if many individuals do not read privacy notices, a mandatory disclosure rule is crucial to the goal of creating a critical mass of informed consumers.

Unfortunately, the GLB Act's promise of informed participation in privacy protection has yet to be realized, due in large part to the relative weakness of its default rule, which allows information-sharing if consumers do not opt out. The opt-out rule fails to impose any penalty on the party with superior knowledge—the financial entity—should negotiations over further use and transfer of data fail to occur. Under the Act, information can be shared with unaffiliated parties unless individuals take the affirmative step of informing the financial entity that they refuse to allow the disclosure of their personal data.[16]

An opt-in rule is, therefore, an improvement over an opt-out rule because an opt-in regime improves the functioning of the privacy market by reducing information asymmetry problems. An opt-in rule forces the data processor to obtain consent to acquire, use, and transfer personal information. It creates an entitlement in personal information and places pressure on the data collector to induce the individual to surrender this entitlement. In addition to having a positive impact on the privacy market, the opt-in regime also promotes social investment in privacy.

---

13. *See id*. § 502 (codified at 15 U.S.C. § 6802 (2000)).
14. *See id*. § 502(a) (codified at 15 U.S.C. § 6802(a) (2000)).
15. *See id*.
16. *See id.* § 502 (codified at 15 U.S.C. § 6802).

However much the opt-in default regime may promise, it still has some weaknesses and thus should only be one of several elements in any privacy-sensitive propertization scheme for personal data. The opt-in regime's first weakness is that many data-processing institutions are likely to be good at obtaining consent on their terms regardless of whether the default requires consumers to authorize or preclude information-sharing.[17] Consider financial institutions, the subject of Congress's regulation in the GLB Act. These entities provide services that most people greatly desire. As a result, a customer will likely agree to a financial institution's proposed terms, if refusing permission to share information means not getting a checking account or a credit card. More generally, consumers are likely to be far more sensitive to price terms, such as the cost of a checking account, than to nonprice terms like the financial institution's privacy policies and practices.[18] Because better information may not cure market failure, the effect of information-forcing defaults should be bolstered through use-transfer restrictions and other protection mechanisms, such as a right of exit.

C. Right of Exit

Consent to data trade should imply not only an initial opportunity to refuse trade, but also a later chance to exit from an agreement to trade. According to Hanoch Dagan and Michael Heller, "[e]xit stands for the right to withdraw or refuse to engage: the ability to dissociate, to cut oneself out of a relationship with other persons."[19] The right of exit, for example, would allow people to disable spyware and adware on the Internet. For the privacy market, a right of exit prevents initial bad bargains from having long-term consequences. For the privacy commons, moreover, a right of exit preserves mobility so people can make use of privacy-enhancing opportunities and otherwise reconsider initial bad bargains. Dagan and Heller have proposed that exit is a necessary element of a "liberal commons" because "well-functioning commons regimes give paramount concern to nurturing shared values and excluding bad cooperators."[20]

Providing a chance to withdraw is especially important in the context of data trade because current standards afford little protection to privacy. Once companies are able to establish a low level of privacy as a dominant

17. Janger & Schwartz, *supra* note 6, at 1244-45.

18. *Id.* at 1237-38, 1240.

19. Hanoch Dagan & Michael A. Heller, *The Liberal Commons*, 110 YALE L.J. 549, 568 (2001) (citing LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW §§ 15-17, at 1400-09 (2d ed. 1988)).

20. *Id.* at 571.

practice, individuals may face intractable collective action problems in making their wishes heard. As a consequence, an information privacy entitlement should include a right of exit from data trades. A right of exit allows customers to discipline deceptive information collectors. Existing customers will leave as a result of the bad practices, and potential customers will be scared off. In this fashion, a privacy market disciplines deceptive information collectors by shrinking their customer base. The right of exit also brings with it a related interest: the ability to re-enter data trades. Individuals may wish to alternate between privacy preferences more than once.

A possible danger of a right of exit, however, is that it might actually encourage, rather than discourage, deceptive claims from data collectors. The risk is that deceptive information collectors will encourage defections from existing arrangements that are privacy-friendly. Indeed, these deceptive information collectors may also generally hinder a privacy market from forming around an opt-in regime; they might be able to do so by scaring off consumers from privacy-friendly data collectors.

D. Damages

This Article's preference when harm occurs to information privacy interests is for state determination of damages, including explicit recourse to liquidated damages. Leaving data sellers and buyers free to set the prices for privacy violations will produce inadequate obedience to these obligations.

First, actual damages are frequently difficult to show in the context of privacy. Already, in two notable instances, litigation for privacy violations under a tort theory has foundered because courts determined that the actual harm that the plaintiffs suffered was de minimis.[21] Second, an individual's personal data may not have a sufficiently high market value to justify the costs of litigation. Finally, due to the difficulty of detection, many violations of privacy promises will themselves remain private. Spyware provides an example of a privacy invasion that is difficult to notice. If damages are to reflect an implicit price payable for violation of a legal right, the monetary amount of damages should be set higher or lower de-

21. Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975) (holding that the sale of magazine subscription lists to direct mail advertisers does not constitute a tortious appropriation of personality because "[t]he right of privacy does not extend to the mailbox"); Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995) (holding that the sale of a credit card company's profiles of customers' spending behaviors does not deprive the cardholders of any value their personality might have).

pending on the probability of detection of the violation. Since many privacy violations have a low probability of detection, damages should be relatively high.

A state determination of damages through privacy legislation is preferable to an approach of enforcing the subjective valuations of private parties with injunctions. Schemes providing for liquidated damages will assist the operation of the privacy market and the construction and maintenance of a privacy commons. State determination of a damages schedule will encourage companies to keep privacy promises so long as the damages are set high enough to deter potential violators and encourage litigation to defend privacy entitlements. In addition, damages support a privacy commons by promoting social investment in privacy protection. Such damages may also reduce the adverse impact of collective action problems in the privacy market by allowing consumers who do not litigate to benefit from the improved privacy practices that follow from successful litigation. This "free riding" on increased privacy protection is a useful result of a statute that permits liquidated damages.

Existing privacy law sometimes adheres to this path by either collectively setting damages or relying on liquidated damages. The Video Privacy Protection Act allows a court to "award . . . actual damages but not less than liquidated damages in an amount of $2,500."[22] The Driver's Privacy Protection Act contains similar language regarding damage awards against a "person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter."[23] Finally, the Cable Communications Policy Act, which safeguards cable subscriber information, allows a court to award "liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher."[24]

E. Institutions

Institutions shape the legal and social structure in which property is necessarily embedded. Many types of property depend on institutional entities for their shape and maintenance.[25] For example, automobiles are a form of property that is structured by legal obligations; they require title recordings, annual safety inspections, and, depending on the state, different mandatory insurance policies. These legal requirements in turn create a

22. 18 U.S.C. § 2710(c)(2) (2000).

23. *Id.* § 2724(a).

24. 47 U.S.C. § 551(f) (2000).

25. Carol M. Rose, *Canons of Property Talk, or, Blackstone's Anxiety*, 108 YALE L.J. 601, 632 (1998).

dynamic of institution-building, involving public and private entities. Private companies compete to provide insurance. In California, registration of one's automobile involves hiring a private service station to test the smog emissions of automobiles as part of registration, but recourse to a state official to check one's mileage and Vehicle Identification Number.

Without these institutions automobiles could certainly exist, but their use would be more polluting (no smog inspections), more dangerous (no safety inspections by specialists), and more risky (no insurance for the inevitable occurrence of accidents). In other words, the value of automobiles would be lower in relation to their disadvantages in the absence of institutions.

Likewise, personal data would possess higher value through the intervention of institutions that shape the rights and responsibilities associated with such property. What role should institutions play as part of a system of propertized personal data? Institutions are needed for three general purposes: to provide trading mechanisms (a "market-making" function), to verify claims to propertized personal data (a verification function), and to police compliance with agreed-upon terms and legislatively mandated safeguards (an oversight function). Institutions filling these roles will assist the privacy market by ensuring that processes exist for the exchange of data and for the detection of violations of privacy promises.

As to the first role of institutions, differing proposals for market-making institutions have appeared, some advocating a centralized market and some advocating a decentralized market. In a detailed proposal to create a central National Information Market ("NIM"), Kenneth Laudon calls for development of "National Information Accounts (NIAs) for suppliers (individuals and institutions) and buyers (information brokers, individuals, and institutions)."[26] In his vision of a single information market, Laudon writes: "Every participating citizen would be assigned an NIA with a unique identifier number and barcode symbol."[27]

While such a system serves the market-making function, it possesses the flaw that a single market might encourage privacy violations because its centralized nature makes it an easy target for attacks. Once someone breaks into the bank, all that it holds within is imperiled. By contrast, decentralized methods of information exchange can handle the market-making function while simultaneously proving to be an elusive target for attack. Such a system would rest on a multiplicity of dealer-customer con-

26. Kenneth C. Laudon, *Markets and Privacy*, COMMS. OF THE ACM, Sept. 1996, at 92.

27. *Id.* at 100.

tacts and sales points rather than a central repository and meeting place for information providers and consumers.

As for the second role of institutions, this Article calls for verification of propertized personal information through an association with nonpersonal metadata. This metadata might contain information such as the database from which the personal information originated, whether any privacy legislation covered that information, and the existence of any restrictions on further data exchange without permission from the individual to whom the data referred. Such a decentralized approach would avoid the possibility of a major privacy meltdown due to the unique identifiers associated with a single NIA.

Decentralized data markets also have the potential to develop privacy-friendly innovations in discrete submarkets. These submarkets might in turn offer the possibility to provide examples of "best privacy trading practices" to be used elsewhere. Given the novelty of an institutionalized data trade, it makes sense to start with multiple small markets that can draw on local knowledge rather than with Laudon's single NIM.

In order to meet the third function of institutions, oversight, data trading laws should allow citizens to participate in protecting their own rights through private rights of action, including class actions, when those rights are violated. This approach builds on the proposals regarding damages that this Article makes above. Such rights of action provide many swords, decentralized among the property holders, whose prodding can be highly effective in increasing compliance with statutory standards. For example, current rules against telemarketing allow lawsuits against companies that continue to make calls after a consumer has requested that they cease.[28] Such suits have resulted in millions of dollars in fines, and have made the words "place me on your do not call list" a potent request.

All of which is not to say, however, that the Federal Trade Commission (FTC) and other governmental agencies do not have an important role to play in privacy protection. Here, the FTC's existing activities illustrate the contribution to policing possible from both public sector institutions and decentralized institutional infrastructures. The FTC has acted in a number of instances to enforce the privacy promises of companies that collect personal data, particularly those who do so on the Internet.[29] Yet, even with a specific grant of authority, the FTC would likely be over-

28. 47 U.S.C. § 227(b)(1) (2000).

29. For information on the FTC's enforcement role, see Federal Trade Commission, *Privacy Initiatives: Introduction*, http://www.ftc.gov/privacy/index.html (last visited Aug. 22, 2005).

whelmed if it were the sole institution responsible for policing the personal information market. Innovative approaches involving multiple institutions are necessary. Thus, as noted, this Article favors a decentralized institutional model.

III. H.R. 29 AND SPYWARE

This Article now turns to spyware. How does a recent bill, H.R. 29, for regulating spyware compare with the model that this Article has developed? Introduced by Representative Mary Bono, H.R. 29 is titled the Securely Protect Yourself Against Cyber Trespass Act or SPY ACT. Although it is not without some positive aspects, H.R. 29 falls short in a number of areas.

First, concerning inalienabilities, recall that this Article calls for a use-transferability restriction plus an opt-in default. Transfer should be permitted for an initial category of use of personal data, but only if the transferee grants the customer an opportunity to block further transfer or use by unaffiliated entities. Any further use or transfer would require the customer to opt-in. H.R. 29 does set some use-transfer restrictions. It requires subsequent notice and consent from the "person who transmitted the program" if a program collects or transfers information "for a purpose that is materially different from, and outside the scope of, the type or purpose set forth in the initial or any previous notice."[30]

Moreover, H.R. 29 carefully tries to regulate the way that consumers receive notice of privacy practices to reduce the possibility for vague notice leading to uninformed consent. The proposed statute carefully defines the terms for notice and consent, which are to include "a clear description" of matters such as "the types of information to be collected and sent (if any) by the information collection program"; "the purpose for which such information is to be collected and sent"; and "the identity of any such software that is an information collection program."[31] The bill even spells out some of the language that is to be included in notices, such as "This program will collect and transmit information about you. Do you accept?"[32] Finally, H.R. 29 also gives a role to the FTC in further defining standards for notice.[33]

30. H.R. 29, 109th Cong. § 3(c)(3)(B) (2005).
31. *Id.* § 3(c)(1)(D).
32. *Id.* § 3(c)(1)(B)(i).
33. *Id.* § 3(c)(4).

Less successfully, however, this statute does not overcome what this Article has termed "verification problems."[34] Third parties will be unable to verify that a given piece of personal information has, in fact, been propertized and to identify the specific rules that apply to it. Interestingly enough, H.R. 29 does take a small step in the direction of verification in its requirement of an "identity function."[35] The statute mandates a function in a program so "that each display of an advertisement . . . is accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identifying the program."[36] The identity function allows the user to know that she should link adware to a given program on her computer.

Regarding defaults, this Article has argued in favor of opt-in to avoid placing the burden of bargaining on the less-informed party, the individual consumer. H.R. 29 does require opt-in; information will not be collected unless the individual selects "an option to grant or deny consent."[37] It also safeguards the ability of individuals to walk away from a transaction in the middle of it—notice must allow the option to "abandon or cancel the transmission or execution . . . without granting or denying . . . consent."[38] In other words, inaction following notice will mean that personal data will not be collected.

H.R. 29 also provides for a more complete right of exit—one that follows an initial agreement. The statute terms this capability a "disabling function."[39] An information collection program is to allow "a user of the program to remove the program or disable operation" of the program.[40] Here, the drafters of the statute attempted to respond to warnings about what one industry expert termed "unrealistic uninstall requirements."[41] As Jeffrey Friedberg of Microsoft testified before Congress, "Requiring standardized uninstall practices for all software would be unworkable in many circumstances."[42] Friedberg was concerned about instances "where a full and complete uninstall is neither technically possible nor desirable, such

34. Hansmann & Kraakman, *supra* note 8, at S384.
35. H.R. 29, § 3(d)(2).
36. *Id*.
37. *Id*. § 3(c)(1)(C).
38. *Id*.
39. *Id*. § 3(d)(1).
40. *Id*.
41. *Safeguards Against Privacy Invasions Act: Hearing on H.R. 2929 Before the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. (2004), *available at* http://www.microsoft.com/presspass-/exec/friedberg/04-29spyware.mspx (testimony of Jeffrey Friedberg).
42. *Id*.

as with a software component that is in use and shared by other programs."[43] In addition, Friedberg warned about "situations where requiring uninstall could actually comprise the security of the system, such as backing out security upgrades or removing critical services."[44]

These concerns have some validity. Unfortunately, H.R. 29 responds to them with opaque language capable of covering evasion of its requirements. The proposed statute limits its requirement of disabling an information collection program to "a function that . . . (A) is easily identifiable to a user of the computer; and (B) can be performed without undue effort or knowledge by the user of the protected computer."[45] This language provides all too ample possible loopholes for spyware purveyors; they will likely argue that their program cannot easily be identified or that removing it requires undue effort or knowledge.

The proposed spyware statute also contains provisions for damages. This Article has proposed use of liquidated damages and has argued in favor of both FTC-enforcement and private rights of action. In contrast, H.R. 29 gives the FTC an oversight role but ignores the benefits of decentralization of enforcement. The FTC is to enforce H.R. 29 under both the Federal Trade Commission Act and in cases of a "pattern or practice" that violates core provisions of the Act, it may seek civil penalties.[46] H.R. 29 adds that the remedies that it proposes are to be exclusive ones.[47] In this fashion, the proposed statute makes explicit its intention to close the door to any private enforcement actions.

Finally, this Article has proposed an essential role for institutions in promoting a well functioning market for data trade. It has called for institutions that fulfill three general purposes: to provide trading mechanisms (a market-making function), to verify claims to propertized personal data (a verification function), and to police compliance with agreed-upon terms and legislatively mandated safeguards (an oversight function). H.R. 29 falls considerably short of providing strong institution-building directives. Admittedly, it may be asking too much of any single statute for it to fulfill all three functions. One is left wondering, however, whether a privacy-promoting market can possibly emerge upon the enactment of this statute.

H.R. 29 does not formally respond to a need for multiple decentralized markets for data exchanges. Assuming well-defined property rights and no transaction costs, a Coasian model would expect these markets to spring

43. *Id.*
44. *Id.*
45. H.R. 29, § 3(d)(1).
46. *Id.* § 4(a).
47. *Id.* § 4(c).

up. As Ronald Coase proposed, "It is always possible to modify by transactions on the market the initial legal determinations of rights. And, of course, if such market transactions are costless, such a rearrangement of rights will always take place if it would lead to an increase in the value of production."[48] Here, the lack of verification mechanisms is especially troubling. Although the statute does require a limited identity function, as noted above, H.R. 29 does not develop approaches for linking information with the person who has the property interest in trading the information. Regarding the final provision of this Article's model, which concerns policing compliance, the proposed statute assigns an exclusive enforcement role to the FTC. As this Article has argued, however, this approach is likely to lead to under-enforcement of the rights that H.R. 29 creates.

Two questions remain. First, is H.R. 29 the best privacy-promoting bargain likely to be enacted by Congress? Second, are there elements of a privacy-promoting market for data trade that Congress can comfortably enact initially, with confidence that the other elements will follow in time? This Article leaves these thorny issues for another day and publication.

IV. CONCLUSIONS

A strong conception of personal data as a commodity is emerging in the United States, and individual Americans already participate in the commodification of their personal data. This Article's goal has been to develop a model for the propertization of personal information that also exhibits sufficient sensitivity to attendant threats to personal privacy. It developed the five critical elements of its model of propertized personal information. This model views information property as a bundle of interests to be shaped through attention to five areas: inalienabilities, defaults, a right of exit, damages, and institutions. Unfortunately, H.R. 29 does not attend sufficiently to all five areas.

Despite some strengths, such as its structuring of notice and consent to help create inalienabilities, H.R. 29 fails to overcome verification difficulties in the information privacy market and allows a considerable loophole in its attention to the right of exit. The statute also falls short regarding damages, where the proposed law does not include a private right of action, and regarding institutions. This Article concluded by raising, and leaving open, questions that addressed whether or not H.R. 29 might provide a better response than no spyware legislation at all.

48. Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 15 (1960).

SPYWARE AND THE LIMITS OF SURVEILLANCE LAW

By Patricia L. Bellia[†]

TABLE OF CONTENTS

I. INTRODUCTION

Electronic surveillance law remains a weapon of choice for policy-makers, litigants, and commentators seeking to address the threats digital technology poses for privacy. The controversy over how best to respond to the "spyware" problem provides only the most recent illustration of that

---

† Lilly Endowment Associate Professor of Law, Notre Dame Law School. A.B. Harvard College, J.D. Yale Law School. I thank A.J. Bellia, Susan Freiwald, and Orin Kerr for helpful discussions. Jeannette Cox provided excellent research assistance.

phenomenon.[1] Federal surveillance statutes bar the unauthorized acquisition of electronic communications and related data in some circumstances.[2] Although there is much debate over how to define "spyware,"[3] that label encompasses at least some software that monitors a computer user's electronic communications. Surveillance statutes thus present an intuitive fit for responding to the regulatory challenges of spyware. Indeed, those who argue that no new federal legislation is needed to address the spyware problem rely in part on the opportunities that surveillance statutes and related doctrines provide for criminal prosecution and civil suits.[4]

A recent report issued by the staff of the Federal Trade Commission, for example, suggests that the Department of Justice "has statutory authority to prosecute distributors of software products, such as spyware, in cases where consumers' privacy or security is compromised."[5] That observation was based in part on testimony of Justice Department officials at a day-long FTC workshop held in April 2004. The Justice Department denied that the absence of specific spyware legislation had impeded law enforcement efforts in any way.[6] As one official noted, "we have in our

---

1. A recent report of the staff of the Federal Trade Commission provides a flavor of the debate. *See* FED'L TRADE COMM'N STAFF REPORT, SPYWARE WORKSHOP: MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE (2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarept.pdf [hereinafter FTC STAFF REPORT].

2. *See* 18 U.S.C. § 2511(1)(a) (2000) (prohibiting "intercept[ion]" of communications); *id.* § 2701(a) (barring one from gaining unauthorized access to facility of service provider and thereby "obtain[ing], alter[ing], or prevent[ing] authorized access" to communications in electronic storage).

3. *See, e.g.*, H.R. REP. NO. 109-32, at 10 (2005) (report of Committee on Energy and Commerce, noting that the committee "received testimony that spyware represents a range of software programs on a broad continuum from the most pernicious criminal activities on one end to the less threatening but still intrusive on the opposite end of the spectrum"); FTC STAFF REPORT, *supra* note 1, at 3 ("Panelists generally agreed that reaching an industry consensus on one definition [of spyware] has been elusive because of the technical complexity and dynamic nature of software.").

4. The Senate and the House have debated various spyware proposals over the last two years; most recently, the House overwhelmingly passed two dramatically different versions of spyware legislation in May of 2005. *See* Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), H.R. 29, 109th Cong. (2005); Internet Spyware (I-SPY) Prevention Act, H.R. 744, 109th Cong. (2005). Both bills were passed on May 23, 2005, H.R. 29 by a margin of 393-4 and H.R. 744 by a margin of 395-1. *See* 151 CONG. REC. H3744 (daily ed. May 23, 2005). For a discussion of disagreement over the need for new legislation, see FTC STAFF REPORT, *supra* note 1, at 22.

5. FTC STAFF REPORT, *supra* note 1, at 21.

6. *See* FED'L TRADE COMM'N WORKSHOP TRANSCRIPT: MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 261 (Apr. 19, 2004), *available*

quiver a number of arrows that we can use in prosecution."[7] Justice Department officials testified at the FTC workshop that some forms of spyware, such as devices and software designed to capture keystrokes, could violate the principal federal electronic surveillance statute—Title III of the Omnibus Crime Control and Safe Streets Act of 1968—which prohibits the "intercept[ion]" of communications, including electronic communications.[8] Other commentators have suggested that spyware may also implicate a separate electronic surveillance statute limiting access to stored communications.[9]

As the debate on the need for new federal legislation proceeds, however, there is good reason to believe that federal electronic surveillance statutes can combat only the most extreme forms of spyware. Electronic surveillance law does not apply by any reasonable construction to most forms of spyware. Moreover, the overall record on application of surveillance law statutes to a variety of digital-age problems is in fact quite mixed. Courts have reached aggressive privacy-protective outcomes on very bad facts, but they have also let seemingly problematic practices pass unsanctioned.

The difficulty with efforts to apply surveillance law statutes to new privacy problems is that our federal electronic surveillance statutes are emphatically not comprehensive data privacy statutes. They may wrongly be perceived as such, particularly by victims of spyware and related privacy threats. The mismatch between the statutes and the goal of protecting online privacy has created a body of confused—even incoherent—case law. To that extent, it diverts attention from important policy questions, including whether Congress should consider legislative solutions tailored

---

at http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf (comments of Mark Eckenwiler, Deputy Chief, Computer Crime and Intellectual Property Section, Department of Justice) [hereinafter FTC WORKSHOP TRANSCRIPT].

7. *Id.*

8. 18 U.S.C. § 2511(1)(a) (2000); *see* FTC WORKSHOP TRANSCRIPT, *supra* note 6, at 260 (comments of Mark Eckenwiler). Justice Department testimony also focused on various prongs of the federal computer crime statute, known as the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2000 & Supp. II 2002). *See* FTC WORKSHOP TRANSCRIPT, *supra* note 6, at 259-60 (comments of Mark Eckenwiler). CFAA claims often go hand-in-hand with claims under the surveillance statutes, but because the CFAA is not technically a surveillance statute, I discuss it only briefly. *See infra* note 168 and accompanying text.

9. 18 U.S.C. §§ 2701-2709, 2711-2712 (2000 & Supp. II 2002); *see* FTC STAFF REPORT, *supra* note 1, at 35 n.206 (citing 18 U.S.C. §§ 2701-2711); CENTER FOR DEMOCRACY & TECHNOLOGY, GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM 10 n.12 (Nov. 2003), *available at* http://www.cdt.org/privacy/031100spyware.pdf (citing 18 U.S.C. §§ 2701-2712).

to specific privacy threats (such as spyware) or whether broader data privacy statutes are necessary or appropriate. In other words, we might be better off if courts and commentators would simply make surveillance law's limits plain.

This Article uses the difficulties of applying electronic surveillance law statutes to spyware to illustrate the broader limits of surveillance law. Part II provides an overview of the electronic surveillance framework. Part III considers the interpretive issues that have arisen and that are likely to arise as litigants and courts seek to apply the federal statutes to various types of spyware. Current case law suggests that electronic surveillance statutes are likely to constrain only the most egregious forms of spyware—and there may even be some difficulties in surveillance law performing that limited task. Efforts to use surveillance law to create more privacy-sensitive industry practices are likely to fail altogether.

The constructions of the law that I offer in Part III may be controversial, partly because surveillance law is sufficiently unstable that there is room for courts to adopt approaches that are more privacy-protective. In Part IV, I consider whether courts *should* use surveillance law to respond more aggressively to privacy challenges such as spyware. Drawing upon case law from other contexts, I show that there are good reasons to be wary of using surveillance law as a vehicle for addressing various information privacy problems. Indeed, if electronic surveillance cases were to plainly expose the limits of surveillance law, they would generate a more fruitful legislative debate about the propriety of true data privacy legislation, whether broadly or narrowly conceived.

II. UNDERSTANDING THE ELECTRONIC SURVEILLANCE LAW FRAMEWORK

In this Part, I introduce three statutes that form the federal electronic surveillance law framework:[10] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as "Title III" or the "Wiretap

10. The electronic surveillance landscape also includes another important statute: the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C.A. §§ 1801-1863 (West 2000 & Supp. 2005). That statute authorizes surveillance to gather "foreign intelligence information," defined in part to include information that relates to the ability of the United States to protect against an attack or other hostile acts by a foreign power. *Id.* § 1801(e). Because I am primarily concerned with legal authorities that constrain private parties' conduct, I do not discuss FISA, which regulates only conduct undertaken "under color of law." *See id.* § 1809(a). For further discussion of FISA, see Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. (forthcoming 2005).

Act");[11] the segment of the Electronic Communications Privacy Act (ECPA) limiting access to stored communications (also known as the "Stored Communications Act (SCA)");[12] and the provisions governing the use of "pen registers" and "trap and trace devices"—that is, devices designed to acquire source and destination information associated with communications.[13]

Before exploring the electronic surveillance framework, it is useful to define "electronic surveillance" and to discuss one shortcoming of that phrase. By "electronic surveillance," I mean techniques that historically have involved the use of certain electronic or mechanical *devices* to acquire the contents of communications and identifying data associated with them. The term "electronic" in "electronic surveillance," then, refers to the technique used in the surveillance, not to the type of communication acquired through the technique. Wiretapping (attaching a device to a telephone wire to acquire the contents of a telephone communication) and eavesdropping (installing a device to transmit or record a conversation) are two electronic surveillance techniques. The Wiretap Act, the principal modern federal surveillance statute, was originally designed to regulate those techniques. As discussed below, technological developments necessitated an expansion of the Wiretap Act to encompass more modern methods of communication.

The phrase "electronic surveillance" is also something of a misnomer. The term "surveillance" is ordinarily used to describe the *government's* acquisition of information about its citizens. Indeed, all three of the federal statutes discussed below were primarily passed in response to, or designed to take account of, Supreme Court decisions addressing the legality under the Fourth Amendment of government surveillance activities. Each statute, however, also regulates *private* conduct. For purposes of understanding

---

11. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801-804, 82 Stat. 197, 211-23 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000 & Supp. II 2002)). I dislike the term "Wiretap Act," because the statute covers not only "wiretapping"—that is, acquisition of the contents of wire communications through use of an electronic or mechanical device—but also the acquisition of oral and electronic communications. It is nevertheless difficult to avoid using it, because it appears in many of the cases that I discuss. When describing provisions of the statute under which government officials seek court authorization to conduct surveillance activities, however, I generally refer to "Title III" orders, in keeping with government practice.

12. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 201-202, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C. §§ 2701-2709, 2711-2712 (2000 & Supp. II 2002)).

13. *See id.* § 301, 100 Stat. at 1868-73 (codified as amended at 18 U.S.C. §§ 3121-3127 (2000 & Supp. II 2002)).

how, if at all, surveillance statutes constrain the distribution or use of spyware, we are primarily interested in the scope of the statutory prohibitions on private conduct. Because each statute to some extent accommodated a Supreme Court decision addressing government surveillance activities, however, it is impossible to understand the structure and terminology of each statute without understanding the Fourth Amendment limitations on government conduct.

I discuss the Wiretap Act, the Stored Communications Act, and the pen register and trap and trace provisions in turn. With respect to each statute, I identify the key interpretive issues that are likely to arise in attempts to apply the statute to the spyware problem.

A. The Wiretap Act

In adopting the Wiretap Act in 1968, Congress prohibited the "intercept[ion]" of certain communications.[14] Although the statute was the product of several years of legislative efforts to regulate wiretapping and eavesdropping activities,[15] two cases decided by the Supreme Court in 1967 provided the immediate impetus for the statute's passage.

In 1928, the Supreme Court held in *Olmstead v. United States*[16] that the government's use of a wiretapping device would not violate the Fourth Amendment unless government agents trespassed onto private property to install the device.[17] Congress responded in 1934 by outlawing wiretapping by private or governmental entities,[18] but these proscriptions were widely disregarded.[19] More than three decades later, as Congress weighed various statutory proposals to revise the prohibition on wiretapping and to add a prohibition on eavesdropping, the Supreme Court decided two key cases that would shape the legislative effort. First, in *Berger v. New York*,[20] the Court invalidated a New York statute setting forth requirements under

14. 18 U.S.C. § 2511(1)(a) (2000).

15. *See* AMERICAN BAR ASS'N PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE, STANDARDS RELATING TO ELECTRONIC SURVEILLANCE app. E (Tentative Draft, 1968) (cataloguing congressional hearings); S. REP. NO. 90-1097, at 134 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2223 (individual views of Sen. Long and Sen. Hart) (noting that Congress had debated bills addressing wiretapping and eavesdropping activities for forty years).

16. 277 U.S. 438 (1928).

17. *Id.* at 466.

18. Act of June 19, 1934, ch. 652, § 605, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605 (2000)).

19. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 12 (2004).

20. 388 U.S. 41 (1967).

which a judge could authorize law enforcement officials to use listening devices. Because the case involved a listening device that had been placed in an office after a "trespassory intrusion," the Court applied the Fourth Amendment notwithstanding its conclusion in *Olmstead*.[21] The Fourth Amendment requirements identified in *Berger* ultimately provided a blueprint for federal legislation.[22] Second, in *Katz v. United States*,[23] the Court abandoned its prior focus on trespass as the trigger for applicability of the Fourth Amendment. The *Katz* Court held that the Fourth Amendment does not simply protect against government intrusions into physical areas in which an individual has a property interest: "[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[24] Because the government's activities "in electronically listening to and recording [Katz's] words violated the privacy upon which he justifiably relied while using the telephone booth," the government's conduct amounted to a search.[25]

These two decisions brought a new sense of urgency to the legislative debate, because they essentially outlawed all wiretapping and eavesdropping activities by federal and state officials not conducted in conformity with the Fourth Amendment requirements outlined in *Berger*. The Wiretap Act reflected Congress's attempt to broadly regulate electronic surveillance by outlawing such activities by both private parties and government officials and excepting certain law enforcement conduct from the prohibition.[26]

The Wiretap Act provides for criminal penalties and civil damages against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept" any covered communication.[27] To "intercept" a communication is to use "any electronic, mechanical, or other device" to acquire its contents.[28] As passed in 1968, the Wiretap Act covered "wire communications," defined

---

21. *Id.* at 44.

22. *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1389-90 (2004); Freiwald, *supra* note 19, at 25.

23. 389 U.S. 347 (1967).

24. *Id.* at 353.

25. *Id.*

26. *See* 18 U.S.C. § 2511(1)(a) (2000) (outlawing interception by "any person"); *id.* § 2518 (setting forth procedures for government officials to request court authorization for electronic surveillance activities).

27. *Id.* § 2511(1)(a).

28. *Id.* § 2510(4).

to include a communication "made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection,"[29] and "oral communications," defined to include a communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[30] In 1986, in ECPA,[31] Congress extended the Wiretap Act's coverage to "electronic communications," defined in part as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[32]

As will become clear, the Wiretap Act presents a number of difficult interpretive issues. First, the statute defines the term "intercept" to include the "aural or other acquisition of the contents of a communication"[33]—but the definition does not specify whether acquisition of a communication must occur contemporaneously with its transmission in order to qualify as an interception, or whether acquisition of stored communications would also qualify. That issue is among the most frequently litigated under the Wiretap Act, both with respect to government and private conduct,[34] and is likely to arise in the spyware context as well. Second, in addition to permitting authorized government conduct, the Wiretap Act exempts conduct undertaken with the "consent" of a party to the intercepted communication.[35] The consent exception essentially preserves a line of cases pre-

29. 18 U.S.C. § 2510(1) (2000 & Supp. II 2002). When Congress revised the Wiretap Act in 1986 by passing ECPA, it distinguished wire communications from electronic communications by amending the wire communication definition to refer to an "aural transfer," a term further defined as a transfer "containing the human voice." 18 U.S.C. § 2510(18) (2000). In addition, ECPA altered the wire communication definition to include "any electronic storage of such communication." *Id.* § 2510(1). That portion of the definition was excised by the USA Patriot Act. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283 [hereinafter USA PATRIOT Act]. For further discussion, see *infra* notes 198-206, 290-293 and accompanying text.

30. 18 U.S.C. § 2510(2) (2000).

31. Pub. L. No. 99-508, § 101, 100 Stat. 1848, 1848 (1986).

32. 18 U.S.C. § 2510(12).

33. *Id.* § 2510(4).

34. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Wesley Coll. v. Pitts, 974 F. Supp. 375, 388 (D. Del. 1997); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996); United States v. Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996); *see also infra* notes 183-189, 194-229, 281-293 and accompanying text.

35. 18 U.S.C. § 2511(2)(c), (d) (2000).

dating the Wiretap Act's passage in which the Supreme Court upheld the introduction into evidence of communications recorded or transmitted to the government by an undercover agent or informant.[36] The Court reaffirmed these cases after its decision in *Katz*, concluding that the Fourth Amendment does not prevent a party to a conversation from revealing its contents to the government, because a defendant has no "constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police."[37] The Wiretap Act permits a person "acting under color of law" to intercept a communication where the person is a party to the communication or another party has given prior consent.[38] In the case of purely private conduct, the Act permits a person to intercept a communication where the person is a party or where a party has given prior consent, so long as the communication is not intercepted "for the purpose of committing any criminal or tortious act."[39]

Each of these interpretive issues—what it means to "intercept" a communication and when an interception is consensual and thus not unlawful—will present challenges for the application of the Wiretap Act to spyware. I discuss these issues further in Part III.

B. The Stored Communications Act

As previously noted, the Wiretap Act initially prohibited only the interception of wire and oral communications. The extension of the Wiretap Act to electronic communications in 1986 was part of a larger effort to update surveillance law to account for the increasing use of electronic communications.

In particular, Congress recognized that systems allowing for the transmission and receipt of electronic communications necessarily involved the *storage* of such communications.[40] During hearings on how

---

36. *See, e.g.*, Osborn v. United States, 385 U.S. 323 (1966) (admitting recording taped by government informant and concluding that case involved "not . . . surreptitious surveillance of a private conversation by an outsider, but . . . the use by one party of a device to make an accurate record of a conversation"); Hoffa v. United States, 385 U.S. 293, 302 (1966) (declining to suppress government informant's testimony because Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); Lopez v. United States, 373 U.S. 427, 439 (1963) (holding that evidence derived from a conversation recorded by a government agent was admissible).

37. United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion); *see* United States v. Caceres, 440 U.S. 741, 750-51 (1979) (following *White*).

38. 18 U.S.C. § 2511(2)(c) (2000).

39. *Id.* § 2511(2)(d).

40. *See, e.g.*, S. REP. NO. 99-541, at 8 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3562 (describing e-mail systems); H.R. REP. NO. 99-647, at 22 (1986) (same).

Congress should update surveillance law, industry representatives emphasized that the development of electronic communication services necessarily depended upon Congress providing a degree of statutory protection for stored communications.[41] Quite apart from the need to protect stored communications against intrusions by private parties, Supreme Court case law cast doubt upon whether stored communications were entitled to any Fourth Amendment protection against government acquisition.[42]

In *United States v. Miller*,[43] the Supreme Court weighed a defendant's Fourth Amendment challenge to the government's use of a subpoena to obtain certain records from the defendant's banks. The defendant moved to suppress the records on the ground that the Fourth Amendment required a search warrant. The Court held that because the defendant had voluntarily conveyed the items in question—including checks, financial statements, and deposit slips—to the banks, he had no legitimate expectation of privacy in the documents' contents.[44]

A broad reading of *Miller* would suggest that users storing electronic communications with service providers similarly surrender Fourth Amendment protection, because they have voluntarily conveyed those communications to a third party. As I have argued elsewhere, there are compelling reasons to reject this broad reading.[45] *Miller* nevertheless pro-

---

41. *See, e.g.*, S. REP. NO. 99-541, at 5, *as reprinted in* 1986 U.S.C.C.A.N. at 3559 (noting that gap in statutory protection "may unnecessarily discourage potential customers from using innovative communications systems" and "discourage American businesses from development of new innovative forms of telecommunications and computer technology"); H.R. REP. NO. 99-647, at 19 (noting that absence of legal protection for "may unnecessarily discourage potential customers from using such systems, and encourage unauthorized users to obtain access to communications to which they are not a party"); *see also Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights and Trademarks, Senate Comm. on the Judiciary*, 99th Cong., 1st Sess. 121-22 (1987) (testimony of Philip M. Walker on behalf of e-mail industry noting vulnerability of communications while stored in provider's systems).

42. Indeed, the committee reports on ECPA reflected conflicting views on whether the Fourth Amendment protected stored communications. *Compare* S. REP. NO. 99-451, at 3, *as reprinted in* 1986 U.S.C.C.A.N. at 3557 (suggesting that communications in the hands of a third party "may be subject to no constitutional privacy protection"), *with* H.R. REP. NO. 99-647, at 22 ("It appears likely . . . that the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required.").

43. 425 U.S. 435 (1976).

44. *Id.* at 440.

45. *See* Bellia, *supra* note 22, at 1397-1412. The reasoning underlying *Miller* is questionable. In particular, *Miller* conflates two distinct lines of Supreme Court cases. *Id.* at 1397-1400. In the first line of cases, the Supreme Court rejected defendants' claims that the government could not acquire business records turned over to third parties with-

vided the foundation for some of ECPA's provisions regulating acquisition of stored communications, also known as the Stored Communications Act (SCA).[46] Like the Wiretap Act, the SCA prohibits all parties from gaining access to certain kinds of communications,[47] but also identifies a range of circumstances in which law enforcement officials are authorized to do so.[48] Although the government access provisions require law en-

---

out a search warrant, finding a subpoena adequate. *See, e.g.*, Couch v. United States, 409 U.S. 322, 335 (1973); Oklahoma Press Pub'g Co. v. Walling, 327 U.S. 186, 208 (1946). In those cases, the Court's reasoning relied not only on the fact that the records were provided to a third party, but on the *nature of the records* involved. *See, e.g.*, *Couch*, 409 U.S. at 335 (rejecting taxpayer's challenge to summons requiring accountant to surrender taxpayer's records and concluding that "there can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return"). In the second line of cases, the Supreme Court rejected claims that the Fourth Amendment prohibits the government from introducing into evidence communications revealed, recorded, or transmitted to the government by a government informant or undercover agent who is a party to the communications. *See supra* notes 36-37 (citing cases). In those cases, the Court essentially concluded that one who converses with another *assumes the risk* that the conversation will be revealed to law enforcement officials, thus eliminating any possible expectation of privacy. *See, e.g.*, United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion) (noting that the *Katz* court did not "indicate in any way that defendant has a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police").

Miller was a business records case. In relying on the government informant cases, however, the *Miller* Court introduced an assumption-of-risk analysis not previously prominent in the business records cases. *See* Bellia, *supra* note 22, at 1402. Even if *Miller*'s analysis is correct, there are other reasons not to use the *Miller* framework in evaluating whether a user has an expectation of privacy in communications the user conveys to a service provider. The circumstances in *Miller* differ significantly from the circumstances involved when a subscriber relies on a service provider to transmit and store communications. First, *Miller* involved negotiable instruments rather than personal communications. Second, in *Miller*, the defendant's purpose in conveying the records to the bank—for the bank to complete certain transactions—made the substance of the records independently relevant to the bank. An e-mail subscriber's purpose in conveying the contents of a communication to a service provider is simply to have the provider transmit the communication. The contents of the communications are of no relevance to the service provider. *See id.* at 1403-05.

46. *See, e.g.*, S. REP. NO. 99-541, at 3, *as reprinted in* 1986 U.S.C.C.A.N. at 3557 (discussing *Miller*); H.R. REP. NO. 99-647, at 23 & nn.40-41 (same); Bellia, *supra* note 22, at 1413 (noting that provisions of the SCA allow for compelled production of the contents of communications without a search warrant in some circumstances—a result that is constitutional only if a user lacks an expectation of privacy in at least some communications stored by a provider).

47. 18 U.S.C. § 2701(a) (2000).

48. *Id.* § 2701(c); 18 U.S.C. § 2703 (2000 & Supp. II 2002).

forcement officials to obtain a warrant in some circumstances,[49] in others they allow law enforcement officials to acquire communications with a subpoena or a special court order with standards lower than those required by the Fourth Amendment.[50] Whether a warrant is required turns on interpretation of key statutory terms, such as when communications are held "in electronic storage" by the provider of an "electronic communication service."[51] Those same terms also appear in the SCA's substantive prohibition, 18 U.S.C. § 2701(a), which provides for criminal penalties and civil damages against one 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 . . . .

Like the Wiretap Act, the SCA presents a number of difficult interpretive issues. The first difficulty is how to reconcile the Wiretap Act with the SCA. As noted, the Wiretap Act does not define interception with enough specificity to foreclose claims that acquisition of stored communications constitute an interception. Second, § 2701(a) applies only when a defendant gains access to a "facility through which an electronic communication service is provided."[52] Although that phrase quite clearly would cover the mail servers of an e-mail provider, it is not clear what other facilities the statute covers. Third, with respect to application of the provisions authorizing government access to stored communications,[53] the Justice Department has argued quite forcefully for a narrow construction of "electronic storage"[54]—an interpretation that obviously has significant bearing on the scope of § 2701(a), which protects electronic communications only "while . . . in electronic storage."[55] Fourth, because liability under

49. *See* 18 U.S.C. § 2703(a) (Supp. II 2002).
50. 18 U.S.C. § 2703(b) (2000).
51. *See* 18 U.S.C. § 2703(a) (Supp. II 2002).
52. 18 U.S.C. § 2701(a) (2000).
53. *See* 18 U.S.C. § 2703(a), (b) (2000 & Supp. II 2002).
54. *See, e.g.*, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 88-89 (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf [hereinafter CCIPS MANUAL].
55. 18 U.S.C. § 2701(a) (2000).

§ 2701(a) turns on whether access to the communications facility is unauthorized,[56] in any given case it will be important to determine the scope of the defendant's authority. Relatedly, like the Wiretap Act, the SCA has a consent exception. Section 2701(c)(2) provides that § 2701(a) does not apply with respect to conduct authorized "by a user of [an electronic communication service] with respect to a communication of or intended for that user."[57] Accordingly, a likely point of contention in any particular case will be whether a "user" has consented to the acquisition of his or her communications.

C. The Pen/Trap Statute

The final federal statute regulating electronic surveillance activities prohibits the use of "pen registers" and "trap and trace devices."[58] The pen/trap provisions formed part of ECPA,[59] and, like the SCA, sought to provide statutory protection following a Supreme Court decision on the application of the Fourth Amendment to certain government conduct.

In the 1979 case of *Smith v. Maryland*,[60] police investigating a robbery requested that a telephone company install a "pen register"—understood at the time to mean a device that records the numbers dialed on a telephone by monitoring electrical impulses triggered when the dial is released—on the defendant's home telephone line.[61] The information gleaned (specifically, the fact that the defendant made repeated calls to the robbery victim) provided the basis for a search warrant. The defendant sought to suppress the fruits of that search on the ground that the pen register was installed without a warrant.[62] Following the reasoning of *Katz* and *Miller*, the Court concluded that the defendant lacked any expectation of privacy in the telephone numbers he dialed: "Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[63]

In light of *Smith*'s conclusion that use of a pen register does not implicate the Fourth Amendment, Congress passed a statute providing minimal

---

56. *Id.*
57. *Id.* § 2701(c)(2).
58. 18 U.S.C. §§ 3121-3127 (2000 & Supp. II 2002).
59. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301, 100 Stat. 1848, 1868-73.
60. 442 U.S. 735 (1979).
61. *Id.* at 736-37 & n.1.
62. *Id.* at 737.
63. *Id.* at 743.

statutory protection against the use of pen registers as well as trap and trace devices (that is, devices designed to capture the origin of an incoming communication). Unlike the Wiretap Act and the SCA, the pen/trap statute does not create a civil action for violation of its provisions. Instead, it is a misdemeanor for one to "install or use a pen register or a trap and trace device without first obtaining a court order" as specified under federal law.[64] Nor does the statute provide for suppression of evidence in violation of its provisions. As a result, litigation involving the pen/trap statute is rare. But in the debate over how electronic surveillance law applies to spyware, there is considerable uncertainty as to where to draw the line between conduct prohibited by the Wiretap Act and conduct prohibited by the pen/trap statute.

As noted earlier, the Wiretap Act prohibits the interception of the *contents* of a communication.[65] The Wiretap Act defines the term "contents" to include the "substance, purport, or meaning" of a communication.[66] Information falling outside of that category—such as dialing information associated with a telephone communication or addressing or routing information associated with an electronic communication—is statutorily protected,[67] if at all, only by the pen/trap statute. With respect to information associated with electronic communications, however, the application of the pen/trap statute has historically been unclear. Although Congress clarified the reach of the pen/trap statute in the USA Patriot Act,[68] it essentially left the determination of where to draw the line between the Wiretap Act and the pen/trap statute in the hands of the courts.

When the pen/trap statute was first passed in 1986, there was ambiguity as to whether it applied to electronic communications at all. On the one hand, portions of the statute appeared to focus exclusively on telephone numbers. For example, the statute required the court order to specify the number of the "telephone line" to which the pen register or trap and trace device would be attached[69] as well as the subscriber of that telephone line.[70] The statute also defined a pen register as a device that "records or

64. 18 U.S.C. § 3121(a) (2000); *id.* § 3121(d) (setting forth penalty).

65. *Id.* § 2510(4) (defining "intercept").

66. *Id.* § 2510(8).

67. Although *Smith v. Maryland* makes clear that dialing information associated with a telephone call is not entitled to Fourth Amendment protection, the application of the Fourth Amendment to information associated with an electronic communication is more complicated. For further discussion, see Bellia, *supra* note 22, at 1428-30.

68. *See* Pub. L. No. 107-56, § 216, 115 Stat. at 283 (codified at 18 U.S.C. § 3127(3), (4) (Supp. II 2002)).

69. 18 U.S.C. § 3123(b)(1)(C) (2000).

70. *Id.* § 3123(b)(1)(A).

decodes electronic or other impulses which identify the *numbers dialed* or otherwise transmitted on the telephone line to which such device is attached."[71] On the other hand, the statute defined a trap and trace device as a device to capture the "originating number" from which "a wire *or electronic* communication was transmitted,"[72] thereby suggesting that the statute covered at least some identifying information associated with electronic communications. It was thus unclear whether the statute regulated the use of devices to obtain address information associated with electronic communications.

In the USA Patriot Act, Congress expanded the "pen register" and "trap and trace device" definitions, thereby clarifying that the statute covers devices used to obtain information associated with electronic communications.[73] The definitions apply to devices that gather "dialing, routing, addressing, or signaling information" indicating the source or destination of a wire or electronic communication.[74] In expanding the definitions, however, Congress expressly excluded from each definition "the contents of any communication." The exclusion was designed to allay concerns that addressing information associated with electronic communications would in some cases reveal the content of a communication, as where a web page's uniform resource locator (URL) incorporates search terms.[75] Rather than responding to these concerns by specifically indicating that URLs were to be considered "contents," Congress left the matter to judicial interpretation.

With respect to spyware designed to gather URLs and similar data, de-

---

71. *Id.* § 3127(3) (emphasis added).

72. *Id.* § 3127(4) (emphasis added).

73. *See* Pub. L. No. 107-56, § 216, 115 Stat. at 283 (codified at 18 U.S.C. § 3127(3), (4) (Supp. II 2002)).

74. *See* 18 U.S.C. § 3127(3) (Supp. II 2002) (defining "pen register" in part as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"); *id.* § 3127(4) (defining "trap and trace device" in part as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication").

75. For example, a search for a book on breast cancer on Barnes & Noble's website might generate a page displaying search results with the following URL: http://search.barnesandnoble.com/booksearch/results.asp?WRD=breast+cancer&userid=[redacted]. For privacy advocates' objections to the expansion of the pen/trap statute, see, for example, *Protecting Constitutional Freedoms in the Face of Terrorism: Hearing Before the Subcomm. on Constitution, Federalism, and Property Rights of the S. Judiciary Comm.*, 107 Cong. (2001) (testimony of Jerry Berman, Executive Director, Center for Democracy & Technology), *available at* http://www.cdt.org/testimony/011003berman.shtml.

fendants will no doubt argue that such data does not reflect the "contents" of a communication for purposes of the Wiretap Act. Although I do not independently discuss application of the pen/trap statute to spyware, I explore the content/noncontent distinction in the course of discussing application of the Wiretap Act.

III. THE CHALLENGES OF APPLYING SURVEILLANCE LAW TO SPYWARE

Part II sets forth the basic structure of the federal electronic surveillance framework. Application of surveillance statutes to spyware is intuitively appealing: the statutes prohibit the interception or unauthorized acquisition of "electronic communications," and some forms of spyware clearly do capture users' electronic communications. As discussed below, however, there are good reasons to be skeptical that surveillance law statutes will curb anything but the most extreme forms of spyware.

Controversy surrounds the application of the term "spyware," and many products might fall within or just outside of the spyware category.[76] In assessing the applicability of surveillance law statutes, I focus on two products that are often labeled spyware: keystroke monitors and software designed to track Internet usage and deliver targeted advertising. These products illustrate a number of problems with applying electronic surveillance law to spyware, although I hope to sidestep the controversy over the appropriate use of the spyware label with respect to these products. In Section A, I briefly discuss the technology at issue. In Sections B and C, I discuss application of the Wiretap Act and the SCA, respectively.

A. The Technology at Issue

I begin with the application of electronic surveillance statutes to software and hardware devices that serve as "keystroke monitors"—that is, programs and devices that monitor every keystroke typed on a given computer.[77] Other devices and programs—such as "screen shot" utilities,

---

76. *See, e.g.*, H.R. REP. NO. 109-32, at 10 (2005) (report of Committee on Energy and Commerce, noting that the committee, "received testimony that spyware represents a range of software programs on a broad continuum from the most pernicious criminal activities on one end to the less threatening but still intrusive on the opposite end of the spectrum"); FTC STAFF REPORT, *supra* note 1, at 3 ("Panelists generally agreed that reaching an industry consensus on one definition [of spyware] has been elusive because of the technical complexity and dynamic nature of software.").

77. Hardware and software advertised to have such capabilities includes KeyKatcher, http://www.keykatcher.com (last visited Sept. 1, 2005); Keylogger Pro, *see* http://www.exploreanywhere.com/kp-intro.php (last visited Sept. 1, 2005); and iSpyNow,

which store images of what a computer screen displays at particular intervals—will raise similar analytical issues.[78] Keystroke monitors represent one of the most egregious forms of spyware when deployed against an unwitting user. Keystroke monitors consist of either hardware devices that attach to a computer at a point between the computer and its central processing unit (CPU)[79] or software programs installed by a person with administrative control of a computer or perhaps even remotely, through a security vulnerability or as part of a bundle of software.[80] Keystroke monitors are used for a range of purposes including lawful ones. An employer may deploy such a tool to monitor or deter abuse of a company computer system, or a parent may use it to monitor a child's Internet usage. Such programs and devices obviously have far more problematic uses as well: for hackers to acquire passwords, credit card numbers, or financial information, for one spouse to monitor another's online behavior, or for one coworker to spy on another.

I also consider the application of surveillance law to software installed on a user's computer to track the user's Internet usage and deliver targeted advertising. Such software is often referred to as "adware"; precisely where to draw the line between "adware" and "spyware" is controversial.[81] Most commentators focus on the issue of consent: when the user does not receive appropriate notice of the software's activities or lacks the ability to decline its installation, such software meets the definition of spyware.[82] Of course, what constitutes appropriate notice or adequate consent is itself a difficult issue. For purposes of my analysis, the "adware" or "spyware" label is less important than an understanding of how the software functions.

Recent litigation over software that allegedly tracks users' Internet ac-

---

see http://www.ispynow.com (last visited Sept. 1, 2005).

78. For a case involving a dispute over a wife's use of a screen shot utility to record her husband's online activities to find evidence of infidelity, see O'Brien v. O'Brien, 899 So. 2d 1133 (Fla. Dist. Ct. App. 2005).

79. KeyKatcher operates in this manner. *See* http://www.keykatcher.com (last visited Sept. 1, 2005). For discussion of a case involving use of this device, see *infra* notes 107-113 and accompanying text.

80. For example, a tool called Perfect Keylogger was advertised as having a "unique *remote installation* feature. You can attach keylogger to any other program and send it by e-mail to install on the remote PC in the stealth mode." *See* http://www.blazing tools.com/bpk.html (last visited Sept. 7, 2004) (on file with author).

81. *See, e.g.*, FTC STAFF REPORT, *supra* note 1, at 3-4 (noting range of views on whether and when adware should be classified as spyware).

82. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2065 (2004).

tivities sheds some light on how targeted advertising software functions.[83] WhenU.com's "SaveNow" software provides one example. Typically, a user downloads the SaveNow software as part of a bundle of free software.[84] Once loaded onto a user's computer, the SaveNow software launches whenever the user's browser is active. The software scans data from a browsing session, including URLs, search terms typed into a search engine, and the contents of a requested page.[85] The software compares the URLs, search terms, or keywords drawn from a web page to terms in its proprietary database.[86] A match triggers contextual pop-up advertising.[87]

Keystroke monitors and software for contextual advertising represent only two among a wide range of products that might be considered spyware.[88] Nevertheless, they illustrate the difficulties of applying electronic surveillance law to spyware. Because of significant overlap among the issues with respect to each type of product, I discuss the issues by statute rather than by product.

As I will show, electronic surveillance law constrains only the most extreme forms of spyware—and even then, there are pitfalls. Although the Wiretap Act presents an obvious option for controlling devices and software with keystroke monitoring capabilities, current case law suggests that the matter is more complicated. With respect to applications that gather data and communications so as to provide targeted advertising, the issue of consent will be an impediment to controlling the distribution of software that many would regard as deceptive and highly privacy-intrusive. In other words, surveillance law may be used to target the most serious forms of spyware, but it is unlikely to otherwise force change in industry practices concerning the distribution and functionality of software.

---

83. *See, e.g.*, 1-800 CONTACTS, Inc. v. WhenU.com, 414 F.3d 400, 2005 U.S. App. LEXIS 12711, at *1 (2d Cir. Jun. 27, 2005); Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734 (E.D. Mich. 2003); U-Haul Int'l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723 (E.D. Va. 2003).

84. *See 1-800 CONTACTS*, 2005 U.S. App. LEXIS 12711, at *9; *Wells Fargo*, 293 F. Supp. 2d at 743; *U-Haul*, 279 F. Supp. 2d at 725.

85. *See 1-800 CONTACTS*, 2005 U.S. App. LEXIS 12711, at *10; *Wells Fargo*, 293 F. Supp. 2d at 743-44; *U-Haul*, 279 F. Supp. 2d at 725.

86. *See 1-800 CONTACTS*, 2005 U.S. App. LEXIS 12711, at *10; *Wells Fargo*, 293 F. Supp. 2d at 743; *U-Haul*, 279 F. Supp. 2d 725-26.

87. *See 1-800 CONTACTS*, 2005 U.S. App. LEXIS 12711, at *10-*11; *Wells Fargo*, 293 F. Supp. 2d at 743; *U-Haul*, 279 F. Supp. 2d at 726.

88. For further discussion of products that might be considered "spyware," see H.R. REP. 109-32, at 10-11 (2005); FTC STAFF REPORT, *supra* note 1, at 2-8.

B. The Wiretap Act

1. The "Interception" Problem

As discussed earlier, § 2511(1)(a) of the Wiretap Act prohibits any person from "intentionally intercept[ing] . . . a wire, oral, or electronic communication."[89] The term "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[90] The first question in applying the Wiretap Act to spyware, then, is whether the use of a particular spyware product in fact results in the "intercept[ion]" of the "contents" of an "electronic communication."

I alluded earlier to one difficulty with the term interception: determining whether a communication must be captured in transmission to qualify or whether the Wiretap Act also covers acquisition of communications from storage (as when an e-mail is held for retrieval by the recipient).[91] Most courts have agreed that interception occurs when electronic communications are acquired during transmission and not when they are acquired from storage.[92] But even with spyware used on an ongoing basis to monitor data as it is being transmitted, interpretive issues may still impede application of the Wiretap Act.

Keystroke monitors present particular difficulties. In many cases, a keystroke monitor will capture data solely within a single computer system—perhaps, as noted, between the keyboard and the CPU. The issue is whether acquisition of data within a single system can constitute an interception of an electronic communication.

Two courts considering that question have concluded that interception of a communication cannot occur within a single system. In *United States v. Scarfo*,[93] federal investigators, after obtaining a warrant, attached a keystroke monitor to the computer of a defendant suspected of running an illegal gambling and loan-sharking operation.[94] The investigators sought to obtain the password for the defendant's encryption software. They successfully obtained that password, which allowed decryption of other previously obtained files.[95] The defendant later moved to suppress evidence

89. 18 U.S.C. § 2511(1)(a) (2000).

90. *Id.* § 2510(4). The statute does not define the term "device."

91. *See supra* notes 33-34 and accompanying text; *infra* notes 194-229, 281-293 and accompanying text.

92. *See supra* note 34 (citing cases).

93. 180 F. Supp. 2d 572 (D.N.J. 2001).

94. *Id.* at 574.

95. *Id.*

derived from the use of the keystroke monitor on the theory that the government should have obtained a full Title III order before installing the device.[96] The issue was whether the government's use of the device resulted in the interception of communications without a Title III order.[97]

The government argued that the keystroke monitor did not "intercept" communications within the meaning of the Wiretap Act. In particular, the government configured the device to determine whether the modem on the defendant's computer was operating at any point in time; if the modem was operating, the keystroke monitor would not collect data.[98] In other words, the device would not capture a keystroke unless all of the computer's communication ports were inactive.[99] The district court concluded that in this context, no Title III order was necessary: the keystroke monitor acquired only data "within" the defendant's computer.[100]

The court's opinion was somewhat opaque in two respects. First, it alternately referred to the communications the government was alleged to have intercepted as "wire communications"[101] and "electronic communications."[102] Because the communications did not contain the human voice, they could not have been "wire" communications.[103] The distinction between electronic and wire communications in fact should have been crucial to the case. The Wiretap Act provides no suppression remedy for acquisition of an electronic communication in violation of its terms;[104] a motion to suppress electronic communications could have been based only on the Fourth Amendment. In *Scarfo*, however, the defendant sought suppression only under the Wiretap Act.[105] Second, the court never clearly explained why the modem's inactivity precluded the court from treating the

96. *Id.*
97. *Id.* at 575.
98. *Id.* at 581-82.
99. *Id.* at 582.
100. *Id.* at 582 n.5.
101. *See id.* at 576, 582.
102. *See id.* at 581-82.
103. *See* 18 U.S.C. § 2510(1) (2000) (defining wire communication as an "aural transfer"); *id.* § 2510(18) (defining aural transfer as "a transfer containing the human voice").
104. *See id.* § 2515 (barring introduction of contents of intercepted wire or oral communications into evidence); *id.* § 2518(10)(a) (permitting motion to suppress contents of wire or oral communication); *id.* § 2518(10)(c) (deeming remedies described with respect to electronic communications "the only judicial remedies and sanctions for nonconstitutional violations of this chapter"). Confusion over Title III's suppression provisions is not uncommon. *See* Bellia, *supra* note 22, at 1392-93 n.106.
105. 180 F. Supp. 2d at 576 (noting defendant's claim that government intercepted a communication "in violation of Title III").

acquisition of the communications as an interception. It is possible to construct one rationale, although the district court did not articulate it. By definition, an "electronic communication" must be transmitted by a system "that affects interstate or foreign commerce."[106] It could be argued that communications purely internal to a computer are not transmitted by a system affecting interstate commerce and therefore are not "electronic communications."

In *United States v. Ropp*,[107] the district court essentially adopted this rationale. *Ropp* involved a government prosecution under the Wiretap Act of a defendant who installed a keystroke monitor on a co-worker's computer.[108] The defendant physically attached a "KeyKatcher" device to the co-worker's computer where the keyboard attached to the computer's CPU.[109] The device picked up every keystroke as it was transmitted from the keyboard to the CPU.

In analyzing the legality of the defendant's behavior under the Wiretap Act, the district court focused on whether an "electronic communication" was involved. Recall the government's position in *Scarfo*: the Wiretap Act is not implicated where data is retrieved from within a computer system without an active communications port. In *Ropp*, the government took a slightly different position: the Wiretap Act applies to the acquisition of "any signal transmitted from a keyboard to a computer *with an internet connection*," "whether or not the internet connection was activated at the time of the transmission."[110] In other words, the government's position in *Scarfo* at least implicitly suggested that a communication that merely exists within a single computer does not constitute an "electronic communication," even if the computer can connect to the Internet. In *Ropp*, the government argued that a communication within a single computer with an available Internet connection does constitute an "electronic communication," because "the system by virtue of that connection 'affects interstate commerce.'"[111]

The *Ropp* court rejected the government's new approach and, relying on *Scarfo*, concluded that the Wiretap Act's definition of electronic communications applies only to data that is in fact being transmitted beyond a local computer by a system that affects interstate or foreign commerce.[112]

---

106. 18 U.S.C. § 2510(12) (2000).
107. 347 F. Supp. 2d 831 (C.D. Cal. 2004).
108. *Id.*
109. *Id.*
110. *Id.* at 835 (emphasis added).
111. *Id.*
112. *Id.* at 836, 837-38.

Even though the defendant's device captured keystrokes used in the composition of e-mail, the court concluded that no interception of an electronic communication occurred. Although the computer system from which the communications were acquired "is connected to a larger system—the network—which affects interstate or foreign commerce, the transmission at issue did not involve that system."[113]

In short, *Scarfo* and *Ropp* essentially hold that if a device or program is capturing communications at a point where the communications are internal to the user's system, then no interception occurs. Under this analysis, the Wiretap Act fails to regulate some of the most problematic forms of spyware, including keystroke monitors. Depending on how a particular piece of software operates, the Act may also fail to regulate software designed to facilitate contextual advertising, regardless of how much data the software acquires. Because such software is proprietary, it is often difficult to determine precisely how the software works. In particular, it is unclear whether such software captures data at a point within the user's computer or as communications are transmitted to the Internet. Under case law such as *Scarfo* and *Ropp*, these seemingly trivial issues become critical.

Of course, the extent to which *Scarfo* and *Ropp* will constrain distribution and use of keystroke monitors depends partly upon the extent to which they remain good law. The Wiretap Act ruling in *Scarfo* was apparently not appealed; the government sought reconsideration of the *Ropp* decision at the district court level, and its motion remains unresolved.[114]

---

113. *Id.* at 838.

114. The *Ropp* court buttressed its conclusion with one decision that is no longer good law, United States v. Councilman, 373 F.3d 197 (1st Cir. 2004), *reh'g en banc granted and opinion withdrawn*, 385 F.3d 793 (2004), *on reh'g en banc*, No. 03-1383, 2005 U.S. App. LEXIS 16803 (1st Cir. Aug. 11, 2005). *See Ropp*, 347 F. Supp. 2d at 836-38. In the *Councilman* case, the government sought to prosecute under the Wiretap Act an Internet service provider that captured the communications of its customers before transmitting them into to the customers' mailboxes. The district court and a panel of the U.S. Court of Appeals for the First Circuit held that the communications were acquired during a brief period of storage within the provider's system and therefore were not intercepted for purposes of the Wiretap Act. *Councilman*, 373 F.3d at 199. Relying on *Councilman*, the *Ropp* court reasoned that if messages momentarily stored within a provider's system are not intercepted for purposes of the Wiretap Act, then signals internal to a computer prior to transmission certainly cannot be. *Ropp*, 347 F. Supp. 2d at 838.

The reasoning in *Councilman* was weak. Several courts construing the Wiretap Act had previously held that the statute does not protect stored communications. *See supra* note 34 (citing cases). Those cases differed from *Councilman* in an important respect, however: they involved a one-time acquisition of communications maintained by a service provider for retrieval by the subscriber, whereas *Councilman* involved an ongoing acquisition of communications briefly stored during the transmission process prior to

With respect to both cases, it is tempting for commentators to argue that the cases involved erroneous reasoning or could be easily overturned with a statutory fix.[115] It is nevertheless important to recognize one outer limit on any judicial or legislative response. Most of the Wiretap Act was enacted under Congress's power under the Commerce Clause;[116] that was undoubtedly one reason for linking the definition of an electronic communication to a transmission involving a system "that affects interstate or foreign commerce."[117] It is difficult to see how, under current Commerce Clause jurisprudence, Congress could attempt to constrain use of a keystroke monitor on a standalone computer. The question then becomes whether the fact that a computer is networked, without more, necessarily sweeps it within Congress's reach.

2. The "Consent" Problem

If courts move past the "interception" problem, the Wiretap Act may become a tool for controlling spyware that is surreptitiously installed. For other forms of spyware, however, the problem of "consent" may become a

---

being made available to the subscriber. On rehearing *en banc*, the First Circuit rejected the district court and panel decisions, holding that the Wiretap Act prohibits the acquisition of electronic communications during transmission, even if those communications are briefly stored during the transmission process. *Councilman*, 2005 WL 1907258, at *10.

Although the *Ropp* court did discuss the panel opinion in *Councilman*, the reversal of the *Councilman* decision has little bearing on the central issue in *Ropp*: whether communications wholly within a single computer system constitute "electronic communications."

115. *See, e.g.*, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1265, 1282 (describing *Scarfo* as involving "an end run around [the Wiretap Act] based on a technicality").

116. *See* S. REP. NO. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2180. As the report of the Senate Judiciary Committee accompanying the Wiretap Act suggested, "the facilities used to transmit wire communications form part of the interstate or foreign communications network." *Id.* For oral communications, the congressional power issues were more complicated. Such communications are far less likely to affect interstate commerce. To the extent that the provisions regulate acquisition of oral communications by state officials, the statute can be viewed as "enforcement" of the Fourth Amendment, as incorporated by the Fourteenth Amendment, because the statute defines oral communications as communications uttered by a person exhibiting a justifiable expectation that such communication is not subject to interception. *See* 18 U.S.C. § 2510(2) (2000). For provisions regulating acquisition of oral communications by private parties, the constitutional hook is less clear. The Judiciary Committee report contains an unusually candid discussion of the potential constitutional problems with application of the statute to private conduct. *See* S. REP. NO. 90-1097, *as reprinted in* 1968 U.S.C.C.A.N. at 2180.

117. *See* H.R. REP. NO. 99-647, at 35 (1986) (noting that the definition was "intended to cover a broad range of communication activities that affect interstate or foreign commerce").

major impediment to the application of the statute. As noted earlier, the Wiretap Act contains consent exceptions both for conduct under color of law[118] and purely private conduct.[119] For purely private conduct, § 2511(2)(d) of the Wiretap Act provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

What constitutes "prior consent" for purposes of the Wiretap Act? As noted earlier, employers may lawfully deploy keystroke monitors or similar devices to monitor employees' use of a company computer system. Generally, employers avoid liability under the Wiretap Act by providing notice of their monitoring activities—by displaying computer screen "banners" to inform employees that use of a company computer system constitutes consent to monitoring or by providing an "acceptable use" policy (perhaps signed by the employee) stating that monitoring may occur. But consent issues may arise even when a user is not directly confronted with a warning banner or fails to sign an acceptable use policy.

Assume, for example, that a user downloads a "bundle" of software products, and one piece of software within that bundle collects a user's data or communications. Those monitoring capabilities may be identified in an accompanying license agreement requiring the user to click "I Agree" before downloading the products. Does clicking "I Agree" constitute "consent" to satisfy § 2511(2)(d) of the Wiretap Act? This question will arise more commonly with software that monitors a user's communications so as to generate targeted advertising than with keystroke monitors. But in either scenario, no clear answer exists. On the one hand, courts applying related doctrines (including different provisions of the Computer Fraud and Abuse Act (CFAA)[120] and common law analogues) have broadly construed license agreements in favor of licensors—even when it

118. 18 U.S.C. § 2511(2)(c) (2000).

119. *Id.* § 2511(2)(d).

120. 18 U.S.C. § 1030 (2000 & Supp. II 2002). Technically, the title Computer Fraud and Abuse Act refers to the 1986 amendments to 18 U.S.C. § 1030, see Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 1, 100 Stat. 1213, but courts commonly use it to describe 18 U.S.C. § 1030 as a whole.

is questionable whether the licensee has manifested assent to particular notices provided by the licensor.[121] On the other hand, commentators (myself included) have criticized this trend.[122] For plaintiffs seeking to argue that the gathering of data or communications constitutes a violation of the Wiretap Act, the First Circuit's decision in *In re Pharmatrak Privacy Litigation* provides perhaps the most support.[123]

---

121. These issues arise in a variety of doctrinal contexts, including contract claims, application of the CFAA, and application of common law trespass to chattels doctrine. For contract claims, cases involving "shrinkwrap" licenses, where the consumer's act of breaking the shrinkwrap is deemed to be assent to the governing terms, form the foundation for courts' analysis. The trend among courts is to enforce such licenses, so long as the consumer has a right to reject the terms by returning the product. *See, e.g.*, ProCD v. Zeidenberg, 86 F.3d 1447, 1452-53 (7th Cir. 1996); Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149-50 (7th Cir. 1997). Extending this reasoning to the online context, courts have enforced "clickwrap" or "click-through" licenses that require a user to click "I Agree" or "I Accept" before downloading a particular product, at least where the "offer" makes clear that clicking the button will signify assent to the terms. *Compare* i.Lan Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002) (enforcing license where terms appeared on screen prior to software installation and defendant checked "I Agree" box), Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007, 1010–11 (D.C. 2002) (enforcing forum selection clause where terms were displayed in scroll box and plaintiff subscriber clicked "Accept" button), Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 530–31 (N.J. Super. Ct. App. Div. 1999) (enforcing forum selection clause contained in agreement with ISP, where prospective subscriber could only access service by clicking "I Agree"), Moore v. Microsoft Corp., 741 N.Y.S.2d 91, 92 (App. Div. 2002) (dismissing claim against software manufacturer where plaintiff user clicked on "I agree" icon before downloading software and claim was barred by license agreement), *and* Barnett v. Network Solutions, Inc., 38 S.W.3d 200, 204 (Tex. App. 2001) (finding forum selection clause enforceable where plaintiff had to scroll through terms and accept them before proceeding), *with* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 31-32 (2d Cir. 2002) (finding license terms unenforceable where terms appeared only on portion of webpage below software download button). For CFAA claims enforcing "terms of use" with minimal discussion of issues of notice and assent, see Am. Online v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1276 (N.D. Iowa 2000); Am. Online v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998); *cf.* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) (suggesting that terms of use appearing on website would define the boundaries of use for purposes of CFAA). For similar approaches in trespass to chattels cases, see *LCGM*, 46 F. Supp. 2d at 448; Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) 1020, 1025 (N.D. Cal. 1998). I discuss the nuances of these and similar cases in Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2225-45 (2004).

122. *See* Bellia, *supra* note 121, at 2245-52. Much of commentators' concern is driven by intellectual property law, in that broad enforcement of license agreements will allow content providers to appropriate control over content that copyright law would not permit. For discussion of such arguments, see *id.* at 2193-2201. There are, however, important fair notice concerns as well. *See id.* at 2192-93.

123. 329 F.3d 9 (1st Cir. 2003) [hereinafter *Pharmatrak II*], *on remand*, 292 F. Supp.

Pharmatrak constitutes one in a series of cases in which plaintiffs claimed that the placement of "cookies" on their hard drives violated the Wiretap Act, the SCA, and provisions of the Computer Fraud and Abuse Act.[124] With respect to the Wiretap Act, plaintiffs argued that, through placing cookies on their hard drives, companies intercepted their personal communications.[125] Most of the cases involved third-party advertisers who had arrangements with various sites to serve advertisements to website users.[126] Source code on the affiliated website triggered the user's browser to contact the third-party advertiser's server to provide the appropriate ad; this contact between the user and the third-party advertiser enabled the advertiser to place a cookie on the user's hard drive.[127] The third-party advertiser could associate various information in its database with that cookie (or update the cookie itself to reflect that information), including which of the advertiser's affiliated sites the user viewed and for how long.[128] Because third-party advertisers may be affiliated with a significant number of such sites, their use of cookies can result in substantial gathering of data. Once a third-party advertiser causes a cookie to be written to the user's hard drive, it can associate with that cookie (or update that cookie to reflect) not only information about the sites the user browsed that first caused the cookie to be set, but also information about sites the user subsequently browsed that were affiliated with the same advertiser.[129]

Allegations that the gathered communications included personal information stemmed from the manner in which browsers and web servers interact. When contacting a web server, browsers convey several pieces of information to facilitate the server's response, including the browser type and the language in which the browser is operating. Browsers may also convey the contents of the so-called "Referer" variable—a variable the user's browser typically sets to contain the URL of the previously ac-

---

2d 263 (D. Mass. 2003).

124. *See* In re Toys R Us, Inc. Privacy Litig., 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001); In re Intuit Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001); In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

125. *See, e.g.*, *Toys R Us*, 2001 WL 34517252, at *1, *6-*8; *Chance*, 165 F. Supp. 2d at 1155; *Intuit*, 138 F. Supp. 2d at 1274; *DoubleClick*, 154 F. Supp. 2d at 500.

126. *Pharmatrak* involved a third party, but not an advertiser. *See* In re Pharmatrak Privacy Litig., 220 F. Supp. 2d 4, 7 (D. Mass. 2002) [hereinafter *Pharmatrak I*]. Of the remaining cases cited, the only one not involving a third-party advertiser was *Intuit*. 138 F. Supp. 2d at 1274.

127. *See, e.g.*, *Chance*, 165 F. Supp. 2d at 1156; *DoubleClick*, 154 F. Supp. 2d at 503.

128. *See Pharmatrak II*, 329 F.3d at 14.

129. *See DoubleClick*, 154 F. Supp. 2d at 503-04 & n.12.

cessed web page.[130] The use of certain web forms can result in the incorporation of personal information into a URL.[131] Accordingly, routine interaction of a browser with a third-party advertiser's server could lead to the advertiser's acquisition of personal information.

I discuss in Part IV some of the significant problems with claims that use of cookies violates the surveillance law statutes.[132] Here, I focus on one aspect of the cases: their discussion of the Wiretap Act's consent exception. In most of the cookie cases, courts concluded that no Wiretap Act claim was available, because the companies had effectively consented to the third-party advertiser's acquisition of any communications between the users and the companies' servers.[133] Courts so held even though it was unclear whether the companies knew precisely what information the third-party advertiser could gather. The sole case to break with this trend was *Pharmatrak*.

Pharmatrak had entered into agreements with several pharmaceutical companies to aggregate certain data concerning the companies' users.[134] Like a third-party advertiser, Pharmatrak arranged with the pharmaceutical companies to require them to place on their websites certain source code causing a customer's browser to communicate with Pharmatrak's servers.[135] Communications between the customer and the pharmaceutical websites occasionally involved an exchange of personally identifiable information.[136] In certain cases, because a customer's communication with a pharmaceutical website immediately preceded its communication with Pharmatrak's servers, Pharmatrak's servers captured this personally identi-

---

130. "Referer" is a misspelling of referrer. *See* R. Fielding et al., Hypertext Transfer Protocol–HTTP/1.1 Request for Comments 2616, § 14.36, at 86 (1999), http://www.faqs.org/ftp/rfc/rfc2616.pdf.

131. *See, e.g.*, *Pharmatrak II*, 329 F.3d at 16; *DoubleClick*, 154 F. Supp. 2d at 504.

132. *See infra* notes 230-253 and accompanying text.

133. *See, e.g.*, *Chance*, 165 F. Supp. 2d at 1162; *DoubleClick*, 154 F. Supp. 2d at 514. In *Toys R Us*, the district court recognized that Toys R Us had consented to the third-party's acquisition of communications. 2001 WL 34517252, at *7-*8. The court declined to dismiss the Wiretap Act claim, however, because it believed that the plaintiffs had sufficiently alleged that any interception, though consensual, was undertaken with a tortious purpose. *Id.*; *see* 18 U.S.C. § 2511(2)(d) (2000) (excluding from private-party consent exception communications intercepted "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State"). Similar claims were raised but rejected in other cases. *See Chance*, 165 F. Supp. 2d at 1163; *DoubleClick*, 154 F. Supp. 2d at 519.

134. *Pharmatrak II*, 329 F.3d at 12.

135. *Pharmatrak I*, 220 F. Supp. 2d at 7.

136. *Pharmatrak II*, 329 F.3d at 15-16.

fiable information.[137]

When a group of plaintiffs brought suit alleging that Pharmatrak's conduct violated the Wiretap Act, Pharmatrak responded by asserting that the pharmaceutical defendants were parties to the allegedly intercepted communications and consented to the use of Pharmatrak's system.[138] Other courts had accepted this line of argument in cases involving third-party advertisers,[139] and the district court granted Pharmatrak summary judgment on the claim.[140] Here, however, the First Circuit rejected the consent argument. Although the pharmaceutical companies had in general terms consented to the use of Pharmatrak's proposed system for gathering data on customers, Pharmatrak never made clear that the system would gather personally identifiable information.[141] The companies' general consent to the use of the system was not sufficient to trigger the Wiretap Act's consent exception.

The First Circuit's approach in *Pharmatrak* suggests that the consent exception to the Wiretap Act's prohibition will be triggered only when the consenting party knows with a high degree of specificity what information will be acquired. *Pharmatrak* remains the exception rather than the rule, however; in none of the other cookie cases did courts examining the consent issue require that degree of specificity. Accordingly, the Wiretap Act's consent exception is likely to remain an impediment to applying the statute to software installed after a user is presented with a license agreement.[142] Of course, purveyors of spyware will sometimes use more deceptive tactics, such as installing software remotely through a security vulnerability, or allowing installation of software to proceed even when a user attempts to decline or cancel installation. The Wiretap Act may be more effective in these situations. It is important to note, however, that once software or a device with the capability to collect data or communications is installed or deployed, the method by which it was installed has little bearing on the degree to which the software or device affects the user's privacy interests. In other words, the Wiretap Act calibrates its coverage

137. *Id.* at 16.

138. *Id.* at 19.

139. *See supra* note 133 and accompanying text.

140. *Pharmatrak I*, 220 F. Supp. 2d at 12.

141. *Pharmatrak II*, 329 F.3d at 20.

142. As noted above, see *supra* note 133, plaintiffs have largely been unsuccessful in arguing that an interception, though consensual, is committed with a tortious or criminal purpose. According to the *Chance* and *DoubleClick* courts, it is not enough that the defendant has committed a tort; rather, the primary motivation or determining factor in its actions must have been to injure the plaintiff tortiously. *See Chance*, 165 F. Supp. 2d at 1163; *DoubleClick*, 154 F. Supp. 2d at 518.

based on whether the user in some sense consented to the software or device's installation, not the degree to which the software or device otherwise affects the user's privacy interests. I return to this point in Part IV.

3. The "Content" Problem

A final issue that arises in applying the Wiretap Act to various forms of spyware concerns whether the data seized, even if it is collected as it is transmitted from the user's computer to the Internet, is properly thought of as the "contents" of a communication. The Wiretap Act prohibits only the acquisition of the contents of a communication.[143] When Congress amended the pen/trap statute in the USA Patriot Act to allow acquisition of data associated with electronic communications, it specified that the pen/trap statute cannot be used to acquire the contents of a communication. In doing so, however, Congress created ambiguity as to precisely where the line between the contents of communications and addressing or routing information associated with a communication is to be drawn.[144]

The Wiretap Act defines the "contents" of a communication to include information concerning the "substance, purport, or meaning" of the communication.[145] No court has yet considered the status under the Wiretap Act or the pen/trap statute of URLs, which clearly identify addressing or routing information concerning the source of a communication and thus would fall within the pen register and trap and trace definitions if not for the exclusion of contents. If a Wiretap Act claim were brought in a case involving acquisition of URLs and search terms through use of a keystroke monitor or software for contextual advertising, there is little doubt that a defendant would argue that the communications in question did not reflect content.

Nevertheless, powerful arguments can be made that much of what a keystroke monitor or software designed to facilitate contextual advertising would capture constitutes the contents of a communication. There are certainly examples of URLs that convey the meaning of a communication. As noted earlier, by virtue of the operation of certain web forms, URLs can sometimes incorporate search terms or other information that a user wishes to remain private. For example, a search of an online bookstore for books on "breast cancer" may generate a page of search results identified by a URL that contains those search terms.[146] Even some URLs, without more, supply information on what the rest of a web page contains, and

143. *See supra* notes 33, 65 and accompanying text.
144. *See supra* notes 65-75 and accompanying text.
145. 18 U.S.C. § 2510(8) (2000).
146. *See supra* note 75 and accompanying text.

thus give information on the "substance, purport, or meaning" of a communication.[147]

Although there are powerful arguments that at least some URLs convey "contents" of a communication, an important impediment to courts' proper resolution of that issue still exists. As with many other statutory distinctions in electronic surveillance law, there are constitutional underpinnings to the distinctions the Wiretap Act and the pen/trap statute draw between content and non-content information.[148] In a dispute involving the government, a court would carefully apply the canon of constitutional avoidance[149] so as to construe the term "contents" fairly broadly, possibly concluding that URLs contain content. A court facing claims involving only private parties is far less likely to be sensitive to this constitutional backdrop.[150] I return to this issue in Part IV.

4. Summary

As this discussion suggests, there is good reason to be skeptical that the Wiretap Act will successfully curb anything but the most extreme forms of spyware. With respect to keystroke monitors, the fact that such programs or devices can capture communications before they are transmitted over the Internet suggests that, at least under existing case law, no interception occurs. For programs that capture communications as they are being transmitted over the Internet, the issue of consent will be extremely important, particularly if the programs were accompanied by a license agreement explaining their capabilities. Finally, the fact that the Wiretap Act covers only interception of the contents of a communication opens avenues for defendants to argue that certain data does not qualify as contents, and in the context of cases involving private parties, courts may be insensitive to the constitutional boundaries between content and non-content information.

---

147. Of course, one could argue that a URL and the accompanying web page are distinct electronic communications. The statute appears to treat as "contents" only information concerning the substance, purport, or meaning of the *communication in question*—for example, the URL—not information concerning the substance, purport, or meaning of *other communications*—for example, the web page.

148. For further discussion, see Bellia, *supra* note 22, at 1428-30.

149. *See, e.g.*, Jones v. United States, 526 U.S. 227, 239 (1999).

150. I discuss below the ways in which surveillance law's coverage of both government and private conduct can act as a double-edged sword. *See infra* notes 188-189, 294-298 and accompanying text.

C. The Stored Communications Act

The previous section explored the application of the Wiretap Act's prohibition on interception of electronic communications to various forms of spyware. Despite the intuitive characterization of spyware as a tool for intercepting communications, several interpretive issues complicate the analysis. The fit between spyware and the SCA is far less intuitive, but the statute is still likely to be invoked in efforts to curb spyware. Parties objecting to privacy-invasive practices with respect to electronic communications frequently tack SCA claims onto Wiretap Act claims.

Despite the frequency with which the SCA is invoked in privacy disputes, the statute protects an extremely narrow category of communications. As a result, it is unlikely to be of real benefit to plaintiffs objecting to most forms of spyware. To be sure, existing case law seems to leave open broader interpretations of the SCA. I return to that case law in Part IV to illustrate its flaws. For now, I focus on the SCA's text and legislative history.

1. The "Facility" Problem

Recall that the SCA prohibits one from gaining unauthorized access to a "facility through which an electronic communication service is provided," and thereby "obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in storage in such system."[151] A threshold requirement for any SCA claim, then, is a demonstration that a defendant gained unauthorized access to a "facility" through which an electronic communication service is provided.

Drawing upon the SCA's language and ECPA's legislative history, it is possible to identify some obvious examples of unauthorized access to a facility of an electronic communication service. The mail server of a service provider such as America Online would certainly qualify: the e-mail service is the "electronic communication service," insofar as it provides "users thereof the ability to send or receive wire or electronic communications,"[152] and AOL's mail server is the "facility" through which that service is provided. Were someone to hack into AOL's mail servers and obtain communications stored on AOL's servers and awaiting retrieval by a subscriber, the SCA would certainly cover the conduct. A similar example with respect to wire communications would be the system of a voicemail provider. Were someone to gain unauthorized access to the voicemail system and then obtain a wire communication, the predicate for § 2701(a)

151. 18 U.S.C. § 2701(a) (2000).
152. *Id.* § 2510(15).

would be met.

These examples are quite consistent with ECPA's legislative history. As the ECPA hearings indicate, much of the impetus for § 2701(a) of the SCA was that industry representatives feared that users would be deterred from using new communications systems if communications stored within those systems were unprotected.[153] Section 2701(a) was not designed as a general hacking statute; in fact, Congress was careful to limit the overlap between ECPA and computer crime amendments under consideration in 1986.[154] It did so by limiting the SCA's reach to communications within the facility of a provider of an electronic communication service.

Once we move beyond the servers of e-mail and voicemail providers, § 2701(a) becomes more difficult to apply. Cases presenting challenges to third-party advertisers' use of cookies provide a ready example. The SCA claims in those cases appeared to be premised on the view that the "facility" to which the third-party had gained access was the user's hard drive, by implanting the cookie. I discuss the problems with that approach in Part IV; for now, it is sufficient to recognize that a similar claim would have to be made with respect to spyware. The software that acquires a user's data or communications would be located on the user's hard drive; if § 2701(a) covers the installation of that software, it can only be because the facility to which the defendant gained unauthorized access is the plaintiff's computer. Section 2701(a) is thus unlikely to apply at all unless the facility requirement is broadly interpreted to cover an end-user's computer.

2. The "Authorization" and "Consent" Problems

Even if an end-user's computer is appropriately viewed as a "facility through which an electronic communication service is provided," other impediments to application of the SCA exist. To trigger the statute, a defendant's access to a protected facility must be unauthorized, whether "access without authorization" or "exceeding authorized access."[155] In addition, the SCA exempts from its prohibition conduct undertaken with the consent of a "user [of an electronic communication service] with respect

153. *See supra* notes 41-42 and accompanying text.

154. The overlap between computer crime statutes and ECPA was the subject of much discussion throughout the ECPA hearings. *See, e.g.*, *Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights and Trademarks, S. Comm. on the Judiciary*, 99th Cong., 1st Sess. 94-95 (1987); *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice, H. Comm. on the Judiciary*, 99th Cong., 1st Sess. 22-23 (1986).

155. 18 U.S.C. § 2701(a) (2000).

to a communication of or intended for that user."[156]

Here, the issues are similar to those discussed above with respect to the Wiretap Act. The terms "access without authorization," "exceed[ing] authorized access," and "consent" are undefined. In the cookie cases, courts disposed of SCA claims in much the same way as Wiretap Act claims: by concluding that the websites affiliated with the third-party advertisers were parties to the communications and consented to their acquisition.[157] For software products installed following presentation of a license agreement, a defendant is quite likely to claim that the agreement adequately revealed that the software would, in the ordinary course of its operations, obtain a user's Internet communications. As in the case of Wiretap Act claims, such a defense may well be successful.[158]

3. The "Electronic Storage" Problem

One final issue is worth mentioning. The SCA requires a showing that a defendant obtained, altered, or prevented authorized access to a communication "while . . . in electronic storage" in a facility through which an electronic communication service is provided. This portion of the SCA obviously raises questions similar to the "facility" issue discussed above, since it seems unlikely that communications stored on a user's hard drive are properly viewed as stored in a facility through which an electronic communication service is provided. Even if the term "facility" were construed to cover an end-user's computer, it is not clear what communications on that computer would meet the technical definition of "electronic storage."

The SCA incorporates the definition of "electronic storage" that appears in the Wiretap Act.[159] Under the Wiretap Act, electronic storage includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[160] With respect to the SCA's provisions governing law enforcement access to stored communications, where the term "electronic storage" also appears,[161] the Department of Justice has argued for a narrow interpretation: to encom-

156. *Id.* § 2701(c)(2).
157. *See infra* note 245 and accompanying text.
158. *See supra* notes 120-142 and accompanying text.
159. 18 U.S.C. § 2711(1) (2000).
160. 18 U.S.C. § 2510(17) (2000 & Supp. II 2002).
161. *See* 18 U.S.C. § 2703(a) (Supp. II 2002).

pass only communications not yet retrieved by a subscriber.[162] The Justice Department bases its approach both on the definition of "electronic storage" and on the overall structure of the SCA. In terms of the definition, as long as a user has not yet retrieved a communication, a service provider's storage of it is "temporary," "intermediate," and "incidental" to its transmission. Once the user retrieves the communication, any further storage by the service provider (as, for example, when the user does not delete the communication) ceases to be "temporary" or "intermediate." Nor is such a communication stored by the provider for purposes of backup protection.[163] In terms of the structure of the SCA, the Justice Department has essentially argued that the statute's distinct treatment of providers of electronic communication services and providers of remote computing services can only be understood if electronic storage is narrowly construed.[164] In particular, once a subscriber retrieves a communication and chooses to retain it on the provider's system, the communication is no longer held in electronic storage by the provider of an electronic communication service; instead, it becomes one "held or maintained" by the provider of a remote computing service "for the purpose of providing storage . . . services" to the subscriber.[165]

I have extensively discussed this interpretation—and its limitations and implications for the SCA's government access provisions—elsewhere.[166] Here, it is sufficient to note that a fairly narrow interpretation of "electronic storage" has prevailed in various contexts.[167]

4. Summary

In sum, the SCA raises a number of difficult interpretive issues that will likely limit its application to spyware. Because keystroke monitors involve ongoing acquisition of data, they are unlikely to implicate the

---

162. *See, e.g.*, CCIPS MANUAL, *supra* note 54, at 88-89.

163. On this point, the Court of Appeals for the Ninth Circuit has concluded otherwise. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1076-77 (9th Cir. 2004). I discuss that case below. *See infra* notes 254-274 and accompanying text.

164. *See* CCIPS MANUAL, *supra* note 54, at 84-89.

165. *See* 18 U.S.C. § 2703(b)(2) (2000 & Supp. II 2002).

166. *See* Bellia, *supra* note 22, at 1416-26.

167. *See, e.g.*, In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (electronic storage occurs only "when an electronic communication service temporarily stores a communication while waiting to deliver it"); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) ("Retrieval of a message from post-transmission storage is not covered by the Stored Communications Act. The Act provides protection only for messages while they are in the course of transmission."), *aff'd on other grounds*, 352 F.3d 107 (3d Cir. 2003). *But see Theofel v. Farey-Jones*, 359 F.3d at 1076-77; *infra* notes 254-274 (discussing *Theofel*).

SCA at all. With respect to software designed to generate targeted advertising, the proprietary nature of the software makes it difficult to determine whether the products are operating in such a way as to collect temporarily stored communications. Moreover, the SCA was not designed as a general hacking statute to protect the computers of network end-users. Rather, the statute was designed to protect storage systems of service providers. In other words, the SCA is a narrow statute designed to protect communications at a certain point in the communications process.

In discussing the application of the SCA to spyware, I do not intend to suggest that a court would lack room to interpret the SCA broadly to encompass some objectionable conduct. I have already alluded to the fact that electronic surveillance law generally, and the SCA in particular, is somewhat unstable and not predictably applied by courts. More specifically, courts have tended to push the envelope in terms of applying the SCA to certain troubling privacy-invasive practices. In the case of the SCA, however, many judicial approaches simply cannot be justified under any appropriate canons of statutory construction. In limiting my discussion of such cases in my predictive analysis, I do not intend to overlook them. As discussed in Part IV, I am simply skeptical that such broad interpretations of the SCA will have any significant privacy benefits.

D. Conclusion

In sum, electronic surveillance statutes, by their terms, do not operate to regulate spyware activities in any comprehensive way.[168] Surveillance

168. I have not discussed another alternative for challenging spyware practices: the CFAA, 18 U.S.C. § 1030 (2000 & Supp. II 2002). The statute is not truly a surveillance statute, and a full discussion of it is therefore beyond the scope of this Article. It is nevertheless interesting to note something of a paradox: that despite the fact that the CFAA and related doctrines are mainly designed to respond to concerns about computer security rather than concerns about privacy, plaintiffs are more likely to have success pursuing spyware-related claims under the CFAA and analogous state law doctrines than they are under surveillance law statutes.

The most relevant provision of the CFAA is § 1030(a)(2), which prohibits one from "intentionally access[ing] a protected computer without authorization or exceed[ing] authorized access and thereby obtain[ing] . . . information from any protected computer if the conduct involved an interstate or foreign communication." *Id.* § 1030(a)(2). Because the CFAA requires a showing that any access to a computer was without authorization or exceeded authorized access, it raises a consent or authorization similar to the Wiretap Act and the SCA. *See supra* Parts II.B.2, II.C.2. But where a plaintiff can overcome the authorization problem—as, for example, when a defendant's installation of spyware was truly surreptitious—a CFAA claim in theory would be more likely to succeed than a Wiretap Act claim or an SCA claim. A plaintiff would not need to show for purposes of the Wiretap Act that communications were acquired contemporaneously with their transmission and not when purely internal to the computer system; and a plain-

law will combat only narrow categories of spyware: perhaps keystroke monitors, but only if courts can move past the problem of applying the "electronic communication" definition to data purely internal to a computer; and perhaps certain software designed to generate targeted advertising, but only if such software was installed surreptitiously or if a court finds that the user's consent was otherwise deficient.

The spyware story is not an unusual one. In a wide variety of contexts, plaintiffs have invoked electronic surveillance statutes in an attempt to curb certain privacy-invasive practices involving electronic communications. The next Part explores *why* surveillance law statutes have been and are likely to remain of marginal value in responding to a range of digital-age privacy threats.

IV. SURVEILLANCE LAW'S LIMITS

The discussion in Part III illustrates significant problems with applying

---

tiff would not need to show for purposes of the SCA that the defendant gained access to a "facility through which an electronic communication service is provided" or that the communications acquired were in "electronic storage."

A civil litigant will nevertheless face one significant obstacle under the CFAA: that of meeting the statute's $5000 threshold for economic damages. *See* 18 U.S.C. § 1030(g) (creating civil cause of action but specifying that underlying conduct must involve one of five "factors" set forth in § 1030(a)(5)(B)); *id.* § 1030(a)(5)(B)(i) (requiring, except with respect to action brought by government, a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5000 in value"). Of course, an impediment such as a $5000 loss threshold is a purely technical one that could be overcome by a legislative change. Moreover, the $5000 threshold does not leave a plaintiff entirely without a remedy: it simply reserves federal court involvement for the most serious claims, while funneling less significant claims into statute courts under analogous state statutes or common-law trespass to chattels claims.

This possibility that plaintiffs challenging spyware practices will be more successful with CFAA claims or analogous state law claims raises something of a paradox with respect to the spyware problem. What tends to make the forms of spyware discussed here objectionable is not merely the fact that in some cases the device or software is surreptitiously installed, but rather that spyware tools can acquire vast amounts of private information. It is that fact that at first blush seems to make surveillance law an attractive avenue to pursue. Statutes such as the CFAA and state law analogues can reasonably respond to issues of surreptitious installation, but they address the privacy concerns only incidentally—for the CFAA, by virtue of § 1030(a)(2)'s prohibition on gathering "information," and for common law trespass, only because the acquisition of private information may constitute a cognizable harm. In other words, even where significant privacy-invasive practices are at issue, a statute such as the CFAA—designed not to protect privacy but to guarantee security—seems to be a better conceptual fit than surveillance law statutes. The next Part considers why it is that surveillance law statutes respond so poorly to digital privacy threats.

surveillance law statutes to spyware. Two questions follow. First, *why* do surveillance law statutes respond so poorly, despite the privacy implications of spyware? Second, *could* surveillance law provide a more useful framework if more aggressively interpreted by the courts?

In exploring these questions, it is helpful to place the spyware problem in the broader context of efforts to use electronic surveillance law to address digital-age privacy challenges. As I will show, the spyware story is not unique. Litigants and commentators frequently assume that surveillance statutes provide appropriate vehicles for responding to such perceived privacy threats as online profiling and employer monitoring of communications, but such claims rarely succeed. The cases in which they do succeed involve unusual facts that are not generalizable across a broad class of cases. Although I do not address the merits of the disputed practices, I explain in Section A why efforts to enhance digital privacy through litigation have largely failed.

I then turn in the remainder of this Part to the normative question of whether courts should more aggressively interpret surveillance statutes to provide broader privacy-protective functions, at least in disputes involving private parties. In other words, if we agree that certain spyware practices (or other disputed practices involving electronic communications) should be curbed, is electronic surveillance law an appropriate vehicle for doing so—particularly since courts have managed to arrive at privacy-protective outcomes in some instances? I argue that aggressive judicial interpretations of surveillance statutes have failed to achieve lasting privacy benefits. In Section B, I offer three examples of courts' attempts to adopt privacy-protective interpretations in cases involving rather bad facts. As the examples illustrate, such interpretations can do considerable violence to the statutory text or legislative intent. Moreover, as Section C demonstrates, privacy-protective outcomes have a way of unraveling, perhaps as a result of the cases' vulnerability to criticism on statutory interpretation grounds. For each case involving a privacy-protective result, one can identify or predict a privacy-destructive response. Finally, in Section D, I show how decisions that reach privacy-protective results, despite textual and other impediments, can derail legislative momentum by giving the impression that only minor, piecemeal statutory changes are necessary to address problems that in fact should be the subject of far broader reforms.

A. The Spyware Problem in Context

The challenges of applying surveillance law to spyware are not unique. Litigants and commentators have increasingly invoked electronic surveillance statutes in an effort to curb perceived privacy-invasive practices in-

volving electronic communications. Such efforts usually encounter the same impediments as discussed in Part III. Attempts to use surveillance law to challenge employer monitoring of communications or to challenge online profiling activities provide useful examples. With respect to claims that employer monitoring violates surveillance statutes, the employer's efforts to acquire the employee's consent to the monitoring will typically defeat any Wiretap Act claim, even if communications are monitored during the transmission phase. SCA claims typically fail because the employer acts as a service provider and thus could "authorize" the conduct in question. I have already discussed some aspects of the online profiling cases—that is, cases involving third-party advertisers' use of cookies to gather data across a range of websites. As noted, both Wiretap Act and SCA claims have typically foundered on the consent element.[169]

In observing that efforts to use litigation to improve privacy practices with respect to electronic communications have generally been unsuccessful, I do not intend to suggest that privacy-protective outcomes do not exist—or, for that matter, that decisions rejecting Wiretap Act or SCA claims are incorrect. In cases involving particularly bad facts, courts have on occasion allowed surveillance law claims to proceed. With respect to employer monitoring, the case of *Konop v. Hawaiian Airlines, Inc.*,[170] which involved a supervisor gaining access to an employee's password-protected website, comes to mind. In that case, the Court of Appeals for the Ninth Circuit rejected a Wiretap Act claim but allowed an SCA claim to proceed past the summary judgment phase.[171] The unique facts of the case—including that the employer did not act as a service provider with respect to the communications in question—make the case sufficiently narrow that it is unlikely to influence subsequent decisions involving more conventional facts. Moreover, as noted below, the *Konop* case itself involves a highly questionable application of the SCA.[172] With respect to the use of cookies, the *Pharmatrak* decision reflects one instance in which a court allowed a Wiretap Act claim to proceed even though the companies whose websites facilitated Pharmatrak's placement of cookies on users' computers arranged for Pharmatrak's services.[173] In addition, even the

169. *See supra* notes 124-133 and accompanying text; *see also infra* note 245 and accompanying text.

170. 302 F.3d 868 (9th Cir. 2002).

171. As discussed below, the court initially allowed the Wiretap Act claim to proceed but abandoned its analysis following a petition for rehearing. *See infra* notes 277-293 and accompanying text.

172. *See infra* note 293.

173. *See supra* notes 134-141 and accompanying text.

cookie cases preceding *Pharmatrak* are interesting in that they rely on consent as the basis for dismissal, when the plaintiffs' claims could potentially have foundered on a number of other grounds (a point to which I return below). The next Section discusses several other cases in which courts faced with bad facts have attempted to draw certain privacy-invasive conduct within the domain of surveillance law.

For our purposes, the interesting question is whether those cases involving *unsuccessful* challenges to privacy-invasive conduct are the result of reasonable application of statutes that are simply too narrow to reach the challenged conduct or the result of misinterpretation. After reading many of the cases that attempt to apply surveillance statutes, particularly to private conduct, one might conclude that cases rejecting surveillance law claims simply reflect confused application of very complex statutes. Courts routinely report substantial confusion concerning how to apply surveillance statutes,[174] particularly with respect to some of the issues discussed earlier in this Article—such as how to draw the line between the Wiretap Act and the SCA[175] and what it means for a communication to be in electronic storage.[176]

My own view, however, is that the failure of electronic surveillance law to curb or reform seemingly privacy-invasive practices is mainly attributable to the problem of narrow drafting rather than the problem of misinterpretation. In particular, ECPA pre-dates the development of our electronic communications infrastructure.[177] Certain electronic communication services existed in 1986, and Congress recognized that such services were unlikely to be widely used unless it provided some statutory protection for electronic communications.[178] The technical aspects involved in the transmission of a communication were largely the same as

---

174. *See, e.g.*, Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (calling Wiretap Act "famous (if not infamous) for its lack of clarity"); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (suggesting that *Steve Jackson Games* court "might have put the matter too mildly"); *Konop*, 302 F.3d at 874 ("Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.").

175. *See supra* note 34 and accompanying text; *infra* notes 183-189, 281-293 and accompanying text.

176. *See supra* notes 162-167 and accompanying text; *infra* notes 254-274 and accompanying text.

177. *See, e.g.*, *Konop*, 302 F.3d at 874 (noting that complexity of surveillance law "is compounded by the fact that ECPA was written prior to the advent of the Internet and the World Wide Web" and that "the existing statutory framework is ill-suited to address modern forms of communication").

178. *See supra* note 41 and accompanying text.

they are today, in that messages were stored regularly as part of the transmission process.[179] In addition, it was not uncommon for businesses to contract for off-site computer storage or processing services; Congress thus also understood the need to protect such remotely stored files.[180] But the Internet as we know it did not exist in 1986. Congress simply did not envision how concepts such as "electronic communication," "electronic communication service," "facility," and "electronic storage" would map onto the Internet.

One example will suffice to illustrate how the concepts reflected in the Wiretap Act and the SCA are difficult to map onto the Internet more broadly. Under the Wiretap Act, acquisition of communications with the consent of one party are not considered unlawful interceptions;[181] similarly, conduct undertaken with the consent of a user of an electronic communication service will not run afoul of the SCA.[182] A consent exception under the original version of the Wiretap Act may have been quite sensible, in that any wire or oral communication likely would have involved a relatively small number of parties, with respect to whom the speaker could gauge the risk that the conversation would be recorded or revealed. The extension of the concept to electronic communications is similarly understandable when a relatively small number of parties are involved. The concept of one-party consent, however, becomes meaningless when applied not to personal communications, but to arms'-length transactions—where a user does not or cannot know of the contractual arrangements the other party may have with third parties and therefore lacks the data to gauge the privacy risks involved.

But even if courts could adequately address issues of consent and map other statutory terms onto the Internet, a more fundamental problem exists: our surveillance law statutes, as written, simply are not general data privacy statutes. In other words, the statutes do not broadly identify a particular category of personal data that should be subject to protection or restrict the acquisition, use, or transfer of such data. The Wiretap Act deals narrowly with *communications* that are *transmitted*, not with any other

179. *See, e.g.*, Brief on Rehearing En Banc of *Amicus Curiae* Technical Experts In Support of Appellant, Urging Reversal, United States v. Councilman 6-8 (1st Cir. Nov. 12, 2004) (No. 03-1383), *available at* http://www.epic.org/privacy/councilman/tech_amicus.pdf (noting that technical specifications for e-mail were developed prior to ECPA's passage in 1986).

180. *See* S. REP. NO. 99-541, at 10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3564.

181. 18 U.S.C. § 2511(2)(c), (d) (2000).

182. *Id.* § 2701(c)(2).

data that an individual might attempt to shield or any other process by which it might be revealed. The SCA protects only communications, and only at a very specific point in the communications process: in electronic storage in the system of an electronic communications service.

That is not to say that all cases rejecting Wiretap Act or SCA claims are properly decided. For example, the U.S. Court of Appeals for the First Circuit, sitting *en banc*, recently reversed a highly problematic decision dismissing a Wiretap Act claim. In *United States v. Councilman*,[183] a district court considered whether an Internet service provider that captured communications of its customers before transmitting them into users' mailboxes had intercepted those communications. The communications were acquired during a brief period of storage in the ISP's system before transmission to the user's mailbox.[184] Because the communications were acquired during this brief period of storage, the district court concluded that the communications were not intercepted for purposes of the Wiretap Act.[185] A panel of the Court of Appeals for the First Circuit affirmed on the same reasoning.[186]

Although several courts construing the Wiretap Act had held that the statute does not protect stored communications,[187] those cases differed from *Councilman* in an important respect. The previous cases each involved a *one-time acquisition* of communications maintained by a service provider *for retrieval by the subscriber*. *Councilman*, in contrast, involved an *ongoing acquisition* of communications briefly stored during the transmission process *prior to being made available to the subscriber*. The implications of the district court's and panel majority's conclusion for electronic communications were profound. By virtue of the architecture of the Internet, electronic communications are stored at numerous points during transmission. Under the district court's and panel majority's reasoning, a communication would move in and out of the Wiretap Act's protective umbrella depending upon whether, at a given moment in time, the communication was between or within the computers relaying it.

The *en banc* court's reversal of the *Councilman* decision was thus a welcome result. The case nevertheless highlights one of the real difficul-

183. 245 F. Supp. 2d 319 (D. Mass. 2003) [hereinafter *Councilman I*], *aff'd*, 373 F.3d 197 (1st Cir.) [hereinafter *Councilman II*], *reh'g en banc granted and opinion withdrawn*, 385 F.3d 793 (1st Cir. 2004), *on reh'g en banc*, No. 03-1383, 2005 U.S. App. LEXIS 16803 (1st Cir. Aug. 11, 2005).

184. *Councilman II*, 373 F.3d at 199.

185. *Councilman I*, 245 F. Supp. 2d at 321.

186. *Councilman II*, 373 F.3d at 204.

187. *See supra* note 34 (citing cases).

ties in applying surveillance law to private conduct. I discussed in Part II the fact that understanding the Fourth Amendment backdrop to each statute is crucial to applying the relevant terminology. This point is often missed by courts construing the statutes in cases involving civil or criminal actions against private parties rather than in the context of a motion to suppress evidence gathered by the government.[188] In *Councilman*, the district court's and panel majority's conclusion that a service provider can acquire the contents of a communication prior to completion of the transmission phase, merely because it is stored at a point in the transmission process, would have dramatically expanded the government's access to electronic communications: the government could have relied on the less stringent procedures of the SCA to compel production of a communication at any one of a number of points along its transmission path, rather than obtaining a Title III order.[189] Had the courts fully considered that fact, it seems unlikely that they would have reached the same result. Courts applying statutes to private conduct in isolation, without attention to the manner in which interpretations affect government conduct, are likely to apply surveillance statutes erroneously. Those errors, of course, can run in either direction: sanctioning privacy-invasive conduct by private parties, thereby opening avenues for the government to engage in the same conduct, and limiting privacy-invasive conduct, thereby constraining investigative tools available to the government.

Even if we accept that interpretation of surveillance statutes is difficult, and that some cases rejecting Wiretap Act or SCA claims are erroneous, the fact remains that surveillance law statutes are very narrowly drafted, and that much privacy-invasive conduct with respect to electronic communications remains outside of their terms.[190] That observation begs

188. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HAST. L.J. 805, 807 (2003) ("[C]ourts have not explained how the complex web of surveillance statutes apply in routine criminal cases, but instead have interpreted those statutes in unexpected civil contexts where the implications of the court's decision for the bulk of criminal cases tends to be unknown to the court and ignored by the parties.").

189. *See, e.g.*, Brief on Rehearing *En Banc* for Senator Patrick J. Leahy as *Amicus Curiae* Supporting the United States and Urging Reversal, United States v. Councilman 10-11 (1st Cir. Nov. 12, 2004) (No. 03-1383), *available* at http://www.cdt.org /wiretap/20041112leahy.pdf; Supplemental Brief of Center for Democracy and Technology et al., United States v. Councilman 1-4 (1st Cir. Nov. 12, 2004) (No. 03-1383), *available at* http://www.cdt.org/wiretap/20041112joint.pdf.

190. For another view that surveillance statutes are narrowly drafted and that courts erroneously apply them to a range of conduct, see Kerr, *supra* note 188, at 807 (arguing that surveillance law "remains unusually obscure, and the rare judicial decisions construing the statutes tend to confuse the issues, not clarify them").

the question of whether courts should more aggressively interpret surveillance statutes to provide broader privacy-protective functions, at least in cases involving private parties. The remainder of this Part explores that question. I argue that aggressive interpretations of surveillance statutes are unlikely to achieve lasting privacy benefits. Although one could offer a range of examples of privacy-protective but deeply flawed applications of surveillance law, I focus on three examples in particular: *United States v. Smith*,[191] *In re Pharmatrak Privacy Litigation*[192] (and its antecedents), and *Theofel v. Farey-Jones*.[193] I begin by explaining the difficulties each case presents as a matter of statutory interpretation; I then explore the broader consequences of the courts' approaches for privacy and for legislative momentum.

B. Deconstructing Courts' "Privacy-Protective" Approaches

1. United States v. Smith

United States v. Smith dealt with a frequently litigated and extremely complex issue: how the Wiretap Act's prohibition on interception of communications relates to the SCA's prohibition on acquisition of communications in electronic storage.[194] Although the case concerned wire communications rather than electronic communications, the implications of the decision for electronic communications were potentially quite significant. The Court of Appeals for the Ninth Circuit ultimately concluded that a private party could "intercept" a voicemail message even when the message was acquired from electronic storage within the voicemail provider's system.[195] The court's effort to reconcile its interpretation of the Wiretap Act with the existence of the SCA, however, resulted in an extremely confused interpretation of both statutes.

In *Smith*, a third party acquired the contents of a voicemail message by guessing a co-worker's password;[196] the message revealed possible insider trading.[197] Section 2511 prohibits the interception of a wire communication, whereas § 2701(a) of the SCA creates civil and criminal liability for one who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby

191. 155 F.3d 1051 (9th Cir. 1998).
192. 329 F.3d 9 (1st Cir. 2003).
193. 341 F.3d 978 (9th Cir. 2003), *reh'g denied and opinion superseded*, 359 F.3d 1066 (9th Cir. 2004).
194. *Smith*, 155 F.3d at 1055.
195. *Id.* at 1059.
196. *Id.* at 1054.
197. *Id.* at 1053.

obtains . . . a wire . . . communication while it is in electronic storage in such system."[198] The determination of which statute governs the acquisition of a voicemail message by a private party is important, because § 2515 of the Wiretap Act requires exclusion of any wire or oral communication that has been illegally intercepted,[199] whereas the SCA lacks such an exclusionary rule.[200] In a criminal trial on the insider trading charges, the district court suppressed a tape of the voicemail message on the theory that it had been intercepted.[201] The district court declined to suppress other evidence despite the defendant's claim that it was derived from the illegally intercepted voicemail message.[202]

When the defendant challenged this ruling on appeal of his conviction, the government argued that the district court was correct to rule that the evidence was not derived from the voicemail message.[203] As an alternative basis for affirmance, the government also argued that the voicemail message was not in fact intercepted within the meaning of the Wiretap Act. Rather, the government suggested, the third party's retrieval of the voicemail message violated only § 2701(a) of the SCA; thus, any evidence derived from the acquisition did not need to be suppressed. In other words, the government argued that § 2511 covers acquisition of a communication only while it is being transmitted, while § 2701(a) covers acquisition of a communication once it is in storage.[204]

Although the court ultimately concluded that the evidence in question was not derived from the voicemail message,[205] it treated the government's claim that the SCA, and not the Wiretap Act, governed the case as a "threshold issue."[206] The court rejected the government's transmission/storage distinction and concluded that a private party could "intercept" a stored voicemail message.[207] The court acknowledged that the government's narrower interpretation of the Wiretap Act comported with the ordinary meaning of the term "intercept"—"'to take, seize, or stop by the way or *before arrival at the destined place*'"—but concluded that this

198. 18 U.S.C. § 2701(a)(1) (2000).

199. 18 U.S.C. § 2515 (2000).

200. The SCA allows for civil damages and criminal penalties and deems those remedies exclusive. *See* 18 U.S.C. § 2707 (2000 & Supp. II 2002) (civil action); *id.* § 2701(b) (criminal penalties); *id.* § 2708 (exclusivity of remedies).

201. *Smith*, 155 F.3d at 1054.

202. *Id.*

203. *Id.* at 1055.

204. *Id.* at 1056-57.

205. *Id.* at 1063.

206. *Id.* at 1055.

207. *Id.* at 1059.

ordinary meaning did not control.[208] The court's reasoning rested in part on a feature of the Wiretap Act that was later eliminated (subject to a sunset provision) in the USA Patriot Act. In particular, § 2510(1) had defined the term "wire communication" to cover "any electronic storage of such communication"[209]; the USA Patriot Act temporarily excised this portion of the definition.[210]

The court's approach suffers from numerous flaws. First, if acquisition of a voicemail message from electronic storage is an interception, then § 2701(a)'s coverage of the acquisition of wire communications from electronic storage is redundant or nonsensical. The court attempted to deflect this argument by reasoning that the Wiretap Act and the SCA cover two different things: the Wiretap Act prohibits acquiring the contents of the communication, whether the communication is in transit or in storage, whereas the SCA prohibits gaining "access" to a communication—with "access" understood to mean conduct that puts a person "*in position to acquire* the contents of a communication."[211] In other words, under the *Smith* court's reasoning, the Wiretap Act covers the acquisition of the communication, whereas the SCA covers preliminary conduct placing one in position to acquire a communication. There are significant problems with this approach. First, in reaching its conclusion, the court conflated two different uses of the word "access" in § 2701(a) and altered the grammatical structure of the prohibition. Section 2701(a) covers one who "intentionally accesses" a "facility" through which an electronic communication service is provided. Drawing on this language, the court observed that the Wiretap Act refers "pointedly" to intercepting a particular communication, while § 2701 refers "broadly" to accessing a communications facility.[212] The court reasoned that "[o]ne assuredly can access a communications facility—such as a company voicemail system—without listening to or recording any of the messages stored within that facility."[213] The court implied that such conduct, without more, would violate the SCA.[214] Section 2701(a), however, requires more than gaining access to a covered facility: one must also "obtain[], alter[], or prevent[] authorized access to a wire or

208. *Id.* at 1057 (quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1176 (1986)) (emphasis in opinion).

209. 18 U.S.C. § 2510(1) (2000).

210. *See* Pub. L. No. 107-56, § 209(1), 115 Stat. at 283 (codified at 18 U.S.C. § 2510(1) (Supp. II 2002)); *id.* § 224, 115 Stat. at 295 (applying sunset provision to § 209).

211. *Smith*, 155 F.3d at 1058 (emphasis added).

212. *Id.* at 1059.

213. *Id.*

214. *Id.*

electronic communication while it is in electronic storage in such system." In other words, the conclusion that merely being in a position to acquire the contents of a communication violates the SCA requires excising the last portion of the prohibition, and focusing on "access[] to a facility" as the sole prohibited conduct.

The court also looked to the second appearance of the word "access" in § 2701(a) and concluded that to "obtain[] . . . access" is to be in a position to acquire its contents, not to actually acquire those contents. Even if that were an appropriate reading of the phrase "obtain[] . . . access," one must alter the grammatical structure of the prohibition to conclude that "obtain[] . . . access" is the operative phrase in the statute. As noted, Section 2701(a) reaches "whoever . . . intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby *obtains, alters,* or *prevents authorized access* to a wire or electronic communication while it is in electronic storage."[215] In reading the provision to prohibit one from "obtain[ing] . . . access" to a communication, however, the court assumes that "access" is the direct object of the verb "obtains." Under this approach, the statute reaches one who "obtains . . . access to a wire or electronic communication," "alters . . . access to a wire or electronic communication," or "prevents authorized access to a wire or electronic communication." The phrase "alters . . . access" is awkward; the more natural reading of the prohibition is that it reaches one who "obtains . . . a wire or electronic communication," "alters . . . a wire or electronic communication," or "prevents authorized access to a wire or electronic communication." When so read, the prohibition does not in fact cover gaining access to a facility and thereby "obtain[ing] . . . access" to a communication in electronic storage. Rather, it covers gaining access to a facility and thereby "obtain[ing] . . . a communication" in electronic storage. The court's conclusion that the SCA covers only conduct that places one in a position to obtain the contents of a communication is thus flawed. The court's interpretation of the Wiretap Act does render the SCA, properly read, redundant, because both statutes would cover acquisition of a stored wire communication.

The *Smith* court also buttressed its conclusion by focusing on the definition of "wire communication" under the Wiretap Act.[216] Prior to the passage of the USA Patriot Act, § 2510(1) defined a wire communication to include storage of such a communication. The *Smith* court reasoned that the inclusion of that phrase would be rendered meaningless if stored wire

215. 18 U.S.C. § 2701(a) (2000).
216. *Smith*, 155 F.3d at 1058.

communications could not be intercepted.[217] Here, the court ignored the most likely explanation for the reference to stored wire communications in § 2510(1). Prior to the passage of the USA Patriot Act, the SCA in fact required the *government* to seek a Title III order before acquiring the contents of any wire communication in electronic storage. Section 2701(a) prohibits the acquisition of wire or electronic communications in electronic storage, but § 2701(c)(3) exempts authorized government conduct—specifically, prior to the Patriot Act's passage, conduct authorized under §§ 2703 and 2704 of ECPA and under § 2518 of the Wiretap Act.[218] Prior to the passage of the USA Patriot Act, and when *Smith* was decided, the first two of these provisions described only how the government may compel a service provider to produce or preserve the contents of stored *electronic* communications: subsections (a) and (b) of § 2703 established the means by which law enforcement officials could require a service provider to disclose the contents of electronic communications,[219] while § 2704 authorized the government to require a service provider to create a backup copy of the contents of electronic communications pending resolution of any proceedings concerning the government's subpoena or court order.[220] Because both § 2703 and § 2704 omitted reference to any process by which the government could obtain or compel production of the contents of stored *wire* communications,[221] the reference in § 2701(c) to § 2518—the provision of the Wiretap Act under which a court grants an order authorizing law enforcement conduct—could only relate to government access to stored *wire* communications.

Accordingly, at the time *Smith* was decided, if the government wished to acquire wire communications in electronic storage without violating § 2701(a), it had to obtain a Title III order.[222] The report of the House Committee on the Judiciary accompanying ECPA confirms this reading of the statute. The analysis of § 2703, which, as noted, then governed access to the contents of electronic communications in electronic storage, states:

---

217. *See id.* at 1058 & n.12.

218. 18 U.S.C. § 2701(c)(3) (2000).

219. *Id.* § 2703(a), (b).

220. *Id.* § 2704.

221. Section 2703(d), which set forth circumstances under which a court may order a service provider to disclose a communication, did refer to "the contents of a wire . . . communication." Since the government could only seek an order under § 2703(d) for disclosure of electronic communications, see *id.* § 2703(b)(1)(B)(ii), and subscriber or customer records, see *id.* § 2703(c)(1)(B), the reference was apparently inadvertent.

222. The USA Patriot Act altered this requirement by adding procedures to compel production of wire communications to §§ 2703(a) and (b). *See* Pub. L. No. 107-56, § 209(2), 115 Stat. at 283 (codified at 18 U.S.C. §§ 2703(a), (b) (Supp. II 2002)).

"The contents of the voice portion of a wire communication in storage such as with 'voice mail' *may not be obtained under this section. [T]he provisions of chapter 119 of title 18 [i.e., the Wiretap Act] apply*."[223] As this discussion suggests, the inclusion of "electronic storage" within the definition of a "wire communication" in the Wiretap Act served only to emphasize the procedure that law enforcement officials had to follow to gain access to voicemail messages. Under this reading, one can conclude that a private party's acquisition of stored communications violates only the SCA and still give effect to the phrase "electronic storage" in the definition of "wire communication."

Finally, in concluding that acquisition of voicemail message constitutes an interception for purposes of the Wiretap Act, the *Smith* court effectively held that the single prohibition on intercepting communications in § 2511(1)(a) would have a different meaning depending on whether wire or electronic communications were at issue. Cases addressing whether acquisition of electronic communications in electronic storage violates not only the SCA but also the Wiretap Act have held that the Wiretap Act only governs the acquisition of communications during transmission.[224] Prior to the passage of the USA Patriot Act, some courts reaching that conclusion relied in part on the inclusion of the phrase "electronic storage" in the definition of a wire communication and the exclusion of that phrase in the definition of an electronic communication.[225] The *Smith* court distinguished those cases on that basis.[226] The effect of the *Smith* decision, however, is that "intercept" is defined differently depending on the type of communication: for wire communications, intercept

223. H.R. Rep. No. 99-647, at 67-68 (emphasis added); *see also* S. Rep. No. 99-541, at 12, *as reprinted in* 1986 U.S.C.C.A.N. at 3566 (noting that amendment to definition of "wire communication" to include "any electronic storage of such communication" was designed "to specify that wire communications in storage like voice mail, remain wire communications, and are protected accordingly"). The House Report's reference to "the voice portion" of a wire communication is somewhat opaque, as a wire communication by definition contains the human voice. The error appears to be a relic of an earlier version of ECPA, in which § 2703(a) applied to government access to "non-voice wire communications." In any event, the Report's statement that Title III applies to stored voice communications is unambiguous.

224. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Wesley Coll. v. Pitts, 974 F. Supp. 375, 388 (D. Del. 1997), *aff'd*, 172 F.3d 861 (3d Cir. 1998); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996); United States v. Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996).

225. *See Steve Jackson Games*, 36 F.3d at 461-62; *Wesley Coll.*, 974 F. Supp. at 386; *Reyes*, 922 F. Supp. at 836.

226. *Smith*, 155 F.3d at 1057.

means the acquisition of a communication in transit or in electronic storage, but for electronic communications, intercept means only the acquisition of a communication in transit. That approach overlooks the fact that, under the Wiretap Act, all communications are encompassed in a single prohibition providing for criminal punishment and a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[227] To assign a different meaning of the term, depending on whether a wire or electronic communication was at issue, would be highly anomalous.[228]

Smith is illustrative of how courts can do violence to statutory text by reading electronic surveillance statutes in privacy-protective ways. Although the *Smith* court ultimately denied the defendant's motion to suppress,[229] the decision was privacy-protective in that the court would have applied the more restrictive provisions of the Wiretap Act to the defendant's conduct. As discussed below, however, *Smith* is among the privacy-protective cases that have in some sense unraveled.

2. In re Pharmatrak, Inc. Privacy Litigation and its Antecedents

In re Pharmatrak, Inc. Privacy Litigation and the "cookie" cases that preceded it provide a second example of courts reading surveillance statutes too broadly. As previously noted, the cases typically involved claims that use of cookies violated the Wiretap Act, the SCA, and the CFAA.[230] *In re Pharmatrak Privacy Litigation*[231] presents a rare example of a case in which a claim that placement of a cookie on a user's hard drive, coupled with other conduct, violated a surveillance law statute was allowed to proceed. In particular, the Court of Appeals for the First Circuit overturned a

---

227. 18 U.S.C. § 2511(1)(a) (2000).

228. The discussion above suggests that the court's textual and structural arguments are unpersuasive. The court also dismissed the Senate and House reports accompanying ECPA because it found the reports' discussions of whether the wiretap provisions or the stored communications provisions govern acquisition of stored communications to be inconsistent: The Senate report suggests that stored wire communications are protected by Title III, while the House report suggests that they are subject to the stored communications access provisions of ECPA. *See Smith*, 155 F.3d at 1056 n.9. The reports, however, can be easily reconciled, on the theory that the Senate report is focusing on *government* access to stored wire communications (which must occur via a Title III order) and the House report is focusing on *non-governmental* access to stored communications (which is regulated by the prohibitions of § 2701(a) of the SCA). *See supra* notes 217-223 and accompanying text.

229. *Smith*, 155 F.3d at 1063.

230. *See supra* notes 123-142 and accompanying text.

231. *Pharmatrak II*, 329 F.3d at 9.

district court's grant of summary judgment to Pharmatrak on a Wiretap Act claim.[232] The court of appeals' reasoning, though privacy-protective, has significant problems. Some of those problems simply build upon problems in prior "cookie" cases. Although most of the cookie cases preceding *Pharmatrak* resulted in summary judgment to the defendant or dismissal, they reflect unusual and unduly broad interpretations of portions of the electronic surveillance statutes.

The first and most important case in the series of cookie cases was *In re DoubleClick Inc. Privacy Litigation*,[233] a class action suit by individuals alleging that DoubleClick's use of cookies resulted in the unauthorized acquisition of personally identifiable information in violation of federal law.[234] Although the court granted DoubleClick's motion to dismiss the Wiretap Act and SCA claims on the ground that DoubleClick's conduct fell within exceptions in each statute for certain consensual conduct,[235] the court assumed, or DoubleClick conceded, that certain substantive predicates for liability with respect to each statute were met.[236] Despite the fact that other portions of the opinion rendered the *DoubleClick* court's conclusion with respect to the substantive predicate for liability dictum, the *DoubleClick* court's framework paved the way for other courts to take a similar approach, with some bizarre consequences.

The premise of the *DoubleClick* plaintiffs' claim that use of cookies violated the Wiretap Act was that DoubleClick had acquired private information when interaction between the plaintiffs' computers and DoubleClick-affiliated websites caused that information to be incorporated into a URL.[237] The plaintiffs claimed that acquisition of the communications constituted an interception.[238] DoubleClick's motion to dismiss rested on the view that any interception was undertaken with the consent

---

232. *See Pharmatrak I*, 220 F. Supp. 2d at 12 (granting summary judgment on Wiretap Act claim), *rev'd*, *Pharmatrak II*, 329 F.3d at 9. The court of appeals remanded for further consideration of whether Pharmatrak's conduct satisfied the intent requirement of the Wiretap Act. On remand, the district court again granted summary judgment to Pharmatrak. 292 F. Supp. 2d 263 (D. Mass. 2003).

233. 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

234. For discussion of the factual basis for the claims, see *supra* notes 127-131 and accompanying text.

235. *DoubleClick*, 154 F. Supp. 2d at 514, 519.

236. *See id.* at 508 ("Assuming the communications are considered to be in 'electronic storage,' it appears that plaintiffs have adequately pled that DoubleClick's conduct constitutes an offense under § 2701(a) . . . ."); *id.* at 514 (noting DoubleClick's concession for purposes of motion to dismiss that its conduct, as pled, violated Wiretap Act's prohibition on interception).

237. *See id.* at 504; *supra* notes 130-131 and accompanying text.

238. *DoubleClick*, 154 F. Supp. 2d at 514.

of a party to the communication—that is, the website for which DoubleClick had arranged to provide advertising. The *DoubleClick* court agreed. The court apparently accepted DoubleClick's concession that the substantive predicates for liability under the Wiretap Act were otherwise met. But note the extremely awkward fit between DoubleClick's conduct and the offense under the statute. Recall that the Wiretap Act prohibits the interception of electronic communications and defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[239] Assuming that the personally identifiable information constitutes the "communication" that was intercepted, it is not clear what "device" DoubleClick used to intercept that communication. The cookie is not itself an intercepting device; the cookie is merely stored on the user's hard drive and communicated to DoubleClick by the user's browser at an appropriate time. DoubleClick may associate information with this cookie in its own database, but the cookie itself does not gather information. To the extent that DoubleClick has access to personally identifiable information, it has access because *the user's browser* and *its client's site* are configured in such a way as to reveal this information. It is difficult to see how this constitutes an interception on DoubleClick's part.[240]

Although the court's ultimate conclusion that the DoubleClick-affiliated sites did consent to any interception meant that the court's apparent assumption that the substantive predicate for liability under the Wiretap Act was met was of little consequence in *DoubleClick* itself, that assumption essentially hardened into law in the court of appeals decision in *Pharmatrak*. Recall that Pharmatrak tracked certain data for several pharmaceutical company clients through the use of cookies.[241] As in *DoubleClick*, the plaintiffs claimed that Pharmatrak intercepted certain personally identifiable information that they revealed to the pharmaceutical companies by filling out electronic forms on the companies' websites.[242] The court of appeals found that any "consent" by Pharmatrak's pharmaceutical partners was too general to trigger the § 2511(d) exception.[243] The *Pharmatrak* court's underlying premise was that Pharmatrak's conduct satisfied

239. 18 U.S.C. § 2510(4) (2000).

240. For related criticism of *DoubleClick* and its progeny, see Kerr, *supra* note 188, at 830-33 (characterizing the court's interpretations as "hallucinogenic").

241. Pharmatrak II, 329 F.3d at 12.

242. *Id.* at 15-16.

243. *Id.* at 20 (concluding that mere purchase of service does not always imply consent).

the elements of § 2511(1)(a)[244]—except for the element of intent, as to which the court remanded for further consideration. Again, however, any information revealed to Pharmatrak was revealed because the user's browser was configured to reveal it or because the pharmaceutical companies' sites were configured in such a way as to reveal it.

The reasoning of courts considering whether use of cookies violates the SCA is equally problematic. There too, courts typically disposed of the claims on the issue of consent—under the exception in § 2701(c)(2) for conduct authorized "by a user of [a wire or electronic communication service] with respect to a communication of or intended for that user."[245] Several courts glossed over the numerous problems with applying the statutory framework at all, either by assuming the elements of the SCA were met or relying on parties' concessions. I alluded to some of these problems above in my discussion of spyware. First, it is difficult to identify a "facility through which an electronic communication service is provided" to which the content provider or advertiser gains unauthorized access.[246] In *DoubleClick*, for example, the plaintiffs seemed to object to the access that DoubleClick had *to the user's hard drive* in placing a cookie.[247] But even if the user's hard drive is properly viewed as a "facility"—a proposition that the *DoubleClick* district court and other courts seemed to accept[248]—that facility provides no electronic communications service. The court treated "internet access" as the relevant electronic communication service,[249] but if it is, then the user's hard drive is not a "facility" through which this service is provided.[250]

---

244. *Id.* at 18 (discussing elements).

245. *See, e.g.*, *Pharmatrak I*, 220 F. Supp. 2d at 13-14; In re Toys R Us, Inc. Privacy Litig., 2001 WL 34517252, at *6 (N.D. Cal. 2001); Chance v. Avenue A, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001); In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001). *But see* In re Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1275 (discussing consent exception, but stating that "[i]t is unclear to the court how this exception buttresses defendant's contention").

246. The *Pharmatrak* district court recognized this problem. *See Pharmatrak I*, 220 F. Supp. 2d at 13.

247. *DoubleClick*, 154 F. Supp. 2d at 509 (referring to "personal computer" as "facility").

248. *See Toys R Us*, 2001 WL 34517252, at *2 n.7 (describing defendant's interpretation of 'facility' as "limited"); *Chance*, 165 F. Supp. 2d 1153, 1161 ("[I]t is possible to conclude that modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities covered under the Act."); *DoubleClick*, 154 F. Supp. at 508 (concluding that plaintiffs had adequately pled offense under § 2701(a)(1), and thus implicitly assuming that hard drive constituted facility).

249. *DoubleClick*, 154 F. Supp. 2d at 508.

250. *See Pharmatrak I*, 220 F. Supp. 2d at 13 ("The relevant *service* is Internet ac-

As noted, the *DoubleClick* court disposed of the SCA claim on a consent theory. In particular, the court reasoned that its acquisition of communications was authorized by the websites DoubleClick served, because the communications were intended for the websites and the companies providing primary content for sites had contracted with DoubleClick to engage in profiling activities—even if the companies did not know the specifics of whether DoubleClick would have access to personally identifiable information.[251] Again, because of the court's ultimate conclusion with respect to consent, its treatment of the other elements of the SCA may not seem important. But the *Pharmatrak* case illustrates the difficulty in this approach. Although the court of appeals in *Pharmatrak* did not address the plaintiffs' claims under the SCA,[252] its disposition of the issue of consent under the Wiretap Act suggests that it would reject the theory that Pharmatrak's website clients authorized acquisition of the communications at issue for purposes of the SCA's consent exception.[253] As with the Wiretap Act, then, the *DoubleClick* court's approach to the substantive predicate for liability has the potential to harden into an accepted framework for similar claims, despite the awkward fit with the statutory text.

3. Theofel v. Farey-Jones

Theofel v. Farey-Jones[254] provides a final example of a privacy-protective but deeply flawed application of surveillance law. A group of plaintiffs alleged that Farey-Jones, a plaintiff in a separate civil suit in which some of the *Theofel* plaintiffs were defendants, and his attorney improperly acquired their electronic communications.[255] In the course of discovery in the separate case, Farey-Jones's attorney issued a civil subpoena seeking certain communications from the *Theofel* plaintiffs' ISP.[256] The subpoena was overbroad and was subsequently quashed,[257] but only after the ISP complied and turned over numerous communications unrelated to the subject matter of Farey-Jones's lawsuit.[258] The *Theofel* plaintiffs filed

---

cess, and the service is provided through ISPs or other servers, not [through] Plaintiffs' PCs.").

251. *DoubleClick*, 154 F. Supp. 2d at 511.

252. The district court had granted Pharmatrak summary judgment on the SCA claims, *Pharmatrak I*, 220 F. Supp. 2d at 14, and the plaintiffs apparently did not appeal that disposition, *Pharmatrak II*, 329 F.3d at 13.

253. *See Pharmatrak II*, 329 F.3d at 19-22.

254. 341 F.3d 978 (9th Cir. 2003) [hereinafter *Theofel I*], *reh'g denied and opinion superseded*, 359 F.3d 1066 (9th Cir. 2004) [hereinafter *Theofel II*].

255. *Theofel I*, 341 F.3d at 982.

256. *Id.* at 981.

257. *Id.* at 981-82.

258. *Id.* at 981.

suit alleging violation of § 2701(a) of the SCA.[259]

The district court dismissed the SCA claim, apparently in part on the theory that the defendants acquired the communications with the authorization of the service provider.[260] The ISP had provided the defendants with access to the communications in response to the subpoena.[261] Section 2701(a) only covers unauthorized access to a communications facility. In addition, § 2701(c)(1) exempts from § 2701(a)'s coverage conduct authorized by the service provider.[262] If the ISP authorized the defendants' access, then § 2701(a) would not prohibit their conduct.

On appeal, the Court of Appeals for the Ninth Circuit reversed.[263] The court analogized § 2701(a) of the SCA to a common-law trespass action.[264] Although a defendant is not liable for a trespass if the plaintiff authorizes his conduct, in some circumstances (though not all) deceit will vitiate consent.[265] Here, because the subpoena was blatantly invalid, it could not form the basis for the ISP's consent to the defendants' access to the plaintiffs' communications.[266] In other words, since the ISP's authorization for the defendants' access to the communications was improperly obtained, it did not qualify as authorization at all.

The court also rejected the defendants' alternative argument that the communications to which the ISP provided access were not in "electronic storage," and therefore were not covered by the SCA.[267] Section 2701(a) of the SCA only prohibits obtaining, altering, or preventing authorized access to a communication while that communication is in electronic storage within the provider's facility.[268] Section 2510(17) defines "electronic storage" to include "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[269] The court acknowledged that other courts have limited application of the term electronic storage to communications not yet retrieved by the intended re-

259. The plaintiffs also brought Wiretap Act and CFAA claims, which I do not discuss here.

260. *Id.* at 982.

261. *Id.* at 981.

262. 18 U.S.C. § 2701(c)(1) (2000).

263. *Theofel I*, 341 F.3d at 985.

264. *Id.* at 983.

265. *Id.*

266. *Id.* at 983-84.

267. *Id.* at 984.

268. 18 U.S.C. § 2701(a) (2000).

269. 18 U.S.C. § 2510(17) (2000 & Supp. II 2002).

cipient.[270] The court concluded, however, that communications not deleted by the recipient and therefore remaining on the ISP's server are stored "for purposes of backup protection."[271]

In response to a petition for rehearing with a suggestion for rehearing en banc, the court replaced its discussion of "electronic storage" with a lengthier discussion reaching the same result.[272] In particular, the court rejected a suggestion by the United States in an *amicus* brief that the court's interpretation of "electronic storage" rendered substantial portions of the SCA irrelevant.[273]

Notwithstanding the egregiousness of the defendants' conduct, the court of appeals's effort to extend the SCA to reach the conduct is problematic for several reasons. First, § 2701(a) of the SCA requires a showing that a defendant gained unauthorized access to a facility through which an electronic communication service is provided. In this case, the relevant facility presumably would have been the service provider's mail servers. But the defendants never gained access to that facility at all. Instead, the service provider copied the e-mail messages in question and made them separately available to the defendants on a website.[274] As to the website, even if it were a "facility through which an electronic communication service is provided" for purpose of § 2701(a), the defendants' access was authorized: the service provider supplied the defendants with the link to the site. The service provider could just as easily have printed the communications and mailed them to the defendants. The court of appeals's application of § 2701(a) and its discussion of common law trespass gives one the impression that the defendants gained access to mailboxes on the service provider's servers dedicated to the plaintiffs' use, but that is simply not the case. In other words, the court took great pains to explain why defendants' access was unauthorized, when there was no "access" to the provider's mail servers at all.

In addition, on the issue of electronic storage, the Ninth Circuit's interpretation reflects a strained reading of the statutory text. The definition of "electronic storage" implies that, in a determination of whether a com-

---

270. *Theofel I*, 341 F.3d at 985.

271. *Id.*

272. *Theofel II*, 359 F.3d at 1069-70, 1076-77.

273. *Id.* at 1076. I alluded earlier to the government's view that messages held by a server after retrieval by a subscriber are no longer in electronic storage with the provider of an electronic communication service; if held by a public provider they are instead merely "held or maintained" by the provider of a remote computing service. *See supra* notes 162-165 and accompanying text.

274. *Theofel I*, 341 F.3d at 981.

munication is in backup protection, the relevant perspective is that of the *service provider*, not the user. The provision covers storage *by* the electronic communication service *for purposes* of backup protection. Moreover, the term "backup" presupposes the creation of a second copy of a communication. A user who simply chooses not to delete a communication may wish to continue to store the communication, but he or she is not actually "backing up" the communication. The court also completely overlooked the relevance of the fact that the defendants simply gained access to a web-based database for which the provider supplied a link rather than to the provider's mail server. There is no theory under which data indefinitely maintained on a website is in "temporary, intermediate storage" "incidental to its transmission." And the service provider's purpose in copying the communications to a web server was quite obviously not to provide backup protection, but to make the communications available to the defendants.

C. The Unraveling of Privacy-Protective Approaches

The cases above reflect instances of courts aggressively interpreting surveillance law statutes in a privacy-protective way in response to bad facts. Even when courts' approaches do not result in an ultimate ruling in favor of the party challenging a particular practice, they constrain other parties' behavior or mark an incremental step toward an ultimate ruling in favor of plaintiffs challenging similar practices. One might argue that courts' approaches are perfectly appropriate—that courts can and should aggressively interpret electronic surveillance statutes, particularly in light of the fact that technological changes have made it difficult to apply those statutes. There are serious difficulties with such a view, however. First, as this section illustrates, some privacy-protective approaches are sufficiently vulnerable on statutory interpretation grounds that they are likely to unravel. Second, as discussed in Section D, decisions that appear to be privacy-protective can derail momentum for legislative change—even when the decisions are sufficiently tailored to specific factual disputes that they are unlikely to affect a broad class of privacy threats.

United States v. Smith[275] provides a useful example of a case in which an approach that appeared to be privacy-protective ultimately unraveled. Congress, of course, amended the definition of wire communication in the SCA so as to overturn the specific result of the *Smith* case.[276] Both before and after Congress's action, however, the Ninth Circuit wrestled with the

275. 155 F.3d 1051 (9th Cir. 1998).

276. *See supra* notes 198-206 and accompanying text; *infra* notes 290-293 and accompanying text.

implications of *Smith* for cases involving private acquisition of *electronic* communications. The result was eventual abandonment of the *Smith* approach with respect to the Wiretap Act.

Konop v. Hawaiian Airlines, Inc.[277] involved claims that a Hawaiian Airlines supervisor violated both the Wiretap Act and the SCA by obtaining communications from the password-restricted portions of an employee's website. Konop, a pilot for Hawaiian Airlines, created and maintained a website where he posted bulletins critical of his employer and union officials.[278] Although the site was password-restricted, a Hawaiian Airlines supervisor, Davis, gained access to it by using the user names and passwords of employees who could legitimately use the site.[279] Konop claimed that the supervisor's conduct violated both the Wiretap Act's prohibition on interception of communications and the SCA's prohibition on accessing a facility without authorization and thereby "obtain[ing] . . . a communication in electronic storage" in that facility.[280]

In its first decision in the *Konop* case (*Konop I*), the Ninth Circuit applied *Smith*'s holding with respect to wire communications to the electronic communications at issue.[281] As noted above, *Smith*'s endorsement of prior precedent concluding that an *electronic* communication can only be intercepted during transmission, coupled with its adoption of a definition of interception that covered acquisition of stored *wire* communications, created an anomaly: the term "intercept" had two different meanings depending on whether wire or electronic communications were at issue.[282] The *Konop I* court acknowledged this problem,[283] but rather than recognizing the error of the *Smith* case, the court concluded that an electronic communication need not be acquired while in transmission to be intercepted for purposes of the Wiretap Act: "[T]he Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit."[284]

Significant problems exist with the approach of the *Konop I* court, both on a practical level and as a matter of statutory interpretation. If acquisition of an electronic communication in storage constitutes an inter-

277. 236 F.3d 1035 (9th Cir. 2001) [hereinafter *Konop I*], *withdrawn*, 262 F.3d 972 (9th Cir. 2001), *new opinion filed*, 302 F.3d 868 (9th Cir. 2002) [hereinafter *Konop II*].

278. *Konop I*, 236 F.3d at 1041.

279. *Id.*

280. *Id.* at 1040.

281. *Id.* at 1046.

282. *See supra* notes 224-228 and accompanying text.

283. 236 F.3d at 1044.

284. *Id.* at 1046.

ception, then law enforcement officials would presumably need a full Title III order to acquire access to such communications. But requiring the government to seek a Title III order to acquire stored electronic communications would render the governmental access provisions of the SCA[285] meaningless, since law enforcement officials presumably could not use them. Moreover, the *Konop* court failed to consider the implications of extending *Smith*'s reasoning not only to ordinary electronic communications such as e-mail, but also to files held on a web server. Under the court of appeals' theory, any acquisition of such material against the wishes of the operator of the web server might constitute an interception for purposes of the Wiretap Act.[286] Perhaps concerned about this fact, the court emphasized that two exceptions would limit application of the Wiretap Act to viewing of a website: § 2511(2)(g)(i)'s exception for accessing an electronic communication "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public," and § 2511(2)(d)'s exception for acquisition of a communication where "one of the parties to the communication has given prior consent to such interception."[287] Because Konop's site was configured to require a password, neither exception applied. And even though Davis accessed the site by using the password of another pilot who did have authority to view Konop's posting, the court concluded that the other pilot was not in fact a "party" to the communication, because that pilot never actually participated in any communication with Konop.[288]

In light of the practical and interpretive difficulties, the *Konop I* court's decision was understandably the target of a petition for rehearing, and the court ultimately withdrew its opinion and abandoned its problematic reading of the Wiretap Act. The superseding opinion followed the line of cases, acknowledged in *Smith*, holding that interception of an electronic communication occurs only during the communication's transmission.[289] By the time the court of appeals reconsidered the case, the USA Patriot Act had eliminated the phrase "in electronic storage" from the definition of a wire communication.[290] The *Konop II* court therefore believed that it could, without disturbing the reasoning of *Smith*, abandon its previous conclusion that stored electronic communications could be intercepted.[291]

---

285. *See* 18 U.S.C. § 2703 (2000 & Supp. II 2002).
286. *See Konop I*, 236 F.3d at 1040.
287. *Id.* at 1046-47.
288. *Id.* at 1047.
289. *Konop II*, 302 F.3d at 878.
290. *Id.* at 877 n.5, 878; *see also supra* notes 198-206 and accompanying text.
291. *See id.* at 877-78.

Of course, the USA Patriot Act did not in any way affect the definition of the term "intercept," so there remained a strong argument that the *Smith* court's interpretation of that term (if correct) should still control. The dissent so argued,[292] although, as I have shown above, the *Smith* court's interpretation simply was erroneous and should have been more explicitly abandoned.[293]

Smith and *Konop* raise another interesting point about why aggressive interpretations of electronic surveillance statutes ultimately fail to provide greater privacy protection. The fact that surveillance statutes restrain both private parties and the government proves to be a double-edged sword. Because privacy-protective outcomes will constrain the government, the Justice Department has a significant incentive to oppose them. Indeed, the Justice Department, as *amicus curiae*, was one of the main proponents of rehearing both *Konop* and *Theofel*. The Justice Department's brief in *Konop* forcefully objected to the fact that, under that case's reasoning, the government would have to secure Title III orders before accessing stored communications—when the SCA clearly contemplated government access upon presentation of a search warrant (or, in some cases, a subpoena or special court order). Similarly, the *Theofel* court's conclusion that communications retained in a user's mailbox can be in backup storage prompted a petition for reconsideration by the government arguing that the court's interpretation would render portions of the SCA meaningless.[294]

To be sure, the government's incentives in this context are quite complicated. To the extent that the government succeeds in pressing for interpretations of surveillance statutes that allow for greater government access to communications, it constrains its own ability to prosecute bad actors.[295]

---

292. *Id.* at 891 (Reinhardt, J., dissenting).

293. While reversing its problematic reading of the Wiretap Act, the *Konop II* court adopted an equally strained reading of the SCA. As discussed earlier, the SCA prohibits one from intentionally accessing without authorization a facility through which an electronic communication service is provided, or exceeding an authorization to access that facility, and thereby "obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a)(1) (2000). Konop claimed that Davis's viewing of material posted on his website violated this provision. Applying this statutory framework to websites, however, is fraught with some of the same problems discussed with respect to spyware and the cookie cases. *See supra* notes 151-167 and accompanying text. A detailed discussion of this aspect of *Konop II* is beyond the scope of this Article.

294. *See supra* notes 273-274 and accompanying text.

295. For an argument that the dual nature of the Wiretap Act successfully limits aggressive government interpretations of the statute, see Paul K. Ohm, *Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1603 (2004).

The *Scarfo* and *Ropp* cases well illustrate that point: the government's argument in *Scarfo* that its keystroke monitor did not require a Title III order played a prominent role in the *Ropp* court's conclusion that a private party's use of a keystroke monitor did not violate the Wiretap Act.[296] The fact that the government both prosecutes offenses under and is constrained by application of the surveillance statutes can therefore act as a disciplining force. Indeed, the *Councilman* case provides a prominent example of a case in which the government opposed an interpretation of the Wiretap Act that would have been quite favorable to its interests. The district court and First Circuit panel majority essentially held that the Wiretap Act does not cover communications briefly stored at any point prior to being made available to the recipient.[297] Under the courts' reasoning, the government would not need to apply for a full Title III order before obtaining such communications; it could instead proceed under the less protective provisions of the SCA, which at most would require a search warrant.[298] The government nevertheless sought reversal of the decisions.

Despite the complexity of the government's incentives, the fact that the effects of too-aggressive interpretations of surveillance statutes will profoundly affect government investigations means that such interpretations will not go unchallenged.

D. The Impetus for Legislative Change

Apart from the instability of case law that aggressively interprets electronic surveillance statutes, such case law has potentially harmful effects on the momentum for legislative change. Here, the *Pharmatrak* case provides a useful example. Nearly all the cookie cases decided prior to *Pharmatrak* resulted in dismissal or summary judgment. To be sure, those cases could have more plainly shown how poor the fit was between the surveillance law statutes and the conduct complained of in those cases.[299] But to the extent that the conduct complained of in those cases was normatively objectionable (and I do not intend to express an opinion on this point), the dismissals made it more likely that such conduct would have been the subject of legislative attention, perhaps to develop a tailored data privacy statute. When a case such as *Pharmatrak* is decided, however, it appears that surveillance statutes *are* in fact successful in combating data privacy challenges posed by the Internet, rendering the need for a legislative response far less urgent.

---

296. *See supra* notes 93-113 and accompanying text.
297. *See supra* notes 114, 183-189 and accompanying text.
298. *See supra* note 189 and accompanying text.
299. *See supra* notes 230-253 and accompanying text.

Indeed, it is not difficult to envision the same phenomenon occurring with the *Councilman* case. The First Circuit panel majority's decision in June of 2004 was quickly condemned in the popular press, and a legislative fix was introduced soon after.[300] *Councilman* served an extremely useful function of bringing attention to the problems that arise at the intersection of the Wiretap Act and the SCA. The problems were in fact far more significant than popular accounts of the *Councilman* case suggested. In particular, although the district court and panel majority were quite clearly wrong to conclude that communications move in and out of the Wiretap Act's protective umbrella during transmission, depending on whether they are between or within computers transmitting them, a significant privacy problem lurks even now that the *Councilman* decision has been reversed by the *en banc* court. Because the defendant in *Councilman* acted as the provider of an e-mail service, he would have been entitled to access the communications in question as soon as the communications were made available in the system for retrieval by the subscriber. Even though such communications would have been in "electronic storage" in the provider's system for purposes of § 2701(a) of the SCA,[301] § 2701(c)(1) provides that the prohibition does not apply with respect to conduct authorized by the service provider.[302] In other words, Councilman's conduct clearly should have been covered by the Wiretap Act because the communications were seized prior to delivery to the subscriber's mailbox; but had Councilman only waited to seize the communications until they were stored in the subscriber's mailbox, retrieval of those communications would have been perfectly legal as a matter of federal law. The overturning of *Councilman* is a welcome result, but it has one unfortunate consequence: sapping much of the legislative momentum for reconsidering the intersection of the Wiretap Act and the SCA.

V. CONCLUSION

The prospects for using surveillance law to effect a significant change in spyware practices are quite limited. Although surveillance law may curtail extreme forms of spyware (if courts overcome obstacles that current case law imposes), a range of seemingly invasive practices will be unaffected, and there is virtually no prospect of reforming industry practices through surveillance law litigation.

The spyware story is simply not unusual. Plaintiffs have sought to use

300. *See, e.g.*, H.R. 4977, 108th Cong. (2004); H.R. 4956, 108th Cong. (2004).
301. 18 U.S.C. § 2701(a) (2000).
302. *Id.* § 2701(c)(1).

surveillance law statutes to address a number of digital-age privacy problems. In many cases, such efforts have failed. Perhaps more damaging, however, are some of the cases in which such efforts have succeeded. Aggressive privacy-protective approaches to surveillance law statutes do not last; they give a false sense that existing law is adequate; and they derail momentum for much-needed legislative change, both with respect to surveillance law itself and with respect to specific data privacy problems such as spyware. As I have suggested, we would do better simply to make surveillance law's limits plain.

CONTRACTING SPYWARE BY CONTRACT

By Jane K. Winn[†]

TABLE OF CONTENTS

I. INTRODUCTION: FROM GOODWARE TO BADWARE[1] TO SOMEWHERE IN BETWEEN

Does contract law provide consumers whose computers are clogged with spyware any tools to defend themselves against this onslaught of unwanted software? The answer is likely to be no, as courts have shown themselves to be generally willing to enforce online contracts notwithstanding questions about what consumers actually knew or intended when the contract was formed. Although at one extreme it is easy to identify "badware"—viruses, Trojan horses, and other clearly malicious programs—and at the other, it is equally easy to identify "goodware"—popular shareware or freeware applications—there is considerable uncertainty about what end users really think about many programs. Furthermore, software that some commentators label pernicious "spyware" is considered to be comparatively benign "adware" by others, making it hard to be certain what an individual consumer would think of the program in question and whether the consumer would agree to contract for it.[2]

---

† Jane K. Winn, Professor & Director, Shidler Center for Law, Commerce & Technology, University of Washington School of Law, http://www.law.washington.edu/Faculty/Winn (last visited Aug. 17, 2005). Many thanks to my research assistant Andrew Braff for all his help.

1. Thanks to my colleague Bill Covington for suggesting these terms to characterize the two ends of the spectrum of applications that have been labeled spyware.

2. *E.g.*, WeatherBug is perceived by some to be a legitimate piece of software and adware/spyware by others. *Compare* PC Hell, WeatherBug Removal Instructions and Help, http://www.pchell.com/support/weatherbug.shtml (last visited Aug. 17, 2005), *with* WeatherBug Frequently Asked Questions, Is WeatherBug spyware or adware?, http://www.weatherbug.com/aws/support/faq_spyware.htm (last visited Aug. 18, 2005).

In evaluating online contracts, courts generally have shown more deference to the intent of the merchants who design the contract interfaces than to the expectations of consumers using them. In the event any consumers claim software was loaded on their computers without authorization, that deference toward the intent of the online interface designer is likely to protect distributors of programs that deliver "targeted marketing"[3] to consumers using a click-through contract interface.

In order for contract law to provide a meaningful constraint on the distribution of spyware programs, a major revision of current contract law would be required. Legislation pending in Congress in 2005 proposes to do just that: require explicit notice and consent from end users before spyware can be loaded onto their computers.[4] Assuming such a strategy might actually have an impact on the volume of spyware distributed,[5] it remains unclear whether such a piecemeal, ad hoc approach is a sensible approach to contract law reform. A similar strategy of narrowly targeted sector-specific reforms has been used in U.S. information privacy law for the last two decades with disastrous results;[6] it is not clear that such a strategy would be any more successful when applied to contract law. By contrast, the more general regulatory approach taken in the EU Unfair Contract Terms Directive[7] could be used both to block the use of misleading contract interfaces to legitimate the distribution of spyware and to provide critical scrutiny of merchant designed contracting interfaces generally.

The label "spyware" has been applied to a wide range of software applications, and it is difficult to identify an authoritative definition of spyware which would clarify the scope of the problem.[8] Because an in-depth

---

3. "Targeted marketing" consists of making "the right offer to the right customer at the right time." AffiliateTip.com, Affiliate Program Glossary, http://affiliatetip.com/affiliate_glossary.php (last visited May 1, 2005).

4. Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), H.R. 29, 109th Cong. (2005).

5. This would be in contrast to the CAN-SPAM Act, which one year after enactment "clearly has had no meaningful impact on the unrelenting flow of spam that continues to clog the Internet and plague inboxes." Keith Regan, *CAN-SPAM Gets Mixed Report Card for First Year*, MACNEWSWORLD.COM, Jan. 3, 2005, http://www.macnewsworld.com/story/39354.html.

6. *See, e.g.*, DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 58 (2003); Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 285 (2003).

7. *See* Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts, 1993 O.J. (L 95) 29 (EC); *infra* text at notes 55-61.

8. *See, e.g.*, SpywareGuide, Intro to Spyware, http://www.spywareguide.com/txt_intro.php (last visited May 1, 2005) (describing over 1,500 programs that met its defini-

analysis of competing definitions of spyware is beyond the scope of this paper, this paper will take the following definition from the Federal Trade Commission 2004 Federal Register Notice:

> [Spyware is] software . . . that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.[9]

Not all distributors of programs covered by this definition of spyware use contracting interfaces to help manage their relationship with those consumers whose computers run their software. Distributors of software that includes viruses or other malware—which permit the software developer to commit identity theft or to access the end user's financial accounts without authorization—can distribute their programs with interfaces that do not require the cooperation of the end user. Therefore, they have no reason to ask the end user to assent to the download. The following discussion will address only those software distributors that include contracting interfaces in their distribution systems.

There are many popular "shareware"[10] or "freeware"[11] programs that provide unambiguous benefits to end users who manifest assent to their end user license agreements by using a click-through interface.[12] Because end users' understanding of a program's function and users' level of interest in granting programs access to their computers is uncertain, many targeted marketing or adware programs fall somewhere in between the ex-

---

tion of spyware in May 2005 including parasiteware, adware, spyware, malware, page hijackers, and dialers as various types of software that may be covered by the term spyware.); *see also* Press Release, Consumers Union, Consumer Reports Investigates How to Protect Against Spam, Spyware and Phishing, August 9, 2004, http://www.consumersunion.org/pub/core_product_safety/001305.html (last visited May 1, 2005) ("Spyware isn't a single type of software. The term covers a diverse range of applications.").

9. Notice Announcing Public Workshop and Requesting Public Comment, 69 Fed. Reg. 8538 (Feb. 24, 2004).

10. "Shareware is software that is distributed free on a trial basis with the understanding that the user may need or want to pay for it later." *Shareware*, Whatis.com, http://whatis.techtarget.com/wsearchResults/1,290214,sid9,00.html?query=shareware (last visited Aug. 30, 2005).

11. "Freeware . . . is programming that is offered at no cost and is a common class of small applications available for downloading and use in most operating systems." *Freeware*, Whatis.com, http://whatis.techtarget.com/wsearchResults/1,290214,sid9,00.html?query=freeware (last visited Aug. 30, 2005).

12. See, for example, the contracting interfaces for the most popular free software downloads listed at http://www.download.com (last visited May 1, 2005).

tremes of universally detested and virulent spyware and acclaimed and popular freeware. While many end users might welcome targeted comparison shopping information about products they are actively seeking, they also may hate pop-up ads. End users might not understand either the specific quid pro quo that a particular targeted marketing company is offering (for example, free access now to desirable content in return for exposure to pop-up ads in the future) or the mechanism by which that quid pro quo is enforced (for example, adware applications loaded on the end user's computer).

This Article focuses only on those ambiguous cases where a merchant has a plausible claim that consumers have consented to the collection of personal information in exchange for some product or service, but consumers also have a plausible claim that there was no consent. The application of contract law to spyware programs in this ambiguous, intermediate position between goodware and badware produces uncertain outcomes, in part because the intent of the end user in contracting or downloading is uncertain. The recent trend in contract cases toward liberalizing contract formation doctrine, in effect removing obstacles to the greater use of new technologies, makes it unlikely that contract law could create a framework within which more explicit consent must be sought before collecting personal information. While courts may be unwilling to invalidate clickwrap agreements that legitimate the distribution of adware programs that many find annoying, such deference has limits. There is no reason to expect that judicial deference to online contracts will extend so far as to legitimate the distribution of clearly malicious programs that support fraudulent or criminal activities.

II. INTERPRETING AMBIGUOUS ONLINE CONTRACTING INTERFACES

Targeted marketing firms that collect personal information in exchange for providing products or services to consumers use contracting interfaces similar to those used by other online merchants: click-through interfaces that seek blanket assent to standard form contracts. What often distinguishes the online contracting processes used by marketing firms such as Claria and WhenU is that consumers may not realize that when they click "I agree" in response to what appears to be a standard end user license agreement (EULA),[13] they are licensing a bundle of different ap-

13. Use of adware distributed by Claria (formerly known as Gator) is governed by an EULA accessible at the website for Gain Publishing. Gain Publishing, Privacy Statement and End User License Agreement, *available at* http://www.gainpublishing.com

plications—including programs labeled spyware by consumer advocates.[14] Consumers may intend to download a single application and instead download several programs—including some they do not want—either by inadvertence, because the desired application is not available without the extra programs, or because the different programs have actually been combined into one. The problem of inadvertent or qualified assent is exacerbated by the fact that many adware programs are difficult to locate and remove because they are not listed in the "Add/Remove Programs" function provided by Microsoft Windows operating systems.[15]

Before asking whether assent to the terms of adware EULAs should be treated differently than assent to other Internet contracts, it may be useful to consider the current state of Internet contracting doctrine generally. Whether assent to an offer to form a contract has been manifested is a fact-specific inquiry. The Restatement provides that manifestation of assent may be by written or spoken words, by other acts, or by failure to act—but the conduct in question must be intentional or the actor must have reason to know that conduct will be treated as assent by other party. In the absence of such a manifestation of assent, then the contract may be voidable for fraud, duress, mistake, or any other invalidating cause.[16] The manifestation of mutual assent to any exchange ordinarily takes the form of an offer or proposal by one party followed by an acceptance by the other party or parties;[17] however, a manifestation of mutual assent may be made even though neither offer nor acceptance can be identified and even though the moment of formation cannot be determined.[18] The application

---

/global/help/app_privacy/app_ps_v70.html (last visited May 1, 2005). WhenU distributes a wide variety of direct marketing programs that are considered spyware by others, including SaveNow, WhenUShop, WeatherCast, ClockSynch, and PriceBandit. Copies of the EULA for each product can be accessed at http://www.whenu.com/support.html (last visited Aug. 17, 2005). The contract interface for WhenU is described at http://www.whenu.com/how_whenu_works_dl.html (last visited May 1, 2005).

14. *See, e.g.*, Tatiana Serafin, Mr. Manners, FORBES, July 26, 2004, at 133 ("The Federal Trade Commission held workshops on spyware in April, knocking companies (read Claria and WhenU) for failing to disclose how their software programs glom on to PCs and how they misbehave thereafter.").

15. *Id.*

16. RESTATEMENT (SECOND) OF CONTRACTS § 19 (1981).

17. *Id.* § 24 states that an offer is defined as the manifestation of willingness to enter into a bargain, so made as to justify another person in understanding that his assent to the bargain is invited and will conclude it.

18. *Id.* § 22. U.C.C. § 2-204 (2003) similarly provides:

> (1) A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract.

of these principles that guide inquiry into a contract formation using standard form contracts raises troubling, unresolved issues about the meaningfulness of the assent.[19] The Restatement's provisions addressing the use of standard form contracting attempt to balance the pervasive use of forms with the desire to preserve some vestige of concern with the character of assent to the contents of forms.[20]

The apparent conflict between the freedom of choice ideology embedded in contract doctrine and the magnitude of the constraints imposed on consumer choice by standard form contracts does not appear to be any more acute in the online environment than it has been in traditional markets.[21] There does not appear to be any clear evidence that consumers are less able to deal with click-through contracting interfaces than they were able to deal with traditional paper form contracts, or that legitimate merchants use click-through interfaces to take advantage of consumers any more often than they did with printed form contracts. Furthermore, the question remains whether the presence of a discernable assent should

---

> (2) An agreement sufficient to constitute a contract for sale may be found even though the moment of its making is undetermined.
> (3) Even though one or more terms are left open a contract for sale does not fail for indefiniteness if the parties have intended to make a contract and there is a reasonably certain basis for giving an appropriate remedy.

19. Contract scholars have recognized for nearly a century that the use of standard form contracts is widespread but at the same time fails to conform to classical 19th century freedom of contract principles and debated strategies for dealing with this contradiction. *See* Nathan Isaacs, *The Standardizing of Contracts*, 27 YALE L.J. 34 (1917); Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943); W. David Slawson, *Standard Form Contracts and Democratic Control of Law-Making Power*, 84 HARV. L. REV. 529 (1971).

20. RESTATEMENT (SECOND) OF CONTRACTS § 211 provides:

> (1) Except as stated in Subsection (3), where a party to an agreement signs or otherwise manifests assent to a writing and has reason to believe that like writings are regularly used to embody terms of agreements of the same type, he adopts the writing as an integrated agreement with respect to the terms in the writing.
> (2) Such a writing is interpreted wherever reasonable as treating alike all those similarly situated, without regard to their knowledge or understanding of the standard terms of the writing.
> (3) Where the other party has reason to believe that the party manifesting such assent would not do so if he knew that the writing contained a particular term, that term is not part of the agreement.

21. Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 432-34 (2002).

really be the criteria for distinguishing between enforceable and unenforceable contracts formed using new contracting systems.[22]

While it may be difficult to ascertain whether courts are more or less deferential to merchants seeking enforcement of contracts formed with new contracting systems than they were toward merchants in traditional markets, it is not difficult to ascertain the overall trend of deference to merchant interface design choices in the face of consumer objections.[23] Because spyware is delivered exclusively in online environments, the debate surrounding the enforceability of "shrinkwrap"[24] and "pay now, terms later"[25] contracts is not relevant here.[26] The best indication of how courts would likely respond to consumer complaints about the enforceability of adware EULAs will come from cases addressing the enforceability of "clickwrap" and "browsewrap" agreements. Clickwrap contract interfaces require some explicit manifestation of assent by the consumer to form a contract; in most cases, the consumer is asked to select between graphical representations signifying "I accept" and "I decline" by clicking on the chosen alternative.[27] Browsewrap terms and conditions are usually found behind a hyperlink marked something like "Legal" or "Terms" or "Use of this site signifies your acceptance of the Terms and Conditions." Because end users must seek out browsewrap terms in order to learn their contents, there is considerable disagreement over whether browsewrap interfaces can be used to form contracts at all.[28] However, the mere fact that some courts have been willing to entertain the idea that an online contract could

22. Clayton P. Gillette, *Rolling Contracts as an Agency Problem*, 2004 WIS. L. REV. 679, 681 (2004) (arguing that it is possible to determine whether a contract should be enforced without reference to intent).

23. *See, e.g.*, James J. White, *Autistic Contracts*, 45 WAYNE L. REV. 1693 (2000) (noting the trend with approval); Jean Braucher, *Delayed Disclosure in Consumer E-Commerce as an Unfair and Deceptive Practice*, 46 WAYNE L. REV. 1805, 1807 (2000) (noting the trend with disapproval).

24. *See generally* Robert W. Gomulkiewicz, *Getting Serious About User-friendly Mass Market Licensing For Software*, 12 GEO. MASON L. REV. 687 (2004).

25. *See generally* Gillette, *supra* note 22 (using the term "rolling contracts" to describe "pay now, terms later" contracts).

26. *See* Gillette, *supra* note 22, at 685-88 (summarizing the debate); *see also* Christina L. Kunz et al., *Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent*, 57 BUS. LAW. 401 (2001) (reporting findings of the ABA Working Group on Electronic Contracting Practices report).

27. *Id*.

28. *See* Christina L. Kunz et al., *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 BUS. LAW. 279 (2003) (reporting findings of the ABA Working Group on Electronic Contracting Practices).

be formed without any apparent manifestation of assent by the end user is an important development in this area.[29]

The first cases holding explicitly that a click-through interface design could be used to form a binding contract appeared in 1998.[30] In all, more than a dozen cases have been decided upholding the enforceability of contracts formed using click-through interfaces.[31] In only a few cases have courts refused to enforce specific terms contained within contracts formed using a click-through interface, and the terms at issue have been found to violate a public policy of the forum state or to be unconscionable. In one, a court refused to enforce a choice of forum term that would have required a Massachusetts resident to file suit in Virginia, which does not generally permit class action law suits, because it found that to do so would in effect deprive Massachusetts consumers of any right to challenge the merchant's performance under the contract.[32] A federal district court refused to enforce an arbitration agreement contained in a click-wrap agreement after the merchant presented inadequate evidence of what contract terms had actually been displayed to the plaintiffs when they enrolled in the service, or of a subsequent modification of the terms to include an arbitration

29. *See generally id.*

30. The first appears to have been Hotmail Corp. v. Van Money Pie Inc., No. C98-20064 JW, 1998 U.S. Dist. LEXIS 1079 (N.D. Cal. Apr. 16, 1998) (granting preliminary injunction to stop spammer from using Hotmail's e-mail service because no e-mail account could be set up without clicking through online registration agreement prohibiting the sending of unsolicited commercial e-mail). A close second seems to have been Groff v. America Online, Inc., No. PC 97-0331, 1998 R.I. Super. LEXIS 46 (R.I. Super. Ct. May 27, 1998) (holding there was no authorization to proceed with a class action lawsuit when all members of putative class would have had to click through online registration agreements with a choice of forum clause pointing to a different jurisdiction).

31. Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999); In re RealNetworks, Inc. Privacy Litig., No. 00-C-1366, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. May 11, 2000); Lieschke v. RealNetworks, Inc., No. 99-C-7274, 2000 U.S. Dist. LEXIS 1683 (N.D. Ill. Feb. 10, 2000); America Online, Inc. v. Booker, 781 So. 2d 423 (Fla. Dist. Ct. App. 2001); Barnett v. Network Solutions, 38 S.W.3d 200 (Tex. App. 2001); Forrest v. Verizon Communs., Inc., 805 A.2d 1007 (D.C. 2002); Moore v. Microsoft Corp., 741 N.Y.S.2d 91 (App. Div. 2002); Net2phone, Inc. v. Superior Court, 135 Cal. Rptr. 2d 149 (Cal. Ct. App. 2003); DeJohn v. .TV Corp. Int'l, 245 F. Supp. 2d 913 (N.D. Ill. 2003); Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1170 (E.D. Mo. 2004); Mortgage Plus, Inc. v. DocMagic, Inc., No. 03-2582-GTV-DJW, 2004 U.S. Dist. LEXIS 20145 (D. Kan. Aug. 23, 2004).

32. Williams v. America Online, Inc., No. 00-0962, 2001 Mass. Super. LEXIS 11 (Mass. Super. Ct. Feb. 8, 2001); *accord* Scarcella v. America Online, 798 N.Y.S.2d 348 (Civ. Ct. 2004) (refusing to enforce AOL forum selection clause when alterative is small claims court). *But see* Celmins v. America Online, 748 So. 2d 1041 (Fla. Dist. Ct. App. 1999); *Booker*, 781 So. 2d at 423 (enforcing the same term against Florida residents).

term.[33] The plaintiffs also made plausible allegations of unconscionable behavior on the part of the merchant.

Given the strong trend in recent cases favoring the enforcement of clickwrap agreements in the absence of a conflict between contract terms and fundamental public policy of the forum, or evidence of misconduct so egregious that it might rise to the level of unconscionable, courts are likely to find that adware EULAs are enforceable contracts. Most recent clickwrap cases deal with consumer objections to the level of service provided by online service providers, and a consumer might try to distinguish a service contract under which a consumer gains access to e-mail and the Internet generally from an agreement under which a consumer gains access to comparison advertising presented in the form of annoying pop-up ads. However, in the absence of any evidence of serious misuse of personally identifiable information by the adware company, the distinction is unlikely to be persuasive.

One distinction between most clickwrap agreements with online service providers and adware companies is that, while consumers may rarely read and understand the terms of the online service provider's form contract before manifesting assent to it, they are likely to have a reasonably accurate idea of what the other party to the contract will provide. In the adware context, consumers may not have an accurate idea of what the other party will provide if the adware programs are bundled with other programs and the bundling is disclosed only in the form contract. Many consumers know they are downloading at least one program they want, but generally do not understand that their access to that program is conditioned on accepting a second program that will monitor their online conduct and transmit information about them to a third party so that relevant comparison ads can be shown to them in the future.[34] In other words, consumers are paying for access to the programs or services they want not with money but with personal information and displays of comparison ads.

Many consumers apparently believe that licenses to online content or access to online services are being granted in return for nothing more than a release of liability from the consumer to the provider. Given the popularity of such business models during the dot-com bubble, it might be difficult to say that such consumer expectations are unreasonable. In cases considering the enforceability of clickwrap agreements, however, few courts have shown an interest in analyzing the reasonableness of consumer

33. Comb v. PayPal, Inc., 218 F. Supp. 2d 1165, 1171 (N.D. Cal. 2002).

34. Ben Elgin, *Guess What—You Asked For Those Pop-Up Ads*, BUS. WEEK, June 28, 2004, at 94.

claims of being surprised by arbitration agreements or choice of forum clauses, even when those contract terms have the effect of making it prohibitively expensive for consumers to sue online merchants. It seems unlikely, therefore, that many courts would refuse to enforce adware EULAs solely on the grounds that to do so would frustrate consumer expectations about receiving free software.

Although several courts have held that browsewrap interfaces do not establish manifestation of assent to contract terms,[35] not all that have considered the issue have so held.[36] While this ambiguity in the case law hardly justifies advising a client that embedding the terms of a contract behind an obscure hyperlink may result in an enforceable contract, courts' unwillingness to reject uniformly such a suggestion as preposterous demonstrates the depth courts' deference to those who develop innovative contracting interfaces with what appears to be cavalier disregard for established contract law. Closer examination reveals that all three cases holding either that browsewrap might be the basis of a contract, or that summary judgment against the party advancing that argument would be premature, involve business-to-business contracts, instead of business-to-consumer contracts. Furthermore, in all three cases the party claiming that a browsewrap interface can be used to form a contract also had strong claims that the defendant should also be held liable for unfair competition. If the cases holding that browsewrap might be enough to form a contract are in substance disguised unfair competition cases, then consumers finding fault with the ambiguity of adware EULA contract interfaces should be able to distinguish those cases. But because adware distributors appear to be happy to use click-through interfaces, this distinction is unlikely to help many consumers who object to the adware on their computers.

---

35. Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654-HLH (BQRx), 2000 U.S. Dist. LEXIS 12987, at *18 (C.D. Cal. Aug. 10, 2000); Specht v. Netscape, 306 F.3d 17 (2nd Cir. 2002); *In re* Northwest Airlines Privacy Litig., No. 04-126 (PAM/JSM), 2004 U.S. Dist. LEXIS 10580 (D. Minn. June 6, 2004).

36. Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974 (E.D. Cal. 2000) (refusing summary judgment dismissing contract claims); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (holding that contract was formed by posted terms even without click-though interface where evidence showed that defendant had actual knowledge of terms); Ticketmaster Corp. v. Tickets.com, No. CV99-7654-HLH (VBKx), 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 6, 2003) (reviewing a revised Ticketmaster interface and refusing Tickets.com summary judgment dismissing contract claims).

III. LIABILITY UNDER OTHER FORMS OF ONLINE MARKET REGULATION

Because it seems unlikely that contract law will provide much protection to consumers from unwanted adware, the possibility that other doctrines that regulate market conduct could provide a shield should be explored. However, a review of unfair competition, deceptive trade practices, electronic surveillance, and computer fraud laws provides little more hope for disgruntled consumers than does contract law.

Both federal and state unfair competition laws provide competitors a cause of action to object to improper conduct by merchants on behalf of consumers rather than providing consumers with a direct cause of action. Section 43(a) of the Lanham Act prohibits the use in commercial advertising of any word, term, name, symbol, or device, or false or misleading statement of fact that misrepresents the nature, characteristics, or quality of goods, services, or commercial activities.[37] Section 2 of the Restatement (Third) of Unfair Competition Law provides that "one who, in connection with marketing of goods or services, makes a representation relating to the actor's own goods, services, or commercial activities that is likely to deceive or mislead prospective purchasers to the likely commercial detriment of another" may be liable to the other. As with Section 43(a), the appropriate remedy in the absence of a showing of specific harm to a competitor is injunctive relief.[38] Companies whose customers are shown comparison ads by means of adware may well have an unfair competition claim against the adware company or its customer whose comparison ad is displayed, but consumers would not be able to bring suit in their own names if no competitor was willing to act.

Because spyware involves the transmission of personal information without the knowledge or consent of the person whose information is being sent, and because federal deceptive trade practices law has been the foundation of Federal Trade Commission (FTC) efforts to increase the level of protection given to personal information,[39] federal deceptive trade

37. 15 U.S.C. § 1125(a)(1) (2000).

38. RESTATEMENT (THIRD) OF UNFAIR COMPETITION LAW § 35 (1995).

39. Section 5 of the FTC Act provides "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful." 15 U.S.C. § 45(a)(1) (2000). Since the late 1990s, the FTC has been encouraging online businesses to disclose their privacy practices and taking enforcement actions based on its deceptive trade practices authority against online businesses that fail to do what their privacy policies say. *See* FTC, Enforcing Privacy Promises: Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last

practices law actions seem like a promising strategy to help consumers fight back against unwanted adware programs. By 2005, however, the FTC had announced only two spyware enforcement actions.[40] Because many states have enacted "Little FTC Acts" with provisions similar to Section 5 of the FTC Act that are enforced by state attorneys general or that grant a private cause of action to consumers, consumers may have better luck fighting spyware with state deceptive trade practices law than with federal.

In 1968, Congress enacted the Wiretap Act to establish a framework within which police would be permitted monitor telephone communications. In 1986, Congress revised the statute to include electronic communications, which is now known as the Electronic Communications Privacy Act (ECPA).[41] The ECPA applies not only to government monitoring of electronic communications, but also to monitoring by private parties. The ECPA generally prohibits anyone other than the sender and intended recipient of a message from intercepting it in transit, accessing it after it has been stored, or disclosing its contents. The ECPA restricts the ability of both government agents and private parties to monitor electronic communications. An important exception to the application of the ECPA exists where one of the parties to the communication has consented to the monitoring.[42] The scope of this exception for monitoring consented to by one of the parties to an electronic communication has recently been the subject of considerable controversy in the context of Internet commerce.

The Computer Fraud and Abuse Act (CFAA)[43] addresses unauthorized access and misuse of computers and computer networks. The CFAA prohibits various forms of unauthorized access of "protected computers." In 1996, the definition of "protected computer" was considerably expanded: now any unauthorized interference with a computer with access to the Internet may be a federal crime.[44] The CFAA prohibits unauthorized ac-

---

visited Aug. 18, 2005) (describing all the enforcement actions the FTC has taken against online businesses for failing to follow their posted privacy policies).

40. FTC v. Seismic Entm't Prods., Inc., No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004); Press Release, FTC, FTC Cracks Down On Spyware Operation, Oct. 12, 2004, *available at* http://www.ftc.gov/opa/2004/10/spyware.htm; In re Advertising.com, Inc., No. 042-3196 (F.T.C. filed Aug. 3, 2005) (proposed settlement); Press Release, FTC, Advertising.com Settles FTC Adware Charges, Aug. 3, 2005, *available at* http://www.ftc.gov/opa/2005/08/spyblast.htm.

41. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

42. 18 U.S.C. § 2511(3)(b) (2000).

43. *Id.* § 1030.

44. *Id.* § 1030(e)(2).

cess or exceeding authorized access to obtain information from a protected computer,[45] accessing a protected computer with intent to defraud or obtain anything of value,[46] or intentionally harming a protected computer.[47]

An in depth analysis of the application of the ECPA and the CFAA to the practices of adware distributors is beyond the scope of this article. However, some recent attempts to use these statutes as the basis for class action lawsuits based on allegations of online privacy violations indicate that their application to unwanted adware in particular may not prove to be very helpful.[48]

If the consumer could claim that unwanted adware running on a computer substantially interfered with the consumer's use of that computer, then it might be possible to make out a trespass to chattels claim.[49] Once again, while there is considerable uncertainty surrounding the scope of such a claim in light of conflicting case law, the trend in recent cases has been for courts to be more skeptical of such claims and to ask computer owners to tolerate more unwanted interference with the use of computers connected to the Internet.[50]

IV. REGULATORY ALTERNATIVES TO CONTRACT DOCTRINE

Because none of the obvious alternatives to liability for breach of contract seem any more likely to give consumers an effective legal remedy against the unwanted distribution of adware, many law reform proposals have been offered. Given that "unfair competition" is the body of law that

---

45. *Id.* § 1030(a)(2).

46. *Id.* § 1030(a)(4).

47. *Id.* § 1030(a)(5).

48. *In re* Doubleclick Privacy Litig., 154 F. Supp. 2d 497, 519-20 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1279-81 (C.D. Cal. 2001).

49. Trespass to chattels is defined as the unauthorized, intentional, and substantial use of or intermeddling with another's tangible personal property. RESTATEMENT (SECOND) OF TORTS §§ 217-218 (1965).

50. Trespass was found in Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003). No trespass was found in Ticketmaster Corp. v. Tickets.com, No. CV99-7654-HLH (VBKx), 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 6, 2003); Intel Corp. v. Hamidi, 1 Cal. Rptr. 3d 32 (Cal. Ct. App. 2003); Southwest Airlines Co. v. FareChase, Inc., 318 F. Supp. 2d 435 (N.D. Tex. 2004); Nautical Solutions Mktg. v. Boats.com, No. 8:02-cv-760-T-23TGW, 2004 U.S. Dist. LEXIS 6304 (M.D. Fla. Apr. 1, 2004).

addresses overzealous competition among merchants, perhaps what is needed is a new doctrine of "unfair marketing" that protects online consumers against overzealous marketing by online merchants. A claim of unfair marketing of adware might be defended by a showing that the adware company had clearly and explicitly disclosed to the consumer what the consumer would be giving up in exchange for whatever product or service the consumer intended to accept. In fact, that was more or less the approach taken in Congress in 2005 when H.R. 29, the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), was introduced.[51]

The SPY ACT's "notice and consent" approach[52] to dealing with unwanted adware appears to be drawn more from tort law than from contract law, which is consistent with an unfair competition approach. As a narrowly targeted response to the problem of unwanted adware, the SPY ACT may well have a material impact on the business models and software designs of legitimate adware distributors.[53] If the SPY ACT is characterized as a narrowly targeted reform of contract law, however, its likely impact will be much less positive. U.S. information privacy law is now in shambles after decades of narrowly focused, piecemeal legislation, and the notice and consent approach taken in various information privacy statutes has achieved only modest success.[54] Perhaps narrowly focused, piecemeal legislation to reform contract law is better than nothing it if can help stem the rising tide of spyware being loaded on consumers, but it is no substitute for a more general reappraisal of the current state of contract law as it applies to online transactions.

The 1993 EU Directive on Unfair Contract Terms provides an example of a more general reform of contract law that could provide consumers with effective legal remedies against unwanted adware distributed using

---

51. The 109th Congress SPY ACT is similar to the 108th SPY ACT that passed overwhelmingly in the House but stalled in the Senate. *Compare* H.R. 29, 109th Cong. (2005), *with* H.R. 2929, 108th Cong. (2004).

52. SPY ACT § 3 provides that it is unlawful to transmit an adware program to a computer or execute adware software on a computer unless the consumer is provided with a clear, explicit notice that personal information will be collected and provided an opportunity to consent to that function; the end user can easily identify the adware program and remove it, and when advertisements are displayed, the adware company is identified as the source of the ad.

53. By contrast, distributors of nefarious or fraudulent spyware are unlikely to be any more deterred by the SPY ACT than distributors of fraudulent spam e-mails have been deterred by the CAN-SPAM Act.

54. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 826-28 (2000) (discussing the shortcomings of the informed consent model of information privacy protection).

clickwrap interfaces.[55] The Directive provides that contract terms not individually negotiated will be deemed unfair if they create a significant imbalance, to the consumer's detriment, between the rights and obligations of the contracting parties.[56] If a contract term is drafted in advance and the consumer has no influence over the substance of the term, then it is always considered not to be individually negotiated, and hence subject to review based on substantive fairness.[57] An annex to the Directive contains an expansive list of terms that may be deemed unfair.[58] The nature of the goods

---

55. Council Directive 93/13/EEC, supra note 7. Member States were expected to pass laws implementing its provisions by the end of 1994. *See generally* James R. Maxeiner, *Standard-Terms Contracting in the Global Electronic Age: European Alternatives*, 28 YALE J. INT'L L. 109 (2003).

56. Council Directive 93/13/EEC, *supra* note 7, at art. 3.

57. *Id*. art. 2.

58. The terms listed in the annex include:

> (a) excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier;
>
> (b) inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations, including the option of offsetting a debt owed to the seller or supplier against any claim which the consumer may have against him;
>
> (c) making an agreement binding on the consumer whereas provision of services by the seller or supplier is subject to a condition whose realization depends on his own will alone;
>
> (d) permitting the seller or supplier to retain sums paid by the consumer where the latter decides not to conclude or perform the contract, without providing for the consumer to receive compensation of an equivalent amount from the seller or supplier where the latter is the party canceling the contract;
>
> (e) requiring any consumer who fails to fulfill his obligation to pay a disproportionately high sum in compensation;
>
> (f) authorizing the seller or supplier to dissolve the contract on a discretionary basis where the same facility is not granted to the consumer, or permitting the seller or supplier to retain the sums paid for services not yet supplied by him where it is the seller or supplier himself who dissolves the contract;
>
> (g) enabling the seller or supplier to terminate a contract of indeterminate duration without reasonable notice except where there are serious grounds for doing so;
>
> (h) automatically extending a contract of fixed duration where the consumer does not indicate otherwise, when the deadline fixed for the consumer to express this desire not to extend the contract is unreasonably early;

or services covered by the contract, the circumstances surrounding the drawing up of the contract, and the other terms in the contract or in another contract to which it relates will be taken into account in assessing the unfairness of a term.[59] Contract terms offered to consumers in writing must always be drafted in plain language and where there is doubt as to the meaning of a term, the interpretation most favorable to the consumer will prevail.[60] In the event that terms in a consumer contract are found to be unfair, those terms will not be binding on consumers, although the remainder of the contract will be enforceable.[61]

If unfair contract terms doctrine were applied to the practices of most U.S. adware distributors, a court in Europe could easily find that consumers were not provided with a real opportunity to learn the terms of the contract before being asked to agree to it. However, the list of unfair terms in

---

> (i) irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract;
> (j) enabling the seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract;
> (k) enabling the seller or supplier to alter unilaterally without a valid reason any characteristics of the product or service to be provided;
> (l) providing for the price of goods to be determined at the time of delivery or allowing a seller of goods or supplier of services to increase their price without in both cases giving the consumer the corresponding right to cancel the contract if the final price is too high in relation to the price agreed when the contract was concluded;
> (m) giving the seller or supplier the right to determine whether the goods or services supplied are in conformity with the contract, or giving him the exclusive right to interpret any term of the contract;
> (n) limiting the seller's or supplier's obligation to respect commitments undertaken by his agents or making his commitments subject to compliance with a particular formality;
> (o) obliging the consumer to fulfill all his obligations where the seller or supplier does not perform his;
> (p) giving the seller or supplier the possibility of transferring his rights and obligations under the contract, where this may serve to reduce the guarantees for the consumer, without the latter's agreement;
> (q) excluding or hindering the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to arbitration not covered by legal provisions, unduly restricting the evidence available to him or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract.

Id. Annex.

59. *Id.* art. 4.
60. *Id.* art. 5.
61. *Id.* art. 6.

the Annex to the Directive is merely suggestive and not in any way limiting. As a result, a court in Europe might also find that contract terms are unfair and thus unenforceable if they purport to permit a software distributor to load several software programs at once without clearly disclosing that more than one program is being loaded, or to load an adware program on a computer without clearly explaining its functions.

The Unfair Contract Terms Directive takes the opposite approach of current U.S. contract law: instead of a presumption of deference to whatever novel contract interface the merchant has developed, the Directive substitutes a presumption that the merchant will be bound to a contract based on the reasonable expectations of the consumer. Under such a standard for contract formation, it would be easy to predict that objectionable adware products would not be protected by click-through contract interfaces. American adware distributors that clearly and explicitly disclose their business models—which is all that proposed U.S. legislation such as the SPY ACT would require—might be surprised to learn that a court in Europe can refuse to enforce their contracts if the court determines that the business model itself is not fair to European consumers.

V. CONCLUSION

Adware distributors believe that consumers want the comparison advertisements they provide. Many others believe that such programs are simply another form of spyware, and that consumers would not accept such programs on their computers if adware distributors were required to disclose the purpose and functions of the software clearly and explicitly. If existing contract law doctrine regarding the formation of contracts were applied rigorously and consistently, then contract law might provide an effective mechanism for determining which description of reality is more accurate. However, whatever rigor and vitality applicable contract law doctrine might once have had is being eroded by the willingness of courts to accommodate with little critical scrutiny many innovations in contracting practices. As a result, courts reviewing the contracting interfaces used by adware distributors in light of current law are unlikely to demand that they make clear and explicit disclosures before claiming that consumers have consented to running their software.

Law reform efforts aimed at filling this apparent gap in contract doctrine appear narrowly targeted at problems associated with a particular technology—spyware—and so are unlikely to have any impact on the balance of power between merchant and consumer under contract law doctrine generally. This piecemeal, sectoral approach to the reform of contract

law is reminiscent of the U.S. approach to information privacy law, which has proved to be a dismal failure. One alternative to a narrowly targeted, ad hoc approach to controversies in contract law triggered by specific technological innovations would be to address the balance of power between merchant and consumer more generally, following the approach taken in the EU Unfair Contract Terms Directive. However, the pronounced U.S. proclivity for market-oriented rather than regulatory approaches to new commercial practices makes it very unlikely that such an approach would be tried in the U.S.

REGULATING "SPYWARE": THE LIMITATIONS OF STATE "LABORATORIES" AND THE CASE FOR FEDERAL PREEMPTION OF STATE UNFAIR COMPETITION LAWS

By Peter S. Menell†

ABSTRACT

Drawing on Justice Brandeis's oft-cited observation that states can serve as "laboratories" of policy experimentation, this Article develops a framework for assessing the allocation of governance authority for regulating Internet activities. In particular, it focuses on whether states should be free to experiment with regulatory approaches or whether the federal government should have principal, if not exclusive (preemptive), regulatory authority over Internet-related activities. Using recent efforts to regulate spyware and adware as a case study, the analysis shows that the lack of harmonization of, and uncertainty surrounding, state unfair competition law produces costly, confusing, multi-district litigation and pushes enterprises to adhere to the limits of the most restrictive state. Such a governance regime unduly hinders innovation in Internet business models. On this basis, the Article favors a uniform federal regulatory system and preemption of state statutes and unfair competition common law as applied to spyware and adware. The final section of the Article extrapolates from this study of spyware and adware regulation to the larger context of Internet governance.

TABLE OF CONTENTS

---

† Professor of Law, University of California at Berkeley School of Law (Boalt Hall), and Director, Berkeley Center for Law & Technology. From 2001 through 2003, I advised Claria Corporation (formerly The Gator Corporation) on intellectual property issues. The views expressed here are my own. I would like to thank Tom Cotter, Ben Edelman, Dan Farber, Eric Goldman, Mark Lemley, and Rob Merges for comments and Richard Ronald, Carol Johns, David Sanker, and Tom Fletcher for research assistance.

I. INTRODUCTION

Like many technological breakthroughs, the Internet has brought about great economic and social advancement, but not without some undesirable consequences. Cybersquatting,[1] computer viruses,[2] denial of service at-

1. Cybersquatting encompasses several problematic activities, most notably the registration of domain names based on the trademarks of others for purposes of diverting web surfers or extorting payments from the trademark holders. *See generally* P. Wayne Hale, *The Anticybersquatting Consumer Protection Act & Story's Farm L.L.C. v. Sportsman's Market, Inc.*, 16 BERKELEY TECH. L.J. 205 (2001); Ughetta Manzone, *Trademark: Domain Name: Dilution—Panavision International, L.P. v. Toeppen*, 13 BERKELEY TECH. L.J. 249 (1998).

2. *See* George Smith, *Billion-dollar Virus Economics*, THE REGISTER, Apr. 29, 2002, http://www.theregister.co.uk/2002/04/29/billiondollar_virus_economics; Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory*

tacks,[3] spam,[4] spIM,[5] phishing,[6] copyright infringement,[7] and spyware[8]

Proposal, 14 BERKELEY TECH. L.J. 839 (1999); Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177 (2000).

3. *See supra* note 2.

4. In its most expansive usage, spam refers to the sending of any unsolicited, inappropriate, or irrelevant messages through e-mail systems. It is often done on a mass scale and with a commercial purpose—such as attracting Internet users to websites offering pornography, "get rich" schemes, advertising, and fraudulent medical products. *See* Lily Zhang, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L.J. 301 (2005).

5. SpIM refers to the sending of unsolicited commercial messages through Instant Messaging systems. *See* Eric Zorn, *R U Ready For a Plague of Instant Messages?*, CHI. TRIB., August 5, 1999, at N1.

6. The term "phishing" refers to a form of identity theft. Phishing is the sending of e-mail messages falsely using the names of legitimate companies in order to entice recipients to visit fake webpages purporting to be operated by the company whose name is used in the message. The replica webpage solicits password, credit-card, or other private information. *See* Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259 (2005).

7. *See* Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models*, 22 CARDOZO ARTS & ENTM'T L.J. 725 (2005); Peter S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63 (2003).

8. The meaning and scope of the term "spyware" has evolved substantially over the past six years and is the subject of significant controversy. Prior to 1999, spyware referred to electronic surveillance equipment such as hidden cameras. *See* Sharon Wienbar, *The Spyware Inferno*, NEWS.COM, Aug. 13, 2004, http://news.com.com/The+spyware+inferno/2010-1032_3-5307831.html. Since 1999, "spyware" has been increasingly used to refer to interactive software programs that record and report Internet user activities. Some in the industry use the term rather broadly "to encompass everything from marketing cookies, pop-ups, and adware downloaded with peer-to-peer file-sharing programs to malicious Trojans and keystroke loggers designed to steal personal data." *See Business Strike Back at Spyware*, PCWORLD.COM, Aug. 16, 2004, http://www.pcworld.com/news/article/0,aid,117384,00.asp. Companies delivering pop-up advertisements with the consent of computer users oppose such a broad interpretation. These companies prefer the term "behavioral marketing" to describe their activities. Such software is also commonly referred to as "adware." A growing consensus believes that spyware should not extend to software that has been obtained with the knowledge and consent of users. *See* Federal Trade Commission, *Monitoring Software on your PC: Spyware, Adware, and Other Software* at 2-4 (Mar. 2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf [hereinafter FTC Spyware Report]. But what constitutes valid consent remains a point of heated disagreement in legal and policy fora. *See id*. at 3-4; Paul Festa, *See You Later, Anti-Gators?*, CNET NEWS.COM, Oct. 22, 2003, http://news.com.com/2100-1032_3-5095051.html (discussing false advertising and trade libel lawsuits brought by Gator Corporation against pop-up blocking software companies that had referred to Gator's products as "spyware").

have dispelled an earlier cyber-libertarian hope that the Internet could adequately be governed through code or social norms ("netiquette").[9] As the Internet has become an ever larger part of social, economic, and political life, various forces have pressed the courts, regulatory agencies (such as the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC)), and legislatures to address some of its undesirable effects. In some contexts, such efforts have worked relatively smoothly and effectively. For example, the World Intellectual Property Organization's (WIPO) Uniform Dispute Resolution Policy (UDRP), in conjunction with the Anticybersquatting Consumer Protection Act of 1999, has largely addressed concerns relating to cybersquatting. Technological fixes, enhanced security, and user vigilance have partially quelled the spread of computer viruses, although not without substantial cost.[10] By contrast, private, state, and federal initiatives have yet to control spam or phishing effectively[11] and efforts to prevent unauthorized distribution of copyrighted works on peer-to-peer networks have proven to be of only limited success.[12]

This conference focuses on the growing concern with the use of software Internet tools to gain access to personal information of web users. In some cases, such technology serves salutary or at least benign purposes. Increasingly, however, unscrupulous entities have used such software for

---

9. *See* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 178 (1997) ("For a long time, the Internet's enthusiasts have believed that it would be largely immune from state regulation."); David R. Johnson & David Post, *Law And Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); George Black, *Call for Controls: The Internet Must Regulate Itself*, FIN. TIMES., Apr 1, 1998, pt. 4, at 12; Vinton G. Cerf, *Building an Internet Free of Barriers*, N.Y. TIMES, July 27, 1997, § 3, at 12; Thomas E. Weber, *The Internet (A Special Report): Debate: Does Anything Go? Limiting Free Speech on the Net*, WALL ST. J., Dec. 8, 1997. *But cf.* Jack Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257 (1998).

10. Robert Lemos, *Melissa's Long Gone, But Lessons Remain*, CNET NEWS.COM, Mar. 29, 2005, http://news.com.com/Melissas+long+gone%2C+but+lessons+remain/2100-7349_3-5643900.html; Kevin P. Kalinich & Kristina McGrath, *Identifying and Evaluating the Business Impact of Network Risks and Liabilities*, 33 W.T.R. Brief 18 (Winter 2004); FTC, SAFE AT ANY SPEED: HOW TO STAY SAFE ONLINE IF YOU USE HIGH-SPEED INTERNET ACCESS (Sept. 2002), *available at* http://www.ftc.gov/bcp/conline/pubs/online/safeonline.pdf.

11. *See* Lynch, *supra* note 6.

12. *See generally* Kristina Groennings, *Costs and Benefits of the Recording Industry's Litigation Against Individuals*, 20 BERKELEY TECH. L.J. 571 (2005); Hughes, *supra* note 7; Menell, *supra* note 7.

fraudulent and pernicious ends.[13] Spyware often operates in conjunction with other software that delivers advertisements (such as pop-up windows), harvests private information, or re-routes web traffic. Recent studies reveal that as many as ninety percent of home computers in the United States as well as many business computers are running automated programs that report users' personal information, many without the users' knowledge or consent.[14] Such software can slow intended computer processing, hijack storage capacity, distract computer users, and potentially lead to identity theft and other serious crimes.[15] The total cost to Internet users of such software—in terms of harm from misuse of personal information, lost productivity, computer repair, and installation of protective software—is large and growing.[16] Many consumers are unaware that spyware is running on their computers and mistakenly believe that their computers are malfunctioning. Even when computer users become aware of spyware, they often encounter difficulty deactivating or removing it.[17]

---

13. *See* Robert Lemos, *Pop-up Program Reads Keystrokes, Steals Passwords*, CNET NEWS.COM, Jun. 29, 2004, http://news.com.com/Pop-up+program+reads+keystrokes%2C+steals+passwords/2100-7349_3-5251981.html (describing software that can monitor a user's keystrokes when visiting various bank websites).

14. *See* John Borland, *Dell Backs Spyware Education Drive*, CNET NEWS.COM, Oct. 15, 2004, http://news.com.com/Dell+backs+spyware+education+drive/2100-1032_3-5410568.html (reporting findings of report from the Consumer Spyware Initiative, a joint project sponsored by Dell Computer and the Internet Education Foundation); John Borland, *Spike in "Spyware" Accelerates Arms Race*, CNET NEWS.COM, Feb. 24, 2003, http://news.com.com/A+secret+war/2009-1023_3-985524.html?tag=st.rn.

15. *See* Dan Ilett, *Worst Spyware Queues Up*, CNET NEWS.COM, Dec. 21, 2004, http://news.com.com/Worst+spyware+queues+up/2100-7349_3-5499609.html (quoting an anti-spyware executive characterizing CoolWebSearch as "probably one of the most vicious programs in terms of how nasty it is. It completely hijacks the browser so you can't do anything.").

16. *See* Declan McCullagh, *Few Solutions Pop Up at FTC Adware Workshop*, CNET NEWS.COM, Apr. 19, 2004, http://news.com.com/Few+solutions+pop+up+at+FTC+adware+workshop/2100-1028_3-5195222.html (noting that spyware concerns have become the leading support problem for computer vendors and computer security companies); Stefanie Olsen, *Revenge of the Pop-ups*, CNET NEWS.COM, Oct. 14, 2004, http://news.com.com/Revenge+of+the+pop-ups/2100-1024_3-5408453.html (characterizing the interplay between browser providers, who seek to block pop-up advertisements, and adware purveyors as a "cat-and-mouse game" in which one side continues to improve its blocking technology and content developers are constantly developing a way to get around the pop-up blockers).

17. *See* Ilett, *supra* note 15 (noting that spyware distributors "are gaining sophistication in their coding practices, as they attempt to evade detection and removal"); Stefanie Olsen, *Google Feels Spyware Strains*, CNET NEWS.COM, Jul. 28, 2004, http://news.com.com/Google+feels+spyware+strains/2100-1024_3-5250383.html (describing software programs that reinstall even after a user removes it from their computer's

Regulating spyware is complicated by the fact that some programs that automatically report personal information can offer benefits to consumers, advertisers, and web publishers by improving the targeting of advertising "vehicles."[18] Emerging "behavioral marketing" software-based business models[19] can be characterized as a more sophisticated form of traditional advertising—another business activity that has encountered adverse reactions over the years, but has become an accepted part of the free enterprise system.[20] Even this activity, however, is subject to a range of regulatory constraints.[21]

Advertising continues to support in whole or in part a large portion of the major entertainment and news media channels. Newspapers, magazines, television, radio, and Internet portals rely in varying degrees upon advertiser support to fund and disseminate content.[22] In at least some contexts, consumers value the advertisements themselves—for product or service information or, occasionally, for entertainment value. In many of

---

registry). Some programs claiming to eliminate spyware actually install other forms of advertising software. *See* John Borland, *Spyware Cures May Cause More Harm than Good*, CNET NEWS.COM, Feb. 4, 2004, http://news.com.com/Spyware+cures+may+cause+more+harm+than+good/2100-1032_3-5153485.html.

18. "The line between adware and spyware is fuzzy. But even critics of WhenU and Claria concede that those companies' practices are nowhere near as objectionable as malevolent ware that surreptitiously infects a PC and uses it to send out spam or divulges a user's credit card numbers." Declan McCullagh, *Adware's Going Mainstream, Report Says*, CNET NEWS.COM, Jun. 30, 2004, http://news.com.com/Adwares+going+mainstream%2C+report+says/2100-1024_3-5253029.html; *see also* Stefanie Olsen, *Catfight in the Spyware Corral*, CNET NEWS.COM, Feb. 8, 2005, http://news.com.com/Catfight+in+the+spyware+corral/2100-1032_3-5567781.html (observing that "[w]hile clear examples of legitimate and illegitimate behavior are easy to find, drawing a bright line between them has proven to be extremely difficult").

19. *See, e.g.*, D. Reed Freeman, Jr., *Privacy and the Future of Behavioral Marketing*, http://www.claria.com/advertise/oas_archive/privacy.html?pub=imedia_module (written by the Chief Privacy Officer for Claria Corporation).

20. *See* Charles K. Ramond, *How Advertising Became Respectable*, 28 J. MKTG. 1 (1964); *cf.* Ralph S. Brown, Jr., *Advertising and the Public Interest: Legal Protection of Trade Symbols*, 57 YALE L.J. 1165 (1948).

21. *See* PETER S. MENELL & SUZANNE SCOTCHMER, *Intellectual Property*, *in* HANDBOOK OF LAW AND ECONOMICS (A. Mitchell Polinsky & Steven Shavell eds., forthcoming 2005) (discussing the range of private and public institutions governing advertising).

22. *See* HAROLD L. VOGEL, ENTERTAINMENT INDUSTRY ECONOMICS: A GUIDE FOR FINANCIAL ANALYSIS 229 (6th ed. 2004) (characterizing television and radio programs as "scheduled interruptions of marketing bulletins").

these market settings, however, consumers would prefer to receive content without the advertising.[23]

The traditional advertising model embodies a technological constraint of mass communication media—messages cannot be tailored to individual consumers. Rather, advertisers are constrained in targeting their advertisements to the distribution of demographic characteristics of consumers of particular newspapers, magazines, or broadcast media. For example, Nielsen Media Research can describe the range of television viewers for particular shows based on its surveys of families. But advertisements for traditional television programming cannot be targeted on a per viewer basis. The medium of traditional television distributes the same advertisement to all viewers in a particular market.[24] For this reason, makers of feminine hygiene products do not purchase advertising for football games because such programming appeals primarily to men. But women interested in feminine hygiene products surely watch football games, just as men watch some programming of particular interest to women. If advertisers could more accurately and easily reach better defined market segments, or ideally particular individuals, advertisers, consumers, and broadcasters would stand to gain. Advertisers would be willing to pay more in order to reach consumers in the market for particular classes of goods, and consumers would not have to endure nearly as much irrelevant advertising per hour of programming for broadcasters to be able to support such content. In addition, consumers would be more likely to gain valuable information through advertising.[25]

---

23. "It's a no-brainer that skipping commercials is one of the attractive features of a personal video recorder like TiVo or Sonicblue's ReplayTV." Katie Dean, *TiVo Loath to Admit Ad Skip Trick*, WIRED, Jan. 14, 2003, http://www.wired.com/news/digiwood/0,1412,57178,00.html. ReplayTV's commercial skipping and file sharing capability led to contributory copyright infringement lawsuits by content owners and televisions networks which eventually pushed the company into bankruptcy. *See* Katie Dean, *Bankruptcy Blues for PVR Maker*, WIRED, Mar. 24, 2003, http://www.wired.com/news/digiwood/0,1412,58160,00.html.

24. *See* Lorne Manly, *The Future of the 30-Second Spot*, N.Y. TIMES, Mar. 27, 2005, § 3, at 1 ("The television commercial—a blunt instrument that often reaches as many disinterested people as desired ones—is beginning to behave like a smarter version of direct mail."). As information technology advances, broadcasters hope to be able to better target and customize advertising. *See* Janet Whitman, *In the Crosshair—Viewers and Target Ads*, DOW JONES NEWSWIRE, Oct. 25, 2004, *available at* http://medialit.med.sc.edu/crosshairs.htm (predicting that advertisers will soon be able to deliver television ads customized for individual households).

25. *See* P. Nelson, *Advertising as Information*, 82 J. POL. ECON. 729 (1974); P. Nelson, *The Economic Consequences of Advertising*, 48 J. BUS. 213 (1975); George J. Stigler, *The Economics of Information*, 69 J. POL. ECON. 213 (1961).

Behavioral marketing technology represents a quantum leap in the ability of advertisers to reach desired market segments at relatively low cost. Even limited and anonymous information about the class of goods that an Internet user seeks enables advertisers to provide highly relevant information. For example, a consumer who types "office supplies" into a search engine is likely in the market for office products. Such consumers would likely be receptive to getting advertisements, discount coupons, or other targeted marketing information about office supplies at that time. For this reason, behavioral marketing software yields relatively high "click through" rates—the percentage of consumers clicking on advertisements to learn more about what is being offered—than randomly targeted pop-up advertisements.[26] Such high click-through rates translate, at least roughly, into higher sales and brand recognition. Thus, behavioral marketing technology can enable advertisers to reach consumers much more effectively and efficiently.[27]

The use of such technology, however, raises numerous legal and policy questions relating to information privacy and adequacy of consent to load software onto a user's computer and monitor their web-searching activity. It may also violate intellectual property rights: Does using a competitor's trademark to trigger an advertisement infringe trademark rights? Does delivering a pop-up window over the webpage of another company implicate copyright law? Is alerting Internet users querying a particular manufacturer's trademark or URL to a competitor's website or discount offer a form of unfair competition? Unlike most of the other papers prepared for this conference, this Article does not seek to determine the optimal type of regulation to address spyware concerns.[28] Rather, it analyzes

---

26. The effects of behavioral advertising on click-through rates for pop-up advertisements and actual purchasing behavior are speculative. One behavioral advertising company reports remarkable success in a campaign for a high-end cosmetics company targeting affluent, beauty-conscious mothers, achieving click-through rates of 24 percent, compared with the industry average of roughly 0.2 percent for general pop-up ads and roughly 0.01 percent for banners. *See* Rachel Konrad, *Reality Check: Does Adware Work?*, CNET NEWS.COM, June 26, 2002, http://news.com.com/Reality+check+Does+adware+work/2009-1023_3-938263.html; Adam L. Penenberg, *Ads That Annoy Also Succeed*, WIRED, Sept. 8, 2004, *available at* http://www.wired.com/news/business/0,1367,64807,00.html (quoting an interactive advertising professional: "Pop-ups generate roughly 5 to 10 times the response rate of standard banner units" because "people are more apt to notice them").

27. Online advertising revenue surpassed $8.4 billion in 2004 and is expected to exceed advertising spending in print magazines in the near future. *See* Penenberg, *supra* note 26.

28. *See generally* Kristen M. Beystehner, *See Ya Later, Gator: Assessing Whether Placing Pop-Up Advertisements on Another Company's Website Violates Trademark*

the proper jurisdiction or governmental level for regulating such technology and activities. In particular, it focuses on whether state unfair competition law should regulate the use of spyware, or whether federal law should preempt such laws.[29]

At first blush, the use of decentralized state unfair competition law and specific legislation to regulate spyware might seem to be a natural application of Justice Brandeis's metaphorical observation that states can provide valuable "laboratories" of experimentation and innovation in areas of government policy where there may be disagreement about the best course of action. "It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[30] As this paper explains, however, state experimentation in regulating Internet-related activities creates significant risks for the nation as a whole. Due to the ubiquity of the Internet and the relatively low threshold

---

Law, 11 J. INTELL. PROP. L. 87 (2003); Michael A. Leon, *Unauthorized Pop-Up Advertising and the Copyright and Unfair Competition Implications*, 32 HOFSTRA L. REV. 953 (2004).

29. Most prior scholarship touching on federalism issues and the Internet have focused on jurisdiction and more abstract issues of governance. *See* Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 323 (2002); Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095 (1996); Goldsmith, *supra* note 9; Johnson & Post, *supra* note 9; Joel R. Reidenberg, *Governing Networks and Rule-making in Cyberspace*, 45 EMORY L.J. 911 (1996). Professor Burk's article does suggest that the dormant Commerce Clause doctrine, a judge-made rule that prohibits states from burdening interstate commerce through the enactment of state or local regulations, provides a useful means of preventing fragmented and uncoordinated governance. *See* Burk, *supra*, at 1123-34. Professors Goldsmith and Sykes question the application of the dormant Commerce Clause doctrine to Internet activity. *See* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785 (2001). This Article confronts this debate in the context of spyware regulation.

30. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting); *see also* Charles Fried, *Federalism—Why Should We Care?*, 6 HARV. J.L. & PUB. POL'Y 1, 2-3 (1982) (arguing that decentralized political power leads to innovation). Justice Brandeis's "laboratory" metaphor is often invoked in case law and academic writing about federalism. *See, e.g.*, Lucian Arye Bebchuck, *Federalism and the Corporation: The Desirable Limits on State Competition in Corporate Law*, 105 HARV. L. REV. 1435 (1992); Richard W. Garnett, *The New Federalism, The Spending Power, and Federal Criminal Law*, 89 CORNELL L. REV. 1, 18 (2003); Lewis B. Kaden, *Politics, Money and State Sovereignty: The Judicial Role*, 79 COLUM. L. REV. 847, 853-55 (1979); Deborah Jones Merritt, *The Guarantee Clause and State Autonomy: Federalism for a Third Century*, 88 COLUM. L. REV. 1, 3-10 (1988); Eric Lamond Robinson, *The Oregon Basic Health Services Act: A Model for State Reform*, 45 VAND. L. REV. 977, 986-88 (1992); Roberta Romano, *The State Competition Debate in Corporate Law*, 8 CARDOZO L. REV. 709 (1987).

for personal jurisdiction,[31] state-by-state regulation creates an environment in which prudent Internet-related businesses must conform to every state unfair competition law, producing in effect a national policy based on the standards of the most restrictive state. In effect, the least common denominator predominates in the context of Internet governance, thereby nullifying the experimentation that Brandeis praised.[32] Given the uncertain contours of state unfair competition law, a federal preemptive regulatory approach provides a better climate than decentralized state regimes for both regulating spyware and encouraging business and software innovation.

This Article begins by developing a framework for assessing the allocation of governance authority for regulating Internet activities. Part II focuses on whether states should be free to experiment with regulatory approaches or whether the federal government should have principal, if not exclusive (preemptive), regulatory authority over Internet-related activities. Part III examines the experience thus far in addressing the legality of behavioral marketing under federal and state unfair competition law. Using litigation pertaining to behavioral advertising companies as a case study, Part III also shows that the lack of harmonization of, and uncertainty surrounding, state unfair competition law produces costly, confusing, multi-district litigation and pushes enterprises to adhere to the limits of the most restrictive state. Such a governance regime unduly hinders innovation in Internet business models. A uniform federal regulatory system would offer substantial advantages without jeopardizing consumer protection or fair business competition. Part IV reviews federal initiatives aimed at addressing spyware concerns. The concluding Part extrapolates from this study of spyware regulation to the larger context of Internet governance.

II. FEDERALISM, REGULATORY LABORATORIES, AND REGULATION OF INTERNET ACTIVITIES

Justice Brandeis's metaphor of states serving as "laboratories" of regulatory experimentation and innovation has long intrigued legal and policy analysts. Public policy is an empirically driven social science. Theoretical

---

31. *See generally* Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1352 (2001); Dennis T. Yokoyama, *You Can't Always Use the Zippo Code: The Fallacy of a Uniform Theory of Internet Personal Jurisdiction*, 54 DEPAUL L. REV. 1147 (2005).

32. I do not mean to question the value of policy experimentation, but to recognize that interstate experimentation can occur most effectively where activities do not cross state boundaries or have interstate impacts—as in the case of local zoning regulation.

models can rarely, if ever, predict perfectly the outcomes of government policy. What works in theory does not always work in the real world. Policy initiatives often produce unintended consequences. Therefore, experimentation plays a vital role in assessing the efficacy of alternative policies, and the notion that states can serve this function resonates with deeply ingrained federalist political values at the core of American democratic institutions. Furthermore, heterogeneity among jurisdictions in terms of geography, demographics, economic infrastructure, and social values may well favor non-uniform policies attuned to local characteristics.[33]

Nonetheless, decentralized public policymaking as well as non-uniform standards can produce undesirable effects, especially where activities cross state boundaries. Interstate commerce serves as a principal justification for national policy trumping state law. Interstate externalities and spillovers also justify national, or at least, regional decisionmaking authority.[34] Conflicting standards can result in the most restrictive regimes trumping more permissive approaches. Such concerns arise with particular force in the context of the Internet—which spans all states (and nationalities).

Before turning to the analysis of the proper jurisdictional authority over spyware regulation, it is useful to develop a general framework for analyzing federalism. In particular, it will be useful to understand those conditions under which Brandeis's "states as laboratories of experimentation and innovation" model holds, and the circumstances under which a national preemptive regime is most efficacious. Although much has been written on federalism in various contexts, few scholars have analyzed the proper allocation of decisionmaking authority with respect to Internet governance.

A. Federalism and Laboratories of Innovation: General Considerations

Justice Brandeis's metaphor draws upon a fundamental and powerful method of modern science—the idea of controlled experimentation. Sci-

33. *See* Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416 (1956) (proposing a model for calculating "the level of expenditures for local public goods which reflects the preferences of the population more adequately than they can be reflected at the national level").

34. *See* Daniel C. Esty, *Revitalizing Environmental Federalism*, 95 MICH. L. REV. 570 (1996); Richard B. Stewart, *Pyramids of Sacrifice? Problems of Federalism in Mandating State Implementation of National Environmental Policy*, 86 YALE L.J. 1196 (1977); Richard O. Zerbe, *Optimal Environmental Jurisdictions*, 4 ECOLOGY L.Q. 193 (1974). *But cf.* Richard L. Revesz, *Federalism and Environmental Regulation: A Public Choice Analysis*, 115 HARV. L. REV. 553 (2001).

ence seeks understanding of the operation of general laws governing the physical world. Understanding of these laws can be gleaned and refined through systematic experimentation. Essential to such testing—and the scientific method more generally—is the use of controlled environments in which particular variables can be examined individually and systematically.

In extrapolating from the scientific laboratory setting to public policy experimentation, Justice Brandeis presumed that each state could be viewed as a controlled and isolated laboratory environment—"[i]t is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[35] In this way, the differing policies of the states could be examined essentially as independent experiments, producing valid, independent data for assessing alternative policies.[36] For various areas of policy, states can be treated as isolated environments. For example, land use policies, at least in non-interstate border areas, tend to have predominantly local effects and do not produce significant out-of-state spillovers. Therefore, policy "experiments" can be implemented and studied in isolation.[37] In fact, land use has long been viewed as an area in which local authority remains paramount.[38] Other policies—such as welfare benefits, property and casualty insurance, local election law, and some aspects of health care—may also be confined within state boundaries. Outside of land use, we see varying patterns of local, state, and national governance.

As a general theory of the role of states in a federal system, Justice Brandeis's metaphor overlooks two essential aspects of the scientific method—the need for uncontaminated (truly isolated) laboratories and identical starting conditions. For purposes of analyzing Internet policy, the

---

35. *New State Ice Co.*, 285 U.S. at 311.

36. The state policy in question in *New State Ice Co*. concerned regulation of the ice industry. At this relatively early stage in the development of refrigeration technology, ice was generally manufactured in factories and distributed to households. Justice Brandeis believed that allowing some experimentation in the regulation of such businesses could produce valuable information. *See id.* Given the inherently local scale of ice manufacturing and distribution at the time, there is little reason to believe that state experiments would have significant interstate effects.

37. Even land use policies can distort out-of-state communities to the extent that they influence interstate commerce.

38. But even here, national interests can trump local autonomy, as in the case of some aspects of wildlife law (migratory birds and endangered species) and habitat protection. *See generally* DALE D. GOBLE & ERIC T. FREYFOGLE, WILDLIFE LAW 831-1099, 1164-1349 (2002).

first issue is most pertinent. Unlike land use—which is stationary and inherently bounded by geographic limitations—and some aspects of social welfare policy, the Internet transcends the borders of any state. Hence, any state-specific policy experiment will inevitably taint the "laboratories" of other states to the extent that Internet activities are subject to regulation in that state. In so doing, they present risks to the nation as a whole.

B. Federalism and Internet Policy

The ubiquity of the Internet contradicts the premise that states can experiment with regulatory policies without distorting activities outside of their borders—thereby posing "risk to the rest of the country." The inherent architecture of the Internet—which makes it difficult if not impossible to restrict Internet access to one or several states[39]—in combination with the relatively liberal rules of personal jurisdiction[40] means that most substantial Internet-based commercial activities are subject to liability in many, if not all, of the fifty states. Consequently, decisions by businesses about use of the Internet are governed, to a significant extent, by the liability standards of every state. Prudent businesses conducting commerce on the Internet must evaluate their potential exposure based on the laws of all 50 states. In seeking to avoid liability exposure, such businesses will conform their practices to the standards set by the most restrictive state, producing what might be called a "least common denominator" approach to due diligence.

Without federal preemption of state law, the "net" effect of state regulation of Internet activities will therefore be an unintended form of national regulation in which the standards of the most restrictive state become de facto national standards, at least for businesses having a substantial web presence. Rather than promoting experimentation, state regulation

---

39. The Internet's "end-to-end" infrastructure enables the transmission of information among geographically independent end points. *See generally* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930-34 (2001); J.H. Saltzer et al., End-to-End Arguments in System Design, Second International Conference on Distributed Computing Systems 509-512 (Apr. 8, 1981), *reprinted in* INNOVATIONS IN INTERNETWORKING 195-206 (Craig Partridge ed., 1988), *available at* http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf. In some contexts, it is possible to restrict Internet communication on the basis of geographic criteria, but such technologies impose costs that may be wasteful. *See* Goldsmith & Sykes, *supra* note 29, at 809-13 (noting that websites can use registration and customer profiles); Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951 (2005) (suggesting that innovations in information technology may afford states greater ability to enforce their regulatory policies electronically).

40. *See supra* note 31; Reidenberg, *supra* note 39.

left unchecked will contaminate laboratories in other states and inhibit federal regulatory initiatives. Therefore, the characteristics of the Internet favor federal preemption of state regulation as the most appropriate default regime. Uncoordinated and diverse state laws will produce a legal environment in which the most restrictive state laws dominate Internet business activities. Thus, Justice Brandeis's "state laboratories" theory of federalism does not apply well to the Internet—a medium that does not and cannot effectively be confined to state boundaries. The effects of state experimentation cannot be cabined within state boundaries, and therefore will present "risk to the rest of the country."

There may well be other justifications for decentralized decisionmaking authority with regard to Internet activities. Differential capture of political actors as between the state and federal levels could, in theory, favor decentralized governance. Concerns about excessive rigidity at the federal level prematurely cutting off policy experimentation at the state level could also favor a federal governance regime. Neither theory, however, seems likely to apply to Internet regulation.

1. Capture Theory

Capture theory derives from the "public choice" branch of political science, which analogizes political decisionmaking to market transactions.[41] Within this framework, legislation emerges from the interaction of interest groups which form the demand side of the market and legislators who form the supply side of the market. Interest groups seek to influence legislators through campaign contributions and other lobbying activities. Those groups which are best mobilized—typically because they stand to gain concentrated benefits or bear concentrated costs as a result of government policy—tend to have more influence than potentially large but diffuse constituencies. Polluting industries, for example, tend to have strong incentives to dissuade legislators from imposing strict and costly pollution controls even where many individuals might stand to gain more collectively, but relatively little individually. The latter face substantial transaction costs in organizing due to the free-rider problem, whereas the former are fewer in number and have much to gain individually as well as collectively, making political mobilization more likely.

This framework has been extended to analysis of federalism in the following manner. To the extent that federal or state legislators are more

41. *See* William Eskridge, Jr., *Politics Without Romance: Implications of Public Choice Theory for Statutory Interpretation*, 74 VA. L. REV. 275, 285-88 (1988); JAMES BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT (1962); MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS (1971).

prone to capture, legislation from such a governmental level is more suspect and should be subject to greater scrutiny. To the extent such differential capture may occur, however, it favors federal preemption of state standards.[42] Adherents worry that states are more prone to capture than the federal government due to the higher costs of organizing at the state level (due to the multiplicity of states) and economies of scale in organizing at the federal level.[43] Many environmental advocates worry that only national standards will provide adequate protection for public health and ecology. Inadequate standards in any one state jeopardize these values.

The technological characteristics of the Internet and the distinctive array of interests affected by its regulation create different conditions for analyzing the optimal allocation of governance responsibilities in a federal system. The ubiquity of the Internet and the inability to constrain Internet activities within state boundaries means that interest groups seeking stringent regulation need only capture the legislature of one state in order to have far-reaching effects. Unlike many environmental effects, which tend to be localized, Internet activities are global. Stringent regulation in any one state potentially constrains activities on a global scale.

The analysis of Internet regulation on behavioral marketing is somewhat more complex due to the multiplicity of business interests. The battle appears to be between traditional web publishers[44] and emerging behavioral marketing companies.[45] As in the environmental area, consumer interests tend to be more diffuse, although various consumer-oriented interest groups have formed around Internet and online privacy issues.[46] It is

---

42. *See, e.g.*, Esty, *supra* note 34; Stewart, *supra* note 34. *But see* Revesz, *supra* note 34.

43. *See* Esty, *supra* note 34, at 597-98 (arguing that "asymmetries [among interest groups] may be more significant at the state and local levels" than the federal level); Stewart, *supra* note 34, at 1213 ("In order to have effective influence with respect to state and local decisions, environmental interests would be required to organize on a multiple basis, incurring overwhelming transaction costs. Given such barriers, environmental interests can exert far more leverage by organizing into one or a few units at the national level.").

44. The Interactive Advertising Bureau (IAB) represents companies that sell interactive advertising such as web publishers—companies that deliver banner and other advertisements to visitors of their websites. *See* Stefanie Olsen, *Chorus of Gator Critics Grows*, CNET NEWS.COM, Aug. 27, 2001, http://news.com.com/Chorus+of+Gator+critics+grows/2100-1023_3-272244.html.

45. *See infra* text accompanying note 139.

46. Organizations mobilized around these issues include: Center for Democracy and Technology (CDT), Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center (EPIC). *See* CDT, Spyware, http://www.cdt.org/privacy/spyware (last visited Aug. 27, 2005); Posting of Wendy Seltzer to Deeplinks, http://www.eff.org/

not at all clear that federal preemption would clearly favor one constituency or another relative to state regulation, although the recent enactment of broad spyware legislation in Utah illustrates the sway even one or a few companies can have in state legislative decisionmaking.[47] In a non-preemption regime, over-regulation by even one state could have distortionary effects on business activity throughout the nation.

2. Excessive Federal Rigidity

The concern about excessive rigidity at the federal level prematurely cutting off policy experimentation at the state level overlooks the inherent nature of the Internet. As noted earlier, state policy experimentation on the Internet will tend to act as a one-way ratchet. Stricter rules in any state will be seen by prudent businesses effectively as national standards unless they can effectuate different web functionality on a state-by-state basis. Therefore, the excessive rigidity problem will be present to the extent that any state implements more restrictive policies.

At least on theoretical grounds, therefore, the case for federal preemption of state regulation of Internet activities appears quite strong.[48] The emergence of behavioral marketing business models provides a natural experiment of how one form of state law—unfair competition—has affected Internet entrepreneurship and the extent to which differential state law standards affect Internet business decisionmaking. Over the past four years, the two most prominent pioneers in the use of behavioral marketing technology—Gator (now Claria) and WhenU—have faced a barrage of lawsuits alleging violations of federal and state laws. A review of this experience suggests that the lack of harmonization of, and uncertainty surrounding, state unfair competition law produces costly, confusing, multi-

---

deeplinks/archives/003536.php (Apr. 28, 2005, 01:54 PM); http://www.epic.org (last visited Aug. 27, 2005). A researcher formerly associated with the Berkman Center for Internet and Society has long followed spyware and adware issues and served an active advocacy role. *See* Benjamin Edelman, http://www.benedelman.org (last visited Aug. 27, 2005).

47. *See infra* text accompanying note 208.

48. The above analysis does not imply that states should have no role in Internet governance, only that standard setting should be done at the federal level. States could play a complementary role in enforcing such standards. *Cf.* Michael Gormley, *Will Spyware Be Spitzer's Next Big Thing?*, MSNBC, May 7, 2005, http://www.msnbc.msn.com/id/6448213/did/7753583 (reporting that Eliot Spitzer, New York's maverick Attorney General, has been investigating spyware for some time now and may expand his office's enforcement efforts into this area); Seltzer, *supra* note 46. State agencies may be better situated to enforce Internet standards by virtue of having better access to victims and knowledge about local businesses. As in other areas of joint enforcement, there would be some benefits to coordination with federal authorities and state officials.

district litigation and pushes enterprises to adhere to the limits of the most restrictive state. Furthermore, the enactment of specialized legislation addressing spyware in one state (Utah) indicates that state legislatures may be prone to capture by unrepresentative political interests.[49] Thus, multiple, conflicting state regimes governing the Internet may well discourage innovation in Internet business models by creating a gauntlet of legal costs and exposure—both in business planning and implementation. A uniform federal regulatory system would offer substantial advantages without jeopardizing consumer protection or fair business competition.

III. A CASE STUDY OF THE APPLICATION OF STATE UNFAIR COMPETITION LAW TO BEHAVIORAL MARKETING BUSINESS MODELS

The emerging area of behavioral marketing provides a useful context for testing the effects of state regulatory regimes on Internet business models and activities. The interactivity of the Internet, in combination with advances in software and database technology, has enabled new forms of advertising that were never before feasible on a wide scale. Behavioral marketing uses automated software agents to deliver advertisements based on the web-surfing behavior of Internet users. At the same time, such technologies can be used in unscrupulous ways—ranging from delivering unwanted pop-up advertisements without the consent of the computer user to monitoring a user's keystrokes as part of an identity theft scheme. Drawing the appropriate regulatory lines to police such activities without choking off potentially beneficial business models requires some care. This Article focuses on how regulatory authority should be allocated between the state and federal levels to achieve an appropriate balance. The working hypothesis, traced in Part II, is that a mixed or decentralized (non-preemptive) governance regime will push the effective governance regime to the standards of the most restrictive state.

In order to assess this hypothesis, we need to understand the existing legal landscape. The free enterprise system generally eschews regulation of business activities unless some market failure arises. But even here, direct government regulation is usually a last resort. Legislators and regulatory agencies will typically allow general background legal rules—often in the form of evolving common law regimes and existing statutes—to play out before taking action. In the case of spyware, several bodies of background rules arguably govern: copyright, trademark, consumer protection, and unfair competition law. For a variety of reasons, copyright is already

49. *See infra* text accompanying note 210.

governed almost exclusively by federal law[50] and therefore does not require further consideration here.[51] Trademark, consumer protection, and unfair competition law have both state and federal counterparts. These areas have evolved together within the rubric of unfair competition law.

This section begins by tracing the evolution and contours of unfair competition law. It then examines how the current legal regime—mixed federal and state law governance—has affected the early entrants into the field of behavioral marketing and assesses whether the least common denominator hypothesis governs Internet-related activities in this particular setting.

A. The Landscape of Unfair Competition Law

For a variety of historical and jurisprudential reasons, unfair competition has long been one of the most amorphous bodies of common law. As Judge Learned Hand observed 80 years ago, "[t]here is no part of the law which is more plastic than unfair competition, and what was not reckoned an actionable wrong 25 years ago may have become such today."[52] In 1959, Judge Medina lamented the lack of harmonization among state common law unfair competition jurisprudence and expressed the hope that "[s]ince most cases involve interstate transactions, perhaps some day the much needed federal statute or uniform laws on unfair competition will be passed."[53] These observations could just as easily be made today. The continuing rudderless quality of state unfair competition common law has only been exacerbated by the spate of differing state unfair competition statutes enacted in the 1960s and 1970s.

A comprehensive delineation of the contours of unfair competition law would require treatise-length coverage[54] and extend well beyond the task

---

50. *See* 17 U.S.C. § 301 (2005). *See generally* 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 1.01 (2005).

51. All of the cases that addressed copyright allegations have ruled that pop-up advertisements do not implicate website owners' display right or right to create derivative works. *See* 1-800 Contacts, Inc. v. WhenU.com, Inc., 309 F. Supp. 2d 467, 484-88 (S.D.N.Y. 2003); Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734, 769-71 (E.D. Mich. 2003); U-Haul Int'l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723, 729-31 (E.D. Va. 2003); *cf.* Aaron Rubin, *Are You Experienced? The Copyright Implications of Web Site Modification Technology*, 89 CALIF. L. REV. 817 (2001).

52. Ely-Norris Safe Co. v. Mosler Safe Co., 7 F.2d 603, 604 (2d Cir. 1925), *rev'd on other grounds*, 273 U.S. 132 (1927).

53. Am. Safety Table Co. v. Schreiber, 269 F.2d 255, 271 (2d Cir. 1959).

54. *See generally* RUDOLPH CALLMANN, CALLMANN ON UNFAIR COMPETITION, TRADEMARK, AND MONOPOLIES (4th ed. 1981); J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION (4th ed. 2005); RESTATEMENT (THIRD) OF UNFAIR COMPETITION (1995).

of assessing the allocation of governance responsibilities between federal and state authorities. Hence, this Article focuses on the general features of unfair competition law and the relationship of federal and state sources of authority. Some discussion of the evolution of this body of law is necessary in order to grasp the relationships between federal and state law.

1. Federal Unfair Competition Law

Federal law governing advertising and marketing reflects two distinct approaches to consumer protection: one organized around the protection of trademarks and a second focused on policing consumer advertising and trade practices directly. The former model, which grew out of the common law tort of passing off and has since been codified in statute, operates primarily on a private enforcement model in which competitors police the use of their marks in commerce. An optional federal registration process complements this system. The latter approach, which took root in the formation of the FTC in 1914, relies principally on a regulatory/public enforcement model.

a) Early 19th Century through 1938: Federal Common Law, Trademark Legislation, and the Creation of the Federal Trade Commission

As the mercantile economy developed in the early to mid 19th century, federal courts came to see trademark infringement as an actionable offense.[55] Justice Joseph Story granted the first injunction based on trademark infringement in 1844.[56] Federal courts played the principal role in the early development of trademark law as the most significant businesses sought to enforce their trademarks under the emerging federal common law. Diversity of citizenship afforded jurisdiction and the federal courts offered the fullest body of legal precedents and broadest enforcement reach. The most influential jurists of that era articulated the elements and limiting doctrines that defined the unfair competition tort.

Congress did not enter the field until 1870, when it enacted the first federal trademark statute[57] pursuant to the Intellectual Property Clause of the U.S. Constitution.[58] After the Supreme Court struck down the act as exceeding the scope of that clause (which authorizes Congress to enact

55. *See generally* Rudolf Callmann, *What Is Unfair Competition?*, 28 GEO. L.J. 585 (1940); Milton Handler, *Unfair Competition*, 21 IOWA L. REV. 175 (1936); Zechariah Chafee, Jr., *Unfair Competition*, 53 HARV. L. REV. 1289 (1940).

56. Taylor v. Carpenter, 23 F. Cas. 742 (C.C.D. Mass. 1844) (No. 13784).

57. Act of July 8, 1870, ch. 230, §§ 77-84, 16 Stat. 198 (entitled "An Act to revise, consolidate, and amend the Statutes relating to Patents and Copyrights").

58. U.S. CONST. art. I, § 8, cl. 8.

laws promoting the progress of science and the useful arts),[59] Congress reenacted a more limited statute in 1881 pursuant to the Commerce Clause limiting protection to marks in foreign commerce.[60] Congress significantly expanded the trademark statute in 1905 by extending its reach to marks in interstate commerce, effectively eliminating the intent to deceive requirement, and expanding protection to include noncompeting goods.[61]

In parallel with the evolution of a federal statutory regime for trademark registration and enforcement, federal courts played a growing role in the evolution of a federal common law of unfair competition. Courts initially limited the doctrine of unfair competition to situations in which one company "passed off" its goods as those of another.[62] Federal decisions gradually expanded upon this basic fact pattern to encompass various other scenarios in which one trader diverted patronage from a rival. The Supreme Court's articulation of a general misappropriation tort under federal common law in *International News Service v. Associated Press*[63] represented a high water mark in common law regulation of trade practices. The Court recognized a quasi-property interest in news gathering: "the right to acquire property by honest labor or the conduct of a lawful business is as much entitled to protection as the right to guard property already acquired."[64] The court analogized the underlying principle to the equitable theory of consideration in the law of trusts—"that he who has fairly paid the price should have the beneficial use of the property."[65] Justice Holmes, concurring in the judgment, viewed the case as a species of reverse passing off, focusing on the fact that the defendant was able to deliver news gathered by the plaintiff to some markets faster than the plaintiff.[66]

In a 1925 decision, Judge Learned Hand broadened the principle of passing off to encompass deceptive promotion:

> While a competitor may, generally speaking, take away all the customers of another that he can, there are means which he must not use. One of these is deceit. The false use of another's name as maker or source of his own goods is deceit, of which the false

59. *See* Trade-Mark Cases, 100 U.S. 82, 94 (1879).

60. Act of Mar. 3, 1881, ch. 138, 21 Stat. 502.

61. Act of Feb. 20, 1905, ch. 592, 33 Stat. 724 (entitled "An Act To authorize the registration of trade-marks used in commerce with foreign nations or among the several States or with Indian tribes, and to protect the same").

62. *See* MCCARTHY ON TRADEMARKS, *supra* note 54, at § 1.12.

63. 248 U.S. 215 (1918).

64. *Id.* at 236.

65. *Id.* at 240.

66. *Id.* at 246-48 (Holmes, J., concurring).

> use of geographical or descriptive terms is only one example. But we conceive that in the end the questions which arise are always two: Has the plaintiff in fact lost customers? And has he lost them by means which the law forbids? The false use of the plaintiff's name is only an instance in which each element is clearly shown.[67]

In resolving this case, Judge Hand articulated what came to be known as the "single source" exception to a significant limitation on the common law of unfair competition: that unfair competition extended only to confusion as to the source of goods and not misrepresentations as to the product itself.[68] Judge Hand held that where a particular product could come from only a single source—in this case, because the manufacturer possessed a patent on an essential feature of the product in question—then another company's advertisement falsely offering such product (with the patented feature) was actionable.

The second branch of federal unfair competition law emerged as part of the mandate of the FTC. In 1914, Congress enacted the Federal Trade Commission Act for the primary purpose of enforcing federal antitrust laws by preventing "unfair methods of competition." In addition to pursuing anticompetitive behavior in the antitrust sense, the FTC interpreted its authority and directed its enforcement resources toward combating deceptive trade practices generally. The Supreme Court validated the FTC's authority to combat false advertising in 1922.[69] In 1938, Congress clarified that the FTC's jurisdiction extends to deceptive practices without regard to evidence of competitive harm.[70] The Commission must, however, establish that its actions respond to specific and substantial harm to the public interest.[71]

---

67. Ely-Norris Safe Co. v. Mosler Safe Co., 7 F.2d 603, 604 (2d Cir. 1925), *rev'd on other grounds*, 273 U.S. 132 (1927).

68. *See* Washboard Co. v. Saginaw Mfg. Co., 103 F. 281 (6th Cir. 1900) (justifying this limitation on the grounds that a competitor of a deceptive advertiser could not necessarily establish that his sales were adversely affected).

69. *See* FTC v. Winsted Hosiery Co., 258 U.S. 483 (1922). Commentators came to see the FTC as "the 'Magna Charta' of truth in interstate trade and of incalculable service to both industry and the public at large." R.S. Ely, *The Work of the Federal Trade Commission*, 7 WIS. L. REV. 195, 210 (1932).

70. Wheeler-Lea Amendment, ch. 49, § 3, 52 Stat. 111 (1938) (codified at 15 U.S.C. § 45(a) (2000)).

71. FTC v. Klesner, 280 U.S. 19 (1929).

b) Post-Erie: The Lanham Act and FTC Efforts to Foster State Consumer Protection Regimes

The development of the federal common law of unfair competition was abruptly derailed in *Erie R.R. Co. v. Tompkins*,[72] in which the Supreme Court largely abolished federal common law. In effect, *Erie* shifted further evolution of the common law of unfair competition to the states and further development of federal unfair competition law to the legislative arena.

In 1946, the U.S. Congress took up where Judge Hand and other jurists had left off and pushed federal statutory protection against unfair competition to the forefront.[73] The Lanham Act supplanted prior trademark enactments and expressly added significant new protections against unfair competition and false advertising. Section 43(a) recognized a right of action against "a false designation of origin, or any false description or representation" used in connection with any goods or services in favor of "any person who believes that he is or is likely to be damaged." Some early interpretations confined § 43(a) to misrepresentations relating to source; other interpretations viewed it as a codification of existing common law liability under the "single source" doctrine.[74] Subsequent decisions in several circuits established the section's general applicability to deceptive advertising and rejected the attempt to engraft common law limitations onto the statutory tort.[75] The 1988 revision of § 43(a) removed any doubt that the Lanham Act extends to both misrepresentations of source and other deceptive representations made in connection with the marketing of goods and services[76] and does away with the single source

72. 304 U.S. 64 (1938).

73. Act of July 5, 1946, ch. 540, 60 Stat. 427 (1946) (codified as amended at 15 U.S.C. §§1051-1127 (2000)).

74. *See* Samson Crane Co. v. Union Nat'l Sales, 87 F. Supp. 218, 222 (D. Mass. 1949), *aff'd*, 180 F.2d 896 (1st Cir. 1950). The "single source" doctrine was a prudential limitation on false advertising which allowed a competitor to recover against a deceptive advertiser only if they could show that they were the only legitimate manufacturer of the product in question. *See* Ely-Norris Safe Co. v. Mosler Safe Co., 7 F.2d 603 (2d Cir. 1925) (finding liability where the plaintiff held a patent), *rev'd on other grounds*, 273 U.S. 132 (1927); Washboard Co. v. Saginaw Mfg. Co., 103 F. 281 (6th Cir. 1900) (justifying this limitation on the grounds that a competitor of a deceptive advertiser could not necessarily establish that his sales were adversely affected).

75. *See* Coca-Cola Co. v. Procter & Gamble Co., 822 F.2d 28 (6th Cir. 1987); Procter & Gamble Co. v. Cheesebough-Pond's Inc., 747 F.2d 114 (2d Cir. 1984); U-Haul Intern., Inc. v. Jartran, Inc., 681 F.2d 1159, 1162 (9th Cir. 1982).

76. Pub. L. No. 100-667, 102 Stat. 3935 (1988). As revised, trademark liability extends to:

limitation on recovery.[77] The plaintiff must, however, establish some likelihood of harm to itself in order to have standing to bring an action under the Lanham Act.[78] Congress has since expanded the federal unfair competition regime to provide causes of action against dilution of famous marks[79] and registration of trademarks as domain names in bad faith.[80]

During the heyday of the civil rights, environmental, and consumer movements of the 1960s, the FTC led an effort to expand the effectiveness of consumer protection regulation by encouraging states to adopt what have come to be known as "little" FTC Acts. In order to guide states in the

---

> (1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—
> (A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or
> (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,
> shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

15 U.S.C. § 1125(a) (2000).

77. *See* ALPO Petfoods, Inc. v. Ralston Purina Co., 913 F.2d 958, 964 (D.C. Cir. 1990); Pacamor Bearings, Inc. v. Minebea Co., 918 F. Supp. 491 (D.N.H. 1996) (holding that trademark owner need only prove that defendants' conduct was likely to be injurious to the plaintiff's business); Forschner Group, Inc. v. Arrow Trading Co., 833 F. Supp. 385 (S.D.N.Y. 1993) (allowing one of two sellers of genuine product to sustain an action for false advertising without the other), *order vacated*, 30 F.3d 348 (2d Cir. 1994).

78. *See* Ortho Pharm. Corp. v. Cosprophar, Inc., 32 F.3d 690 (2d Cir. 1994); PDK Labs, Inc. v. Friedlander, 37 U.S.P.Q.2d 1195 (S.D.N.Y. 1995) (denying standing to sue under § 43(a) to one who is not yet a competitor of the alleged false advertiser), *aff'd*, 103 F.3d 1105 (2d Cir. 1997). Moreover, the harm must be caused by the false or otherwise improper advertisement. *See* Seven-Up Co. v. Coca-Cola Co., 86 F.3d 1379 (5th Cir. 1996); Zschaler v. Claneil Enterprises, Inc., 958 F. Supp. 929, 936-37 (D. Vt. 1997) (noting that the mere fact that the parties are in competition does not establish causation, at least where the false advertisement is non-comparative); Brown v. Armstrong, 957 F. Supp. 1293 (D. Mass. 1997) (denying relief where plaintiff offered no evidence that any consumer was actually misled or made a purchasing decision as a result of having been misled), *aff'd*, 129 F.3d 1252 (1st Cir. 1997).

79. *See* Federal Trademark Dilution Act of 1995, Pub. L. No. 104-98, 109 Stat. 985 (1996) (codified as amended at 15 U.S.C. §§ 1125(c), 1127 (2000)) (defining "dilution").

80. *See* Anticybersquatting Consumer Protection Act, Title III of the Intellectual Property and Communications Omnibus Reform Act of 1999, Pub. L. No. 106-113, 113 Stat. 1501 (1999) (codified at 15 U.S.C. § 1125(d)).

development of such laws, the FTC drafted a model act in the late 1960s—the Unfair Trade Practices and Consumer Protection Law (UTPCPL).[81] Like the FTC Act, the model state law authorized the creation of state agencies to promulgate standards to combat unfair and deceptive practices[82] and expand enforcement. Of comparable significance, the model law, reflecting the spirit of the times, proposed the establishment of a private right of action against those who engage in unfair or deceptive selling practices.[83] This provision—focusing on persons who suffer ascertainable

---

81. *See* UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, *in* Council of State Governments, 29 Suggested State Legislation 141-52 (1970).

82. Section 2 of the Model Act offered states three formulations for their laws: Alternative 1 prohibits "methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Alternative 2 prohibits "false, misleading, or deceptive acts or practices in the conduct of any trade or commerce." Alternative 3 specifies a detailed list of unfair practices—such as passing off and false advertising—as well as a general bar against "any act or practice which is unfair or deceptive to the consumer."

83. The private cause of action is set forth in Section 8:

> (a) Any person who purchases or leases goods or services primarily for personal, family or household purposes and thereby suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by Section 2 of this Act, may bring an action under rules of civil procedure in the (trial court of general jurisdiction of the county or judicial district) in which the seller or lessor resides or has his principal place of business or is doing business, to recover actual damages or $200, whichever is greater. The court may, in its discretion, award punitive damages and may provide such equitable relief as it deems necessary or proper.
>
> (b) Persons entitled to bring an action under subsection (a) of this Section may, if the unlawful method, act or practice has caused similar injury to numerous other persons similarly situated and it they adequately represent such similarly situated persons, bring an action on behalf of themselves and other similarly injured and situated persons to recover damages as provided for in subsection (a) of this Section. In any action brought under this Section, the court may in its discretion order, in addition to damages, injunctive or other equitable relief.
>
> (c) Upon commencement of any action brought under subsection (a) of this Section the clerk of court shall mail a copy of the complaint or other initial pleading to the attorney general and, upon entry of any judgment or decree in the action, shall mail a copy of such judgment or decree to the attorney general.
>
> (d) In any action brought by a person under this Section, the court may award, in addition to the relief provided in this Section, reasonable attorney's fees and costs.
>
> (e) Any permanent injunction, judgment or order of the court made under Section 5 [providing for the Attorney General to bring

losses from the purchase or lease of goods or services primarily for personal, family, or household purposes—envisioned consumer and consumer class action suits against unscrupulous sellers.

Mindful of the need for harmonization among jurisdictions (and with the federal regime), the FTC model state unfair competition law tethered interpretation to the FTC's evolving definitions and standards.

> Section 3. Interpretation
>
> (a) It is the intent of the legislature that in construing Section 2 of this Act due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. § 45 (a)(1)), as from time to time amended; and
>
> (b) the attorney general may make rules and regulations interpreting the provisions of Section 2 of this Act. Such rules and regulations shall not be inconsistent with the rules, regulations and decisions of the Federal Trade Commission and the federal courts in interpreting the provisions of Section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45 (a)(1)), as from time to time amended.[84]

The FTC's "unfairness" and "deception" standards have since gone through several stages of evolution. The FTC Act was deliberately framed in general terms in order to provide the Commission flexibility to address trade practices as they developed.[85] In 1964, the Commission identified three factors that it considered when applying the prohibition against consumer "unfairness": (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been

---

> enforcement actions] shall be *prima facie* evidence in an action brought under Section 8 of this Act that the respondent used or employed a method, act or practice declared unlawful by Section 2 of this Act.

84. UTPCPL, § 3.

85. *See* H.R. REP. NO. 1142, at 19 (1914) (stating that if Congress "were to adopt the method of definition, it would undertake an endless task"). As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'" FTC v. Raladam Co., 283 U.S. 643, 648 (1931); *see also* FTC v. R. F. Keppel & Bro., 291 U.S. 304, 310 (1934) ("Neither the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories.").

established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; and (3) whether it causes substantial injury to consumers (or competitors or other businessmen).[86] In 1980, the FTC narrowed its "unfairness" standard by emphasizing the need for "substantial" consumer injury, adopting a cost-benefit test (weighing harm against offsetting consumer or competitive benefits), and limiting the public policy prong to "clear and well-established" statements of public policy.[87]

Similarly, the FTC reined in its "deception" standard in the 1980s. Dating back to the Supreme Court's 1934 decision in *FTC v. Algoma Lumber Co.*,[88] the FTC had applied a relatively broad standard to the interpretation of "deception" in the statute—any trade practice having the "tendency or capacity to deceive" violated the Act. In what had come to be known as the "fool's test," the Second Circuit approved a broad standard for deception based on the principle that the FTC Act was not developed to protect experts, but rather the general public—"that vast multitude which includes the ignorant, the unthinking and the credulous."[89] In 1983, the FTC replaced the "tendency or capacity to deceive" standard with a definition of a deceptive act as "a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances,

86. Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (1964). These factors were later quoted with apparent approval by the Supreme Court in FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244-45 n.5 (1972). *See also* Spiegel, Inc. v. FTC, 540 F.2d 287, 293 n.8 (7th Cir. 1976); Heater v. FTC, 503 F.2d 321, 323 (9th Cir. 1974).

87. FTC Policy Statement on Unfairness, Letter from Wendell H. Ford & John C. Danforth to Senate members of the Consumer Subcommittee of the U.S. Senate Committee on Commerce, Science, and Transportation (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm. The FTC dropped the "immoral, unethical, oppressive, or unscrupulous" factor on the ground that it overlapped with the other two. *Id.*

88. 291 U.S. 67, 81 (1934).

89. Charles of the Ritz Distribs. Corp. v. FTC, 143 F.2d 676, 678-79 (2d Cir. 1944) (quoting the Supreme Court's decision in *FTC v. Standard Education Society*, 302 U.S. 112, 116 (1937), the court observed that "the fact that a false statement may be obviously false to those who are trained and experienced does not change its character, nor take away its power to deceive others less experienced."). *See generally* Ernest Gellhorn, *Proof of Consumer Deception before the Federal Trade Commission*, 17 U. KAN. L. REV. 559 (1969).

to the consumer's detriment."[90] This standard was ratified a year later in *In re Cliffdale Associates*.[91] By focusing upon whether an act or practice is likely to mislead consumers acting reasonably in the circumstances to their detriment, the 1983 standard narrowed the reach of the FTC Act.[92]

2. State Unfair Competition Law

In addition to shifting federal unfair competition law from a common law foundation to statute (the Lanham Act), the *Erie* decision[93] relocated development of the common law to state courts. State courts have since developed a variegated jurisprudence within the general contours of pre-*Erie* federal common law.[94] In the false advertising area, state courts have retained the single source limitation as a barrier to recovery;[95] although many state legislatures have abolished this restriction through legislation. The misappropriation tort articulated by the Supreme Court in *Interna-*

90. FTC Policy Statement on Deception, Letter from FTC to John D. Dingell, Chairman U.S. House of Representatives Committee on Energy & Commerce (Oct. 14, 1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

91. 103 F.T.C. 110 (1984). *See generally* Jack E. Kairns, *State Regulation of Deceptive Trade Practices Under "Little FTC Acts": Should Federal Standards Control?*, 94 DICKINSON L. REV. 373 (1990).

92. *See* Patricia Bailey & Michael Pertschuk, *The Law of Deception: The Past as Prologue*, 33 AM. U. L. REV. 849 (1984) (authored by the two dissenting commissioners in the *Cliffdale Associates* case).

93. *See supra* note 72.

94. *See generally* RESTATEMENT (THIRD) OF UNFAIR COMPETITION (1995).

95. *See, e.g.*, California Apparel Creators v. Wieder of California, Inc., 162 F.2d 893 (2d Cir. 1947). *See generally* 1A CALLMANN ON UNFAIR COMPETITION, TRADEMARK, AND MONOPOLIES § 5:2 (4th ed. 1981). "[I]n an action for false advertising, a plaintiff, in order to have standing to sue, must demonstrate that defendant has either palmed off his goods as those of the plaintiff or that the plaintiff has a monopoly of the goods involved, so that injury can be readily inferred." Smith-Victor Corp. v. Sylvania Elec. Prods., Inc., 242 F. Supp. 302, 309 (N.D. Ill. 1965); *followed in* Julie Research Labs., Inc. v. Gen. Resistance, Inc., 268 N.Y.S.2d 187 (N.Y. App. Div. 1966), *order aff'd*, 227 N.E.2d 892 (N.Y. 1967); *followed in* Magnus Organ Corp. v. Robbins Music Corp., 163 U.S.P.Q. 695 (N.Y. 1969) ("[W]hile it may be morally wrong and improper to impose upon the public by the sale of spurious goods, false advertising does not give rise to a private right of action, unless some property right of the plaintiff has thereby been invaded."); Ortho Pharm. Corp. v. Cosprophar, Inc., 32 F.3d 690 (2d Cir. 1994) (finding no standing to sue for false advertising without a showing of harm to the plaintiff); Nordictrack, Inc. v. Soloflex, Inc., No. 93-1432-JE, 1994 U.S. Dist. LEXIS 16172, at *9 (D. Or. 1994): ("[T]o prevail under Minnesota [common] law, [plaintiff] must establish that it lost sales through [defendant's] false advertising."); Multi-Tech Sys., Inc. v. Hayes Microcomputer Prods., Inc., 800 F. Supp. 825, 848 (D. Minn. 1992).

tional News Service v. Associated Press[96] has been elaborated to some extent, but has not been expanded.[97]

State unfair competition law has expanded most significantly through several waves of legislation. Although the impetus for the first wave of state unfair competition legislation was to unify this field of law, the effects have tended in the opposite direction. Even the FTC's encouragement of state consumer protection regimes tethered to federal standards has resulted in centrifugal rather than centripetal results. The landscape of unfair competition law today can best be characterized as fragmented, uncoordinated, and amorphous. The proliferation of state statutes aimed at controlling deceptive advertising, including many authorizing treble or punitive damages, has broadened the field, expanded the tools available, and promoted recourse to state unfair competition law.

a) State Unfair Competition Protection for Competitors

State common law and statutory protections against trademark infringement and unfair competition developed along tracks roughly parallel to the federal regime. Prior to the *Erie* decision in 1938, federal common law tended to dominate the field as federal courts took a leadership role in setting the scope of the emerging common law of unfair competition. The rise of the Lanham Act less than a decade later reinvigorated the federal role and it has continued to dominate the field of unfair competition.[98] Following the abrupt elimination of federal common law in 1938, litigants continued to invoke state common law where their claims did not fall squarely within federal or state statutory protections. The absence of a unifying mechanism produced confusing, if not conflicting, legal standards. As noted earlier, the lack of harmonization among state common law

96. 248 U.S. 215 (1918).

97. *See, e.g.*, Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 847 (2d Cir. 1997); United States Golf Ass'n v. St. Andrews Sys., Data-Max, Inc., 749 F.2d 1028 (3d Cir. 1984). *But see* United States Golf Ass'n v. Arroyo Software Corp., 81 Cal. Rptr. 2d 708, 714 (Cal. Ct. App. 1999). *See generally* Bruce P. Keller, *Condemned to Repeat the Past: The Reemergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property*, 11 HARV. J.L. & TECH. 401 (1998) (arguing that flexible and evolving common law norms are an effective means for addressing the dynamism brought about by technological change); Leo J. Raskind, *The Misappropriation Doctrine as a Competitive Norm of Intellectual Property Law*, 75 MINN. L. REV. 875 (1991); Richard A. Posner, *Misappropriation: A Dirge*, 40 HOUS. L. REV. 621 (2003); Edmund J. Sease, *Misappropriation Is Seventy-Five Years Old; Should We Bury It or Revive It?*, 70 N.D.L. REV. 781 (1994).

98. *See* Bruce P. Keller, *"It Keeps Going and Going and Going": The Expansion of False Advertising Litigation Under the Lanham Act*, 59 LAW & CONTEMP. PROBS. 131 (1996).

precedents prompted Judge Medina of the U.S. Court of Appeals for the Second Circuit to lament that distillation of the applicable law was an area "where angels fear to tread."[99] He called for the adoption of either a preemptive federal statute or a uniform state law to govern unfair competition.[100]

The American Bar Association's Section of Patents, Trademark and Copyright Law also took note of the problem. In its 1958 report,[101] a special committee concluded that with the exception of California unfair competition law,[102] which was codified in statute, all state unfair competition laws were "ambiguous," "archaic," and inadequate to cope with current conditions of commerce. The Committee passed a resolution which stated that "there should be uniformity in the law of unfair competition among the respective states."[103] Efforts to achieve a new federal law, however, stalled in Congress. Meanwhile, the ABA Committee drafted the Uniform Deceptive Trade Practices Act (UDTPA), which the National Conference of Commissioners on Uniform State Laws adopted in 1964.[104]

The Uniform Act sought to update state law to provide businesses with a direct cause of action against competitors for deceptive trade practices. In so doing, it removed traditional common law restrictions, such as the single source rule.[105] The uniform law was modeled roughly after California law.[106] The Act incorporated the following principles: likelihood of confusion is sufficient to establish liability; actual competition between the parties is not a prerequisite to relief; and a defendant need not be an intentional wrongdoer to incur liability. The statute avoids a restrictive or exclusive definition of unfair competition, providing instead a list of a dozen specific and broad prohibited practices ranging from passing off to

---

99. Am. Safety Table Co. v. Schreiber, 269 F.2d 255, 271 (2d Cir. 1959).

100. There was still substantial discord among the federal courts over whether the Lanham Act confined § 43(a) to misrepresentations relating to source or whether it could be invoked to address any form of deceptive advertising. Many circuits did not broaden their interpretation until the early 1980s, which Congress codified in the 1988 amendments. *See supra* note 76.

101. *See* National Conference of Commissioners of Uniform State Laws, Prefatory Note, Revised Uniform Deceptive Trade Practices Act (1966) (referencing the 1958 ABA Report), *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1920_69/rudtpa66.htm.

102. *See* CAL. CIV. CODE § 3369 (West 2004); Victor S. Netterville, *California Law of Unfair Competition: Unprivileged Imitation*, 28 S. CALIF. L. REV. 240 (1955).

103. *See supra* note 101.

104. *Id.* NCCUSL amended this report in 1966 to provide for the award of reasonable attorney fees in some circumstances.

105. *Id.*

106. *See* CAL. CIV. CODE § 3369.

various forms of false advertising.[107] The UDTPA provides solely for injunctive relief, although it permits damages to be awarded for the same conduct where actionable under the common law or other statutes.[108]

The UDTPA affords business enterprises a cause of action against other businesses which obtain a competitive advantage by deceiving consumers. After being adopted by fourteen states[109] relatively soon after its promulgation, the UDTPA lost momentum and has declined in significance. The 1988 amendments to the Lanham Act fully extended the coverage of federal law into this field.[110] The UDTPA was withdrawn from recommendation for enactment by the National Conference of Commissioners on Uniform State Laws in 2000 on the grounds that it had become obsolete. The NCCUSL website no longer maintains information about this uniform statute.[111] Nonetheless, the dozen or so state statutes modeled after the UDPTA remain in effect and they have assumed a life of their own within the particular states in which they were enacted. The ABA's goal of creating "uniformity in the law of unfair competition among the respective states" through adoption of a uniform state law has not come to pass. Even in states with such statutes, common law remedies have remained viable. Hence, unfair competition law continues to be amorphous and variable across state jurisdictions.

b) Consumer Protection Against Deceptive Trade Practices

In theory, state common law doctrines of deceit and fraud afforded remedies against unscrupulous sellers, although neither proved particularly effective in practice.[112] These causes of action impose relatively high burdens of proof upon plaintiffs.[113] Since most consumers suffer relatively

---

107. UDTPA, § 2.

108. UDTPA, § 3.

109. Colorado, Delaware, Georgia, Hawaii, Illinois, Kansas, Minnesota, Nebraska, Nevada, New Mexico, Ohio, Oklahoma, Oregon, and Utah. *See* Legal Information Institute, Uniform Business and Financial Laws Locator, http://www.law.cornell.edu/uniform/vol7.html#dectr (last visited Aug. 28, 2005).

110. *See supra* note 76.

111. *See* National Conference of Commissioners on Uniform State Laws Drafts of Uniform and Model Acts, http://www.law.upenn.edu/bll/ulc/ulc_frame.htm (last visited Aug. 28, 2005).

112. *See generally* Jeff Sovern, *Private Actions under the Deceptive Trade Practices Acts: Reconsidering the FTC Act as Rule Model*, 52 OHIO ST. L.J. 437 (1991).

113. The common law action for deceit requires that the plaintiff prove:

> (1) a material representation which is (2) false and (3) known to be false, or made recklessly as an assertion of fact without knowledge of its truth or falsity, and (4) made with the intention that it shall be acted upon, and (5) acted upon with damage. . . . In addition to these

small harms, common law remedies were rarely utilized to combat practices that collectively imposed significant consumer harm. In recognition of these limitations, the limited effective reach of the FTC Act (due to resource and information constraints), and the growing public support for stronger consumer protection laws, every state had passed its own consumer protection statute by the mid 1970s. Most of these statutes trace their specific provisions to one of the alternatives recommended by the FTC in the Unfair Trade Practices and Consumer Protection Law. Fourteen states[114] adopted some variation on Alternative 1 of the FTC model act.[115] Kentucky and Texas adopted Alternative 2, which omits reference to the FTC's standard of "unfair methods of competition" and focuses on "false, misleading, or deceptive acts or practices." Ten states[116] adopted some version of Alternative 3, which enumerates twelve (and in some cases more) specific unlawful trade practices. Twenty other states and the District of Columbia have an itemized list of unlawful acts or practices.[117]

By creating a private right of action and the opportunity to obtain treble and/or punitive damages in many states, these statutes expanded the role of courts in regulating unfair and deceptive practices. These statutes provide a much broader assault on unfair and deceptive trade practices than the UDTPA and have come to dominate the field, at least with regard to consumer-related harms.[118] Variation in the substantive provisions of

---

> elements, it must also be proved that the plaintiff (6) relied upon the representations, (7) was induced to act upon them, and (8) did not know them to be false, and (9) by the exercise of reasonable care could not have ascertained their falsity.

Coffin v. Dodge, 76 A.2d 541, 543 (Me. 1950); Inman v. Ken Hyatt Chrysler Plymouth, 363 S.E.2d 691, 692 (S.C. 1988) (a fraud "complaint is fatally defective if it fails to allege all nine elements of fraud"). Even breach of contract claims can be difficult to prove and they do not permit recovery of punitive damages or attorney fees. *See generally* Ernest Rice, *Exemplary Damages in Private Consumer Actions*, 55 IOWA L. REV. 307 (1969).

114. Connecticut, Florida, Hawaii, Louisiana, Illinois, Massachusetts, Maine, Montana, Nebraska, North Carolina, Vermont, South Carolina, Washington, and West Virginia. California, Wisconsin, and Utah have statutes patterned directly upon the FTC Act, including the Act's emphasis on "unfair methods of competition."

115. *See* Anthony Paul Dunbar, Comment, *Consumer Protection: The Practical Effectiveness of State Deceptive Practices Legislation*, 59 TUL. L. REV. 427 (1984).

116. Alabama, Alaska, Georgia, Idaho, Maryland, Mississippi, New Hampshire, Pennsylvania, Rhode Island, and Tennessee.

117. Indiana, Michigan, New York, South Dakota, Virginia, and Wyoming have crafted their own consumer protection statutes blending elements of the different model acts with distinctive language and procedures.

118. *See generally* JONATHAN SHELDON & CAROLYN L. CARTER, UNFAIR AND DECEPTIVE ACTS AND PRACTICES (National Consumer Law Center, 4th ed. Supp. 2000).

these statutes as well as the role of the courts in interpreting them have resulted in a rather complex legal landscape for companies operating nationally. As noted by two commentators, "[t]he process of judicial interpretation followed by legislative clarification or adjustment has further eroded the uniformity of the [FTC's] original proposal."[119] Furthermore, some states have enacted both deceptive practices statutes focused on business competition as well as FTC-like consumer protection statutes. Over time, the courts have tended to blur the distinctions between the two regimes.

From a practical standpoint, the state regimes differ along three critical dimensions: (1) standing to sue; (2) scope and extent to which they look to applicable federal law (under either the Lanham Act or the FTC Act); and (3) remedies. With regard to standing, the FTC's model act (the UTPCPL) limited the private right of action to consumers purchasing goods for personal use.[120] Many states, however, adopted a modified version of this provision omitting the limitations on the type of injured party. Furthermore, some state courts have interpreted standing under such statutes broadly. With regard to scope, the UTPCPL provided for states to look to federal interpretations of unfair competition in construing their acts.[121] State commissions and courts have varied in the extent to which they have followed the evolution of federal standards, producing divergent standards. Most states do not require that private litigants meet a "public interest" standard, as required under the FTC Act.[122] States also vary in terms of whether they follow the pre or post-*Cliffdale Associates* test[123] for deception and the remedies available, with some states allowing plaintiffs to recover treble or punitive damages and fees.

From the standpoint of businesses operating in many or all states, the patchwork of unfair competition and consumer protection regimes creates significant confusion, increases the costs of assessing legal standards, and

---

119. *See* EDMUND W. KITCH & HARVEY S. PERLMAN, INTELLECTUAL PROPERTY AND UNFAIR COMPETITION 144 (5th ed. 1998).

120. *See* UTPCPL, § 8 ("[a]ny person who purchases or leases goods or services primarily for personal, family, or household purposes and thereby suffers any ascertainable loss of money or property.")

121. *See* UTPCPL, § 3.

122. Of the forty-two states that afford a private cause of action under statutes derived from the UTPCPL, only six have imposed a showing of a "public interest" by a private plaintiff. *See* Marshall A. Leaffer & Michael H. Lipson, *Consumer Actions Against Unfair or Deceptive Acts or Practices: The Private Uses of Federal Trade Commission Jurisprudence*, 48 GEO. WASH. L. REV. 521 (1980).

123. 103 F.T.C. 110 (1984); *see supra* note 89 (discussing evolution of federal "deception" standard).

may inhibit some forms of innovation. Due to the relative ease of hauling Internet businesses into court in just about any state,[124] such businesses are particularly exposed to the constraints of the most restrictive state unfair competition laws.

B. The Application of State Unfair Competition Law to Behavioral Marketing Businesses

With this backdrop in place, we turn to the case study of Internet-based behavioral marketing businesses. The goal is to assess how the patchwork of federal and state unfair competition law standards has affected this emerging sector.

1. History of Internet-Based Advertising

Internet marketing began more than a decade ago, shortly after the launch of the World Wide Web.[125] The first generation of Internet advertising utilized banner advertisements. Advertisers could deliver these advertisements to web surfers visiting particular websites. Early efforts to customize advertising delivery mimicked traditional media advertising by using relatively crude sampling techniques to map demographic characteristics.[126] The ability to monitor response "click through" rates in real time, however, provided web-based advertising companies new opportunities for measuring advertising efficacy. Web-based advertising grew rapidly, along with the dot com boom, rising from essentially zero in 1994 to $8 billion by the year 2000.[127] During this time, online advertisers developed more sophisticated techniques for customizing advertisements, including advertising networks (consortia of websites that allow advertisers to buy advertisements on multiple sites), keyword-triggered advertisements, geographic indicators to localize advertisements, and the use of "cookies" (data files stored on computer users' hard drives that can be used to track

124. *See supra* note 31.

125. *See* RICK E. BRUNER, DOUBLECLICK, THE DECADE IN ONLINE ADVERTISING 1994-2004 (Apr. 2005), http://www.doubleclick.com/us/knowledge_central/documents/RESEARCH/dc_decaderinonline_0504.pdf#search='the%20decade%20in%20online%20advertising%20and%20rick%20bruner'.

126. CNET NEWS.COM, *See Advertising as a science*, Oct. 4, 1996, http://news.com.com/Advertising+as+a+science/2100-1001_3-235158.html (citing study by Internet Profiles (I/Pro) and DoubleClick Network, entitled "A Comprehensive Analysis of Ad Response," finding that web surfers click on 2.11 percent of all ad banners displayed, while direct mail typically generates a 1 percent to 2 percent response rate and print ads 0.5 percent to 0.75 percent response rate).

127. *See* DoubleClick, *supra* note 125, at 4.

surfing activity).[128] Online advertisers also used response information to tie advertising pricing to various measures of performance, such as click through rates and revenues attributable to online advertisements.[129]

Web advertising slowed in the late 1990s, with revenues leveling and then declining as the dot com bubble burst.[130] In addition, web users began to recognize some of the more aggressive modes of online advertising, such as e-mail spam, as a nuisance. The use of increasingly sophisticated data tracking tools generated controversy over the privacy rights of web surfers. Consumer privacy groups objected when DoubleClick, one of the leading online advertising companies, proposed to combine online and off-line information databases to develop detailed consumer profiles.[131] In response to pressure from privacy organizations, the FTC, and members of Congress, DoubleClick scaled back its plans and instituted a privacy policy and review board.[132]

Behavioral marketing took root in the wake of these events. In 1999, The Gator Corporation introduced technology that utilized Internet users' search queries as a vehicle for delivering category-specific advertising in the form of pop-up and pop-under windows and banners that overlay ad-

---

128. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502-06 (S.D.N.Y. 2001) (describing DoubleClick's Dynamic Advertising Reporting & Targeting (DART) technology); CNET NEWS.COM, *Ads find strength in numbers*, Nov. 4, 1996, http://news.com.com/Ads+find+strength+in+numbers/2009-1001_3-243757.html; Tim Clark, *User profiles in privacy stir*, CNET NEWS.COM, Aug. 17, 1998, http://news.com.com/User+profiles+in+privacy+stir/2100-1023_3-214527.html; Tim Clark, *DoubleClick localizes Web ads*, CNET NEWS.COM, Jul. 14, 1998, http://news.com.com/DoubleClick+localizes+Web+ads/2100-1023_3-213317.html; Janet Kornblum, *DoubleClick launches ad service*, CNET NEWS.COM, Oct. 5, 1998, http://news.com.com/DoubleClick+launches+ad+service/2100-1023_3-216287.html.

129. *See* J. William Gurley, *How to succeed in advertising*, CNET NEWS.COM, Apr. 20, 1998, http://news.com.com/How+to+succeed+in+advertising/2009-1023_3-210389.html.

130. *See* DoubleClick, *supra* note 125, at 4.

131. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d at 497; Sandeep Junnarkar, *DoubleClick accused of unlawful consumer data use*, CNET NEWS.COM, Jan. 28, 2000, http://news.com.com/DoubleClick+accused+of+unlawful+consumer+data+use/2100-1023_3-236216.html.

132. *See* Jim Hu, *Consumer advocates to head DoubleClick privacy efforts*, CNET NEWS.COM, Mar. 8, 2000, http://news.com.com/Consumer+advocates+to+head+DoubleClick+privacy+efforts/2100-1023_3-237710.html;; Patricia Jacobus, *"Cookies" targeted as Congress, advocates address Net privacy*, CNET NEWS.COM, Feb. 11, 2000, http://news.com.com/Cookies+targeted+as+Congress%2C+advocates+address+Net+privacy/2100-1023_3-236800.html?tag=st.rn; Stefanie Olsen, *Ad firms benefit from FTC privacy decision*, CNET NEWS.COM, Jul. 28, 2000, http://news.com.com/Ad+firms+benefit+from+FTC+privacy+decision/2100-1023_3-243822.html.

vertisements delivered by the website that a consumer was visiting. With venture capital backing from Garage.com and founders of Sun Microsystems, Symantec, and Intuit,[133] Gator set out to develop a large audience for its advertising vehicles by offering free software products—such as its eWallet product, which stores a user's passwords in an encrypted file on the user's computer and automatically fills in authentication forms as users surf the web—in exchange for users' consent to receive contextual advertising.[134] Gator earned revenue principally from advertisers who paid for advertisements on its contextual advertising platform. This system enabled Gator and its clients to measure click-through rates and various other metrics relating to advertising success. Gator rapidly expanded the size of its audience by offering other "free" software products and entered agreements with emerging peer-to-peer distributors to bundle Gator software with downloads of peer-to-peer software.[135]

As its advertising platform grew into the tens of millions of computers running its software, Gator attracted a large and diverse clientele of national brands, including Allstate Insurance, American Express, Apple, Mastercard, Chrysler, Expedia, FTD.com, NetFlix, Orbitz, Priceline, Sun Microsystems, and Verizon DSL.[136] Gator was also able to serve as a conduit for Overture, an online advertising company that charges clients on a "cost-per-click" basis.[137] Gator's growing visibility, however, raised concerns among some traditional web publishers, who complained that Gator's advertising technology—which allowed precise targeting of advertisements by competitors—interfered with their own on-line advertising

133. *See* Brian McWilliams, *Gator Branded A Trojan Horse Despite Security*, NEWSBYTES, Mar. 7, 2002, http://www.newsbytes.com/news/02/175046.html, *available at* http://seclists.org/lists/isn/2002/Mar/0045.html.

134. *See* Claria, Corporate Overview, http://www.claria.com/companyinfo (last visited Aug. 28, 2005).

135. In 2003, Gator paid $19.3 million on such distribution agreements, approximately 43 cents per active user. *See* Wienbar, *supra* note 8; FTC Spyware Report, *supra* note 8, at 5.

136. *See* Benjamin Edelman, *Documentation of Gator Advertising and Targeting*, http://cyber.law.harvard.edu/people/edelman/ads/gator/gator-customers.html (last visited Aug. 23, 2005); PC Pitstop, *Gator's Advertisers*, http://www.pcpitstop.com/gator/advertisers.asp (last visited Aug. 23, 2005).

137. *See* Wienbar, *supra* note 8. In 2003, nearly one-third of Gator's revenue came from Overture. *See* Stefanie Olsen, *Adware anxiety gives Claria cold feet*, CNET NEWS.COM, Aug. 12, 2004, http://news.com.com/Adware+anxiety+gives+Claria+cold+feet/2100-1024_3-5307545.html.

and poached visitors to their websites.[138] Consumers and privacy organizations also became concerned about the means by which adware was being loaded onto their computers and the difficulty of removing it.[139]

More recently, Gator has sought to soften its image by changing its name to Claria Corporation, expanding its advertising product and research offerings, distancing itself from more aggressive web advertisers, and seeking to build partnerships with traditional web publishers.[140] At the same time, other behavioral marketing companies, such as WhenU, 180Solutions, and Direct Revenue, have developed their own behavioral marketing networks and further raised the ire of web publishers and consumer organizations.

2. Unfair Competition Challenges to Internet-Based Behavioral Marketing Ventures

Gator's rise in the online advertising world quickly generated controversy over whether contextual advertising infringed the intellectual property rights of web publishers. WhenU soon found itself in a similar situation. Web publishers brought the first wave of litigation, seeking to prevent behavioral marketing companies from delivering advertisements when consumers visit their websites. Such litigation has alleged copyright infringement (on the ground that presenting a pop-up window or banner advertisement above a copyrighted website constitutes an unauthorized derivative work), trademark infringement (for the use of website owners' trademarks to trigger advertisements as well as confusion as to the source, sponsorship, or affiliation of pop-up advertisements), and various forms of

---

138. *See* Stefanie Olsen, *Chorus of Gator critics grows*, CNET NEWS.COM, Aug. 27, 2001, http://news.com.com/Chorus+of+Gator+critics+grows/2100-1023_3-272244.html; Stefanie Olsen, *UPS sues Gator for wrongful delivery*, CNET NEWS.COM, Oct. 2, 2002, http://news.com.com/UPS+sues+Gator+for+wrongful+delivery/2100-1023_3-960535.html (noting that Gator's software "might display a Federal Express ad to people viewing UPS.com").

139. *See* CDT, GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM (Nov. 2003), http://www.cdt.org/privacy/031100spyware.pdf; *Guess What—You Asked For Those Pop-Up Ads*, Jun. 28, 2004, http://www.businessweek.com/magazine/content/04_26/b3889095_mz063.htm; Stefanie Olsen, *Web surfers brace for pop-up downloads*, CNET NEWS.COM, Apr. 8, 2002, http://news.com.com/Web+surfers+brace+for+pop-up+downloads/2100-1023_3877568.html.

140. Stefanie Olsen, *Adware anxiety gives Claria cold feet*, CNET NEWS.COM, Aug. 12, 2004, http://news.com.com/Adware+anxiety+gives+Claria+cold+feet/2100-1024_3-5307545.html; Stefanie Olsen, *Gator sheds skin, renames itself*, CNET NEWS.COM, Oct. 29, 2003, http://news.com.com/Gator+sheds+skin%2C+renames+itself/2100-1024_3-5099212.html.

federal and state unfair competition claims. In the few cases that have gone to trial, the courts have been skeptical of the federal copyright and trademark allegations.[141] No case has yet fully addressed the unfair competition allegations, in part because many of the cases settled before trial.

This section explores the contours of the state law claims as a gauge of the exposure that behavioral marketing firms face. Within a relatively short period of time, web publishers filed suit against Claria in California, Florida, Georgia, Michigan, New Jersey, North Carolina, South Carolina, Utah, and Virginia.[142] WhenU was sued in Michigan, New York, Utah, and Virginia.[143] Whereas the federal law claims were largely the same in each of these cases, the state law unfair competition claims reflected a range of statutory and common law sources. Even where the underlying statutes or common law doctrines were parallel, the jurisprudence surrounding such causes of action varied. This predicament can best be illustrated by surveying the unfair competition regimes in several of these states.

a) California

California's unfair competition regime is set forth rather tersely in its Business & Professions Code: "unfair competition shall mean and include

141. *See* 1-800 Contacts, Inc. v. WhenU.Com, Inc., 2005 U.S. App. LEXIS 12711 (2d Cir. 2005); U-Haul Int'l., Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723 (E.D. Va. 2003); Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734 (E.D. Mich. 2003).

142. Hertz Corp. v. The Gator Corp., 250 F. Supp. 2d 421 (D.N.J. 2003); Tigerdirect, Inc. v. The Gator Corp., No. C-02-23615 (S.D. Fla. Dec. 20, 2002); The Gator Corp. v. TigerDirect, Inc., No. C-02-5875-BZ (N.D. Cal. Dec. 19, 2002); The Gator Corp. v. PriceGrabber, Inc., No. C-02-5875-BZ (N.D. Cal. Dec. 16, 2002); Lendingtree, Inc. v. The Gator Corp., No. 3:02-CV-519-V (W.D.N.C. Dec. 11, 2002); Extended Stay Am., Inc. v. The Gator Corp., No. 7:02-3845-20 (D.S.C. Nov. 14, 2002); Six Continents Hotels v. The Gator Corp., No. 1:02-CV-3065-JOF (N.D. Ga. Nov. 12, 2002); The Gator Corp. v. Extended Stay Am., No. C-02-5226-CRB (N.D. Cal. Oct. 29, 2002); United Parcel Serv. of Am. v. The Gator Corp., No. 1:02-CV-2639-BBM (N.D. Ga. Sept. 26, 2002); Washington Post.Newsweek Interactive Co. v. The Gator Corp., No. CV 02-909-A (E.D. Va. June 25, 2002). The Hertz Corp. lawsuit brought in New Jersey does not allege violations of any state deception or unfair competition statutes. *See Hertz Corp.*, 250 F. Supp. 2d at 421.

143. Louis Vuitton Malletier v WhenU.com, No. 1:05-CV-01325 (S.D.N.Y. Feb. 3, 2005); Louis Vuitton Malletier v WhenU.com, No. 1:04-CV-03249 (S.D.N.Y. Apr. 28, 2004); 1-800-Contacts, Inc. v. WhenU.com, No. 1:03-CV-08043 (S.D.N.Y. Nov. 7, 2003); Overstock.com v. WhenU.com, No. 2:03-CV-00570 (D. Ut. Jun. 25, 2003); Wells Fargo Co. v. WhenU.com, No. 2:03-CV-71906 (E.D. Mich. May 16, 2003); Vision Direct, Inc. v. WhenU.com, No. 1:02-CV-09788 (S.D.N.Y. Dec. 11, 2002); Tiger Direct, Inc. v. WhenU.com, No. 1:02-CV-23306 (S.D. Fla. Nov. 12, 2002); U-Haul Int'l v. WhenU, No. 1:02-CV-01469 (E.D. Va. Oct. 2, 2002).

any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising. . . ."[144] This provision can be traced back to a 1930's enactment inspired by the enlargement of the FTC's regulatory jurisdiction to include unfair business practices that harmed not merely the interests of business competitors but also those of the general public.[145] It was a pioneering state law that significantly expanded the substantive standard for pursuing unfair competition claims and the class of enforcers of such law (by creating a private right of action). While affording broad standing to consumers as well as competitors,[146] the statute affords only injunctive relief (including restitution where money has been paid) but does not authorize the award of civil damages.[147]

California's unfair competition regime prohibits "any unlawful, unfair, or fraudulent business act or practice."[148] Virtually any state, federal, or local law can serve as the predicate for the unlawful prong of this standard. With regard to the unfairness prong, courts have resisted a purely subjective standard, favoring an open-ended, nuisance-type balancing framework.[149] As such, the unfairness standard is quite broad, allowing courts wide discretion to prohibit new schemes to defraud. The fraud prong bears little resemblance to common law fraud or deception; rather, the test is whether the public is likely to be deceived. Thus, a violation of the fraud prong, unlike common law fraud, may be shown even if no one was actually deceived, relied upon the fraudulent practice, or sustained any damage.[150]

Although similar in some respects to both the Lanham Act's unfair competition provisions and the FTC's unfairness and deception tests, California's unfair competition regime may have broader reach because of dif-

---

144. CAL. BUS. & PROF. CODE § 17200 (West 2004).

145. *See* Gregory v. Albertson's, Inc., 128 Cal. Rptr. 2d 389 (Cal. Ct. App. 2002).

146. *See id.*; CAL. BUS. & PROF. CODE § 17204 (West 2004).

147. *See* CAL. BUS. & PROF. CODE § 17203 (West 2004); *cf.* People v. Thomas Shelton Powers, M.D., Inc., 3 Cal. Rptr. 2d 34 (Cal. Ct. App. 1992) (ordering disgorgement of profits under § 17200). *But see* Kraus v. Trinity Mgmt. Servs., Inc., 999 P.2d 718, 732 (Cal. 2000) (overruling, in part, disgorgement in *Thomas Shelton Powers, M.D., Inc.*). Public enforcers, however, may recover civil damages. CAL. BUS. & PROF. CODE §§ 17206, 17206-1 (West 2004). A successful plaintiff may seek attorney fees where the action has been brought as a "private attorney general" action. *See* CAL. CIV. PROC. CODE §1021.5 (West 2004).

148. CAL. BUS. & PROF. CODE § 17200.

149. *Gregory*, 128 Cal. Rptr. 2d at 389.

150. *See* People *ex rel.* Lockyer v. Fremont Life Ins. Co., 128 Cal. Rptr. 2d 463 (Ct. App. 2002), *opinion modified on denial of reh'g*, 129 Cal. Rptr. 2d 298 (Ct. App. 2003).

ferent legal standards. At a minimum, the California regime creates some added uncertainty regarding the boundaries of liability.

b) Florida

Florida has both statutory and common law restraints on unfair competition. Florida's Deceptive and Unfair Trade Practices Act (FDUTPA),[151] enacted in 1973, follows Alternative 1 of the proposed FTC model act: "Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."[152] As a guide to interpreting the scope of this provision, the Act declares that it is the "intent of the Legislature that . . . due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to § 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) as of July 1, 2001."[153] Although court decisions frequently applied the FTC's pre-1983 standards for determining what constitutes an "unfair" or "deceptive" trade practice, more recent decisions consider the modern interpretations of these terms by the FTC.[154] The Florida statute confers broad standing upon "anyone aggrieved by a violation" of the Act, extending to consumers and competitors.[155] The FDUTPA provides for injunctive relief, damages, and attorney fees. Prior versions of the Act allowed only consumers to obtain damages, but recent amendments have broadened the provision to apply to any "person who has suffered a loss as a result of a violation" of the Act.[156] Florida's common law of unfair competition does not appear to extend beyond these statutory limits.

Thus, Florida's statutory unfair competition regime parallels the federal regime. The courts have also consistently held that the analysis of Florida statutory and common law claims of trademark infringement and unfair competition is the same as under the federal trademark law.[157]

---

151. *See* FLA. STAT. § 501.201 (2004).

152. FLA. STAT. § 501.204 (2004).

153. FLA. STAT. §§ 501.202, 501.205 (2004).

154. *See* David J. Federbush, *Obtaining Relief for Deceptive Practices Under FDUTPA*, 75 FLA. BAR J. 22 (Nov. 2001); David J. Federbush, *The Unexplored Territory of Unfairness in Florida's Deceptive and Unfair Trade Practices*, 73 FLA. BAR J. 26 (May 1999).

155. *See generally* Federbush, *supra* note 154.

156. FLA. STAT. § 501.211 (2004).

157. *See* Gift of Learning Found., Inc. v. TGC, Inc., 329 F.3d 792 (11th Cir. 2003); Investacorp, Inc. v. Arabian Inv. Banking Corp. (Investcorp) E.C., 931 F.2d 1519, 1521 (11th Cir. 1991); Monsanto Co. v. Campuzano, 206 F. Supp. 2d 1252 (S.D. Fla. 2002) ("The legal standard for federal trademark and unfair competition, and for common law

c) Georgia

Georgia's unfair competition law comprises four distinct statutes as well as common law protection. Modeled after the Uniform Deceptive Trade Practices Act, Georgia's Deceptive Trade Practices Act (DTPA), enables competitors to enjoin a wide range of deceptive practices.[158] A separate statute prohibits false advertising.[159] Georgia's Unfair Competition Act,[160] dating back well over a century, prohibits the tort of passing off.[161] Federal courts have held that the substantive standards of liability under § 23-2-55 "mirror" the standards of liability applicable under the Lanham Act.[162] The Fair Business Practices Act (FBPA),[163] enacted in 1975, combines Alternatives 1 and 3 of the FTC's proposed Unfair Trade Practices and Consumer Protection Law. Thus, it both provides a general prohibition against unfair and deceptive trade practices and offers a large illustrative list of unfair and deceptive practices. The FBPA, however, is limited to "[u]nfair or deceptive acts or practices in the conduct of *consumer transactions and consumer acts* or practices in trade or commerce,"[164] and therefore denies standing to competitors.[165] Georgia's common law of unfair competition, although evolving beyond pre-*Erie* jurisprudential restraints,[166] does not appear to reach beyond the modern

---

trademark infringement, are essentially the same. . . . To prevail on [] unfair competition claims under Florida common law, [a plaintiff] must show 'deceptive or fraudulent conduct of a competitor and likelihood of consumer confusion.'"); *see also* Great S. Bank v. First S. Bank, 625 So. 2d 463 (Fla. 1993) (applying Lanham-like framework to common law trademark claim and noting that Florida's trademark act, § 495.181, states that "[i]t is the intent of the Legislature that, in construing this chapter, due consideration and great weight be given to the interpretations of the federal courts relating to comparable provisions of the Trademark Act of 1946, as amended (15 U.S.C. §§ 1051 et seq.)").

158. *See* Deceptive Trade Practices Act, GA. CODE ANN. § 10-1-370 (2004).

159. *See* GA. CODE ANN. § 10-1-420 (2004).

160. *See* GA. CODE ANN. § 23-2-55 (2004).

161. *See* Sofate of Am., Inc. v. Brown, 318 S.E.2d 771 (Ga. 1984).

162. *See* Univ. of Ga. Athletic Ass'n v. Laite, 756 F.2d 1535, 1539 n.11 (11th Cir. 1985) (observing that standards under §23-2-55 "are similar, if not identical to those under the Lanham Act").

163. *See* GA. CODE ANN. § 10-1-390 (2004).

164. GA. CODE ANN. § 10-1-393(a) (2004).

165. *See* Friedlander v. PDK Labs, Inc., 465 S.E.2d 670 (Ga. 1996) (emphasis added).

166. *See* Kay Jewelry Co. v. Kapiloff, 49 S.E.2d 19 (Ga. 1948) ("In the light of modern business trends in marketing and advertising, we think the better view of the question is that it is not essential, as a prerequisite to the granting of equitable relief in an action for infringement of a trade name, that actual and direct market competition between the litigants be shown, and that the test as to whether equitable relief is

Lanham Act or Georgia's unfair competition statutes. Thus, Georgia's unfair competition regime does not appear to extend beyond the federal Lanham or FTC Acts.[167]

d) Michigan

Michigan protects consumers and competitors against unfair competition under its Consumer Protection Act (MCPA),[168] passed in 1970, and common law. Rather than employing an open-ended standard like many other states and the FTC Act, the MCPA prohibits more than 30 specific practices, ranging from passing off to particular misleading inducements. For example, the Act prohibits representing that a consumer will receive free goods without clearly and conspicuously disclosing the conditions, terms, or prerequisites to the use or retention of the goods or services advertised.[169] The MCPA does, however, incorporate the FTC Act's standards by authorizing class actions to be pursued on the basis of a federal appellate decision finding a business practice to be unfair or deceptive within the meaning of section 5(a)(1) of the FTC Act.[170] Although initially focused on consumer harm,[171] recent decisions have expanded standing under the MCPA to include competitors.[172]

---

available, should not be limited to those cases where it is shown that there has been an actual diversion of trade from one business to another.")

167. *See* Step Co. v. Consumer Direct, Inc., 936 F. Supp 960, 967 (N.D. Ga. 1994) (observing that the case law indicates Georgia's common law of unfair competition and the GDTPA are "coextensive with the Lanham Act analysis").

168. MICH. COMP. LAWS § 445.901 (2005).

169. MICH. COMP. LAWS § 445.903 (2005). The standard applied in determining whether defendant has engaged in "unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce," in violation of the MCPA, is the same confusion as to source standard applicable to trademark violations under the Lanham Act. *See* Microsoft Corp. v. Compusource Distribs., Inc., 115 F. Supp. 2d 800 (E.D. Mich. 2000); Schreiber Mfg. Co. v . Saft Am., Inc., 704 F. Supp. 759 (E.D. Mich. 1989) (holding that the likelihood of confusion standard applicable to a claim under the MCPA is the same as that involved in federal and state trademark law).

170. Mich. Comp. Laws § 445.911(b)(3)(c) (2005).

171. *See* Wynn Oil Co. v. Am. Way Serv. Corp., 736 F. Supp. 746 (E.D. Mich. 1990), *aff'd in part, rev'd in part on other grounds*, 943 F.2d 595 (6th Cir. 1991); Noggles v. Battle Creek Wrecking, Inc., 395 N.W.2d 322, 324 (Mich. Ct. App. 1986). Section 445.902(d) of the MCPA defines "trade or commerce" narrowly as "the conduct of a business providing goods, property, or service *primarily for personal, family, or household purposes* . . ." (emphasis added).

172. *See* Florists' Transworld Delivery, Inc. v. Fleurop-Interflora, 261 F. Supp. 2d 837, 848 (E.D. Mich. 2003); Action Auto Glass v. Auto Glass Specialists, 134 F. Supp. 2d 897 (W.D. Mich. 2001); John Labatt Ltd. v. Molson Breweries, 853 F. Supp. 965 (E.D. Mich. 1994) (holding that MCPA authorizes suits against competitors so long as the underlying deceptive practice relates to "goods, property, or service primarily for

Michigan's common law of unfair competition prohibits unfair and unethical trade practices that are harmful to one's competitors or to the general public.[173] As applied by Michigan courts, unfair competition consists in the simulation by a person of the name, symbols, or devices employed by a business competitor for the purpose of deceiving the public, or the substitution of the goods or wares of one person for those of another, thus falsely inducing the buying of the goods, and obtaining for the seller profits belonging to a business rival.[174] No one has the right to sell or advertise his or her own business or goods as those of another, so as to mislead the public and injure the other person, nor may any person by imitation or unfair device induce the public to believe that the merchandise he or she is selling is that of another in order to appropriate the value of the reputation which a competitor has acquired for his or her own merchandise.[175] Thus, Michigan courts have followed the general law of unfair competition.[176] As in most other jurisdictions, Michigan's common-law doctrine of unfair competition was ordinarily limited to acts of fraud, bad-faith misrepresentation, misappropriation, or product confusion,[177] and has retained its 1930s era constraints.[178] Since the passage of the MCPA, there has been little reason to invoke the Michigan common law of unfair competition in pursuing deceptive advertising and related claims.

---

personal, family, or household purposes"). *But see* Cosmetic Dermatology and Vein Ctrs. of Downriver, P.C. v. New Faces Skin Care Ctrs., Ltd., 91 F. Supp. 2d 1045 (E.D. Mich. 2000) (rejecting an MCPA lawsuit between competitors on the ground that there was no "purchase or transaction" involving goods or property "primarily for personal, family, or household purposes").

173. *See* Clairol, Inc. v. Boston Disc. Ctr., Inc., 608 F.2d 1114, 1118 (6th Cir. 1979).

174. *See* James Heddon's Sons v. Millsite Steel & Wire Works, 128 F.2d 6 (6th Cir. 1942); Moon Bros. v. Moon, 1 N.W.2d 488 (Mich. 1942); Carbonated Beverages v. Wisko, 297 N.W. 79 (Mich. 1941); Schwannecke v. Genesee Coal & Ice Co., 247 N.W. 761 (Mich. 1933).

175. *See* James Heddon's Sons v. Millsite Steel & Wire Works, 128 F.2d 6 (6th Cir. 1942); Carbonated Beverages v. Wisko, 297 N.W. 79 (Mich. 1941); Williams v. Farrand, 50 N.W. 446 (Mich. 1891).

176. *See* A & M Records, Inc. v. MVC Distrib. Corp., 574 F.2d 312, 313 (6th Cir. 1978); Tas-T-Nut Co. v. Variety Nut & Date Co., 245 F.2d 3, 8 (6th Cir. 1957).

177. *See generally* 54A Am. Jur. 2d *Monopolies, Restraints of Trade and Unfair Trade Practices* § 1107 (2004); *see also* In re MCI Telecomm. Corp., 612 N.W.2d 826, 837 (Mich. App. 2000) (noting that Michigan's Telecommunications Act extends further than the common law of unfair competition in regulating conduct that is "adverse to the public interest").

178. *See, e.g.*, Burns v. Schotz, 72 N.W.2d 149 (Mich. 1955); Good Housekeeping Shop v. Smitter, 236 N.W. 872 (Mich. 1931). *But cf.* Boron Oil Co. v. Callanan, 213 N.W.2d 836 (Mich. 1973) (loosening the competition requirement).

Although it appears that Michigan's unfair competition regime largely parallels the scope and remedies available under federal law, the MCPA's somewhat different formulation of standards could potentially afford wider coverage.

e) North Carolina

The North Carolina Unfair Trade Practices Act (NCUTPA),[179] enacted in 1969, adopted Alternative 1 of the FTC's proposed Unfair Trade Practices and Consumer Protection Law. It does not expressly tie interpretation of its terms to interpretations given by the FTC, although courts have borrowed the expansive definition of "deception" that the federal courts have traditionally employed in interpreting the FTC Act.[180] The statute expressly provides for a broad private right of action extending to both consumers and businesses (including competitors).[181] It also affords victorious plaintiffs treble damages.[182] Courts may, in their discretion, award attorney fees.[183]

Because common law remedies were ineffective, the North Carolina legislature enacted the statute to provide a private cause of action for aggrieved consumers.[184] In order to prevail under the statute, plaintiff must demonstrate the existence of three factors: "(1) an unfair or deceptive act or practice, . . . (2) in or affecting commerce, and (3) which proximately caused actual damage to the plaintiff . . . ."[185] In interpreting the first element, courts apply the broader, pre-1983 standard for deception. A trade practice is "deceptive" if it has capacity or tendency to deceive; proof of actual deception is not required. A trade practice is "unfair" when it of-

179. *See* N.C. GEN. STAT. § 75-1.1 (2005).

180. *See* Hageman v. Twin City Chrysler-Plymouth Inc., 681 F. Supp. 303 (M.D.N.C. 1988); *cf.* E. Roofing & Aluminum Co. v. Brock, 320 S.E.2d 22 (N.C. 1984) (same); State *ex rel.* Edmisten v. J.C. Penney Co., 233 S.E.2d 895 (N.C. 1977) (noting that federal decisions construing the FTC Act may furnish some guidance to the meaning of this section, but federal court decisions are not controlling).

181. *See* McDonald v. Scarboro, 370 S.E.2d 680 (N.C. Ct. App. 1988); Harrington Mfg. Co. v. Powell Mfg. Co., 248 S.E.2d 739 (N.C. Ct. App. 1978) (holding that the statute applies to disputes between competitors, and not only to dealings between buyers and sellers).

182. *See* N.C. GEN. STAT. § 75-16 (2005). *See generally* Robert Morgan, *The People's Advocate in the Marketplace—The Role of North Carolina's Attorney General in the Field of Consumer Protection*, 6 WAKE FOREST INTRAMURAL L. REV. 1 (1969).

183. *See* N.C. GEN. STAT. § 75-16.1 (2005); Canady v. Crestar Mtg. Corp, 109 F.3d 969 (4th Cir. 1997).

184. *See* Bhatti v. Buckland, 400 S.E.2d 440 (N.C. 1991).

185. *See* Cash v. State Farm Mut. Auto. Ins. Co., 528 S.E.2d 372, 375 (N.C. Ct. App. 2000).

fends established public policy as well as when the practice is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.[186]

Litigation under North Carolina's UTPA statute involving competitors has been particularly brisk.[187] In *Polo Fashions, Inc. v. Craftex, Inc.*,[188] the owner of the "Polo" and "Ralph Lauren" trademarks brought suit under the Lanham Act and the North Carolina Unfair Trade Practices Act. The court held that while damages could not be awarded under the Lanham Act because 15 U.S.C. § 1111 requires the statutory notice or registration before damages are permitted, damages were available (and trebled) under the state statute.[189] Thus, the North Carolina unfair competition statute may well impose broader liability than federal law.

f) South Carolina

The South Carolina Unfair Trade Practices Act (SCUPTA) was initially enacted in 1962 and was amended in 1971 in light of the FTC proposed act.[190] In its amended form, the SCUPTA adopts Alternative 1 of the FTC's proposal but provides much more open-ended standing. Under the Act, "[a]ny person who suffers any ascertainable loss of money or property,"[191] not merely consumers purchasing for personal use, may bring a private action under this statute. Thus, competitors have standing under this statute.[192] Private parties are entitled to recover actual damages (which shall be trebled in cases of willful or knowing violations of the Act) as well as reasonable attorney's fees and costs,[193] although only the Attorney General may obtain injunctive relief under the statute.[194]

In order to make out a claim under this statute, a plaintiff must establish: (a) unfair or deceptive act or practice in the conduct of trade or commerce; (b) that the plaintiff suffered actual, ascertainable damages as a re-

186. *See* Huff v. Autos Unlimited, Inc., 477 S.E.2d 86 (N.C. Ct. App. 1996).

187. *See* EDMUND W. KITCH & HARVEY S. PERLMAN, INTELLECTUAL PROPERTY AND UNFAIR COMPETITION 153 (5th ed. 1998).

188. 816 F.2d 145 (4th Cir. 1987).

189. *But see* Sideshow, Inc. v. Mammoth Records, Inc., 751 F. Supp. 78, 80 (E.D.N.C. 1990) (limiting *Polo Fashions* to intentional infringement and holding that the North Carolina automatic trebling statute does not apply to innocent and unintentional infringement of unregistered trademarks because the plaintiff is "not an injured consumer and has several other adequate remedies").

190. *See* S.C. CODE ANN. § 39-5-10 et seq. (2004).

191. S.C. CODE ANN. § 39-5-140.

192. *See* Global Prot. Corp. v. Halbersberg, 503 S.E.2d 483, 487 (S.C. Ct. App. 1998).

193. S.C. CODE ANN. § 39-5-140.

194. S.C. CODE ANN. § 39-5-50.

sult of the defendant's use of the unlawful trade practice; and (c) that the unlawful trade practice engaged in by the defendant had an adverse impact on the public interest.[195] The scope of unfair or deceptive trade practices under the Act "will be guided by the interpretations given by the Federal Trade Commission and the Federal Courts to § 5(a)(1),"[196] although as in North Carolina, South Carolina courts continue to apply the somewhat broader pre-1983 federal standard of deception: a practice is "deceptive" when it has a tendency to deceive.[197] An act is "unfair" when it is offensive to public policy or when it is immoral, unethical, or oppressive.[198] To satisfy the second requirement, the plaintiff must establish actual damage as well as causation. The third element mirrors the "public interest" requirement of the FTC Act.[199] An adverse impact upon the public interest can be established by showing that an unfair or deceptive act has the potential for repetition. This can be established by a showing that the same kind of actions occurred in the past or by showing that company's procedures create a potential for repetition of the unfair and deceptive acts.[200]

There are at least two significant reasons to believe that the application of the SCUPTA is not merely duplicative of federal Lanham Act causes of action and could expose behavioral marketing firms to more liberal liability standards. First, a finding of liability under the SCUPTA entitles the plaintiff to recover attorney fees and costs and opens up the possibility of an award of treble damages should willfulness be established.[201] Second, as noted above, the South Carolina courts apply the more capacious pre-1983 standards for deception and unfairness.

A 1996 case decided under the SCUPTA, although not involving Internet-related activities, suggests that South Carolina courts might consider advertisements that obscure website banners to be troubling. *Daisy Outdoor Advertising Company, Inc. v. Abbott*[202] involved two fiercely

---

195. *See* Havird Oil Co. v. Marathon Oil Co., 149 F.3d 283, 291 (4th Cir. 1998).

196. S.C. CODE ANN. § 39-5-20(b).

197. *See* Johnson v. Collins Entm't Co., 564 S.E.2d 653, 665 (S.C. 2002); Williams-Garrett v. Murphy, 106 F. Supp. 2d 834 (D.S.C. 2000).

198. *See id*.

199. *See* Daisy Outdoor Advert. Co. v. Abbott, 473 S.E.2d 47, 49-50 (S.C. 1996); Noack Enters., Inc. v. Country Corner Interiors, 351 S.E.2d 347, 350-51 (S.C. Ct. App. 1986).

200. *See* Lib. Mut. Ins. Co. v. Employee Res. Mgmt., Inc., 176 F. Supp. 2d 510, 516 (D.S.C. 2001).

201. *See* State *ex rel*. Medlock v. Nest Egg Soc'y Today, Inc., 348 S.E.2d 381, 383 (S.C. Ct. App. 1986) (finding "willful" violation when the party committing the violation knew or should have known that his conduct violated the Act).

202. 473 S.E.2d 47 (S.C. 1996).

competitive billboard sign companies. After one of the companies (Abbott) invested in the construction of a large billboard along a stretch of highway, a competing advertising company owning an adjacent parcel of land (Daisy) erected a sign entirely blocking Abbott's sign. The second billboard violated a state law regulating the placement of billboards. After being notified of this violation, Daisy replaced the illegal sign with a "For Sale" sign advertising the property on which the sign is located.[203] "For Sale" signs were exempt from the state statute regulating placement of billboards.[204] Like Daisy's previous sign, the unregulated "For Sale" sign completely blocked the Abbott billboard, requiring Abbott to find an alternative location for its customer's advertisement. The trial court held that Daisy's actions constituted an unfair or deceptive act or practice in the conduct of trade or commerce, caused harm to Abbott's business, and adversely affected the public interest. It awarded Abbott treble damages. On appeal, the intermediate appellate court overturned the decision under the "public interest" requirement, applying a more stringent standard.[205] The South Carolina Supreme Court reversed, reinstating the trial court's decision.[206]

3. State Legislative Spyware and Adware Initiatives

In addition to this diverse, complex, and rather amorphous landscape of state unfair competition statutory and common law, more than half of the states have either recently enacted or are actively considering legislation specifically targeting spyware. Chart I summarizes this explosion of legislative activity.[207]

The extent to which these laws would regulate behavioral marketing activities depends on several variables—requirements related to the means by which software triggering advertisements is installed on users' computers (notice, consent, ease of removal); restrictions on specific practices (for example, using trademarks of others to trigger advertising delivery, keystroke monitoring); scope of liability (whether it extends to advertisers as well as companies that distribute advertisements); enforcement (public, private right action, class action); and remedies (statutory damages, treble damages, fees and costs). Behavioral marketing companies have pushed for relatively lax requirements whereas traditional web publishers have

---

203. Under § 57-25-140(E) of South Carolina's Highway Advertising Control Act, a billboard may not be built within 500 feet of another billboard.

204. *See* S.C. CODE ANN. § 57-25-140(A)(5) and (D) (2004).

205. 451 S.E.2d 394, 397 (S.C. Ct. App. 1994).

206. 473 S.E.2d 47, 48 (S.C. 1996).

207. *See infra* Supplement for Chart I.

lobbied for strong notice, consent, and removal requirements.[208] The Internet Alliance, a consortium of leading Internet businesses including America Online, eBay and Microsoft, have opposed spyware legislation out of concern that it could unintentionally hamper some means of doing legitimate business on the Internet.[209] Many of the pending bills (Alabama, Arizona, Arkansas, California, Delaware, Illinois, Iowa, Kansas, Maryland, Massachusetts, Missouri, Nebraska, New Hampshire, New York, Texas, Virginia, and Washington) opt for weaker notice and consent requirements. A few states, most notably Alaska and Utah, have favored stronger regulation.

Utah became the first state to enact spyware legislation in March 2004.[210] Utah's Spyware Control Act prohibits installation of spyware or adware (triggered by use of a trademark of another) without the computer user's informed consent. The Act empowers website owners (or registrants), trademark or copyright owners, or authorized website advertisers harmed by such activities to bring suit. The legislation grew out of lobbying by website owners seeking to prevent targeting of their sites by behavioral marketing firms. Shortly thereafter, Overstock.com, a Utah-based online retailer, sued its competitor, Massachusetts-based SmartBargains.com, for allegedly serving pop-up ads over Overstock.com's site in violation of Utah's Spyware Control Act. This lawsuit also alleged common law causes of action based on unfair competition and interference with prospective economic advantage.[211] In an unrelated action,

---

208. *See* John Borland, *States join spyware battle*, CNET NEWS.COM, Mar. 4, 2004, http://news.com/States+join+spyware+battle/2100-1024_3-5170263.html; Ben Edelman, *California's Toothless Spyware Law* (Sept. 29, 2004), http://www.benedelman.org/news/092904-1.html; Tobi Elkin, *A Conversation with Claria's Privacy Chief*, MEDIAPOST Q&A PART II, Aug. 5, 2004, http://www.mediapost.com/PrintFriend.cfm?articleId=262798; RED HERRING, *A bill on the California governor's desk seeks to block spyware on your PC, but some say it will do little to curb annoying pop-ups and intrusive software*, Sept. 17, 2004, http://www.redherring.com/article.aspx?a=10859&hed=Should+spyware+be+a+crime?; Memorandum in Support of Plantiff WhenU.com Inc.'s Application for a Temporary Restraining Order and Motion for Preliminary Injunction at 7 n.6 (Apr. 12, 2004), http://www.benedelman.org/spyware/whenu-utah/whenu-memotro_pi.pdf (noting lobbying efforts by 1-800 Contacts).

209. *See* Stefanie Olsen, *Utah judge freezes anti-spyware law*, CNET NEWS.COM, June 22, 2004, http://news.com.com/Utah+judge+freezes+anti-spyware+law/2100-1024_3-5244151.html.

210. *See* Utah Spyware Control Act, H.B. 323 (codified at UTAH CODE ANN. § 13-4-1 (2005)); Brice Wallace, *Spyware Act has detractors*, DESERET MORNING NEWS, Mar. 19, 2004, *available at* http://deseretnews.com/dn/print/1,1442,595050017,00.html.

211. *See* Janis Mara & Ron Miller, *Lawsuit Filed Under Utah's Challenged Anti-Spyware Act: Massachusetts based companies fighting it out in Utah*, INTERNET NEWS, May 19, 2004, http://internetnews.com/ec-news/article.php/3356441. Shortly before the

WhenU.com brought an action seeking to have the Utah legislation declared invalid under the Commerce Clause. In June 2004, a state court granted a preliminary injunction blocking the Act from taking effect.[212]

In March 2005, Utah amended its Spyware Control Act in an attempt to circumvent the Commerce Clause bar.[213] The revised act retains the strong form approach—prohibiting display of pop-up advertisements in response to a mark without authorization and imposing liability upon an advertiser who receives actual notice from a mark owner of the use of its mark to trigger advertisements and fails to take reasonable steps to stop violations. It seeks to address the Commerce Clause infirmity by exempting from liability those who request information about a user's state of residence prior to sending spyware or pop-up advertisements and the user indicates a residence outside of Utah. The Act provides for both public enforcement and a private right of action by a mark owner who does business in Utah and is directly and adversely affected. It also awards treble damages in the case of willful and knowing violations.

C. Testing the Least Common Denominator Hypothesis and Policy Implications

The review of state unfair competition law, the early state legislative forays into spyware legislation, and the first lawsuits under state laws support the hypothesis that the most restrictive state law regimes have nationwide effect on Internet-related activities. The common law of South Carolina or spyware legislation in Utah directly affect Internet-related businesses based anywhere in the nation due to the ubiquity of the World Wide Web and the minimal standards for personal jurisdiction. Furthermore, the process by which the first and arguably most restrictive state spyware laws came into existence demonstrates that state legislation can result from the lobbying efforts of even one persistent company.

Given the unpredictability of the state unfair competition law, it is perhaps not surprising that Claria chose to settle many of the lawsuits it has

---

passage of the first Utah anti-spyware legislation, an active sponsor of that legislation (1-800-Contacts) brought suit against Coastal Contacts, a competitor that sponsored advertisements on WhenU.com's advertising platform targeting 1-800-Contacts' website. *See Draper firm files lawsuit over pop-up ads*, DESERET MORNING NEWS, Mar. 19, 2004, *available at* http://deseretnews.com/dn/print/1,1442,595050012,00.html.

212. *See* Stefanie Olsen, *Utah judge freezes anti-spyware law*, CNET NEWS.COM, June 22, 2004, http://news.com.com/Utah+judge+freezes+anti-spyware+law/2100-1024_3-5244151.html.

213. *See* H.B. 104, 2005 Gen. Sess. (Utah 2005), *available at* http://www.le.state.ut.us/~2005/bills/hbillenr/hb0104.htm.

faced.[214] The range of states in which these cases were brought supports the nationwide exposure that Internet-based businesses face under personal jurisdiction jurisprudence and the reality that the state with the most restrictive rules serves as a least common denominator to which a prudent company must adhere.

Due to the recent vintage of the state spyware legislation, there has not been much litigation. Although many of these statutes have common elements, they will tend to diverge as courts interpret the provisions. As with state common law and existing unfair competition legislation, the provisions of the most restrictive state will set the bar for prudent Internet-based businesses.

Thus, the premise of Justice Brandeis's often cited aphorism about states serving as "laboratories" on policy innovation does not hold in the case of spyware regulation. The decisions of any one state will have significant impacts on activities in other states due to the ubiquity of the Internet. The least common denominator hypothesis suggests that spyware should be governed at the federal level and that state legal regimes—whether common law or statutory—should be preempted.

IV. FEDERAL SPYWARE INITIATIVES AND FEDERALISM IMPLICATIONS

The rapidity with which the Internet evolves creates unprecedented challenges for overworked deliberative bodies like legislatures and courts. For example, the rush to register trademarks of others as domain names and the scourge of computer viruses occurred in ways that few foresaw. The 1998 Digital Millennium Copyright Act, which sought to ensure the protection of copyrighted works in the digital environment,[215] failed to anticipate the emergence of peer-to-peer technology less than a year later. Similarly, the concerns surrounding spyware appeared suddenly and have generated a good amount of litigation and legislative hand-wringing.

Given the advantages of uniform standards for regulating Internet-related activities, are there systemic reasons to question the adequacy of federal regulators (FTC) and the federal legislature to address the public policy concerns raised by spyware? Furthermore, do these reasons over-

214. Stefanie Olsen, *Pop-up purveyor Claria settles suits*, CNET NEWS.COM, Aug. 31, 2004, http://news.com.com/Pop-up+purveyor+Claria+settles+suits/2100-1024_3-5333003.html; Stefanie Olsen, *Web publishers settle with Gator*, CNET NEWS.COM, Feb. 7, 2003, http://news.com.com/Web+publishers+settle+with+Gator/2100-1023_3-983870.html.

215. *See* S. REP. NO. 105-190, at 8 (1998); *see also* H.R. REP. NO. 105-551, pt. 2, at 23 (1998).

ride the advantages of national uniformity and coordinated policy development? This section reviews the actions of the FTC and Congress in coming up to speed in addressing the policy concerns. During the relatively short time period that spyware has aroused concern, federal authorities have been attentive to the emerging problems. Although no federal legislation has yet passed, Congress has sought to balance the complex considerations and appears likely to pass balanced legislation which preempts some state initiatives. Based on the foregoing analysis, Congress should preempt state regulation of spyware. The general provisions of the Lanham Act and the FTC Act largely parallel state unfair competition and consumer protection regimes. Preempting the state counterparts to these laws in the context of Internet-related activities would substantially harmonize legal standards, reduce business planning costs, and eliminate needless and costly litigation of vague and uncertain state causes of action.

A. FTC Enforcement and Regulatory Analysis

Federal authority over deceptive practices falls within the general jurisdiction of the Federal Trade Commission. The FTC Act authorizes the agency to promulgate rules and initiate enforcement proceedings directed at deceptive and unfair trade practices.

As the concerns relating to spyware emerged, the FTC began oversight of this area, responding to consumer complaints and studying the problems. Since 1998, the agency has brought fourteen cases relating to spyware.[216] For example, in 2003, the FTC initiated an enforcement proceeding against D Squared Solutions, a San Diego based software vendor that sold pop-up blocking software. D Squared Solutions promoted the software by bombarding consumers with pop-up advertisements through the use of a feature within Microsoft's Windows operating system that allows network administrators to notify users about critical maintenance. D Squared Solutions would then offer consumers the opportunity to purchase its software as a solution to such annoyance.[217] Under its general authority to combat unfair and deceptive trade practices, the FTC successfully obtained a court order barring D Squared Solutions from sending pop-up ads to computer users through this security hole.[218]

---

216. *See* FTC Spyware Report, *supra* note 8, at 20 n.204; *see also* Bob Sullivan, *Federal spyware crackdown continues: But relief for consumers may be slow in coming*, MSNBC, Oct. 12, 2004, http://msnbc.msn.com/id/6228258.

217. *See* Stefanie Olsen, *Pop-up purveyor fights FTC*, CNET NEWS.COM, Dec. 10, 2003, http://news.com.com/Pop-up+purveyor+fights+FTC/2100-1032_3-5119482.html.

218. *See FTC Obtains Order Barring Pop-up Spam Scam, Urges Consumers to Take Steps to Protect Themselves*, Nov. 6, 2003, http://www.ftc.gov/opa/2003/11/

The FTC has also devoted substantial resources to monitoring spyware activities and studying regulatory solutions. In April 2004, the agency sponsored a full day public workshop exploring the public policy issues surrounding spyware.[219] In March 2005, it released a detailed study, entitled "Monitoring Software on your PC: Spyware, Adware, and Other Software," seeking to define the spyware problem, measuring its effects, exploring industry responses, and assessing enforcement and regulatory policies. At this stage, the FTC believes that its existing regulatory authority enables it to address present concerns relating to spyware adequately.[220] Although some critics have complained that the FTC has not been sufficiently proactive in confronting the threats posed by spyware,[221] the FTC's deliberative and cautious approach ensures that the broad range of considerations will be fully considered and provides an opportunity for nonregulatory solutions to emerge.[222]

B. Legislative Proposals

Spyware first appeared on the federal legislative radar screen in 2000. Senator John Edwards introduced the first bill to address surreptitious collection through the use of computer programs.[223] This bill would have required conspicuous notice of such data collection activities by software distributors. With growing concern about the effects of spyware, legislative interest in the field gained momentum in in 2003.[224] Several bills have

---

dsquared.htm; Grant Gross, *FTC Shuts Down Pop-Up Ad Spammers*, PC WORLD, Aug. 9, 2004, http://www.pcworld.com/news/article/0,aid,117299,00.asp.

219. *See* FTC, Monitoring Software on your PC: Spyware, Adware, and Other Software (Apr. 19, 2004), http://www.ftc.gov/bcp/workshops/spyware.

220. *See* Declan McCullagh, *FTC officials blast spyware measures*, CNET NEWS.COM, Apr. 29, 2004, http://news.com.com/FTC+officials+blast+spyware+measures/2100-1023_3-5202016.html (noting FTC concerns that proposed laws could harm legitimate software products and innovation).

221. *See* Declan McCullagh, *Few Solutions Pop Up at FTC Adware Workshop*, CNET NEWS.COM, Apr. 19, 2004, http://news.com.com/Few+solutions+pop+up+at+FTC+adware+workshop/2100-1028_3-5195222.html.

222. Declan McCullagh, *Making the wrong move against spyware*, CNET NEWS.COM, May 2, 2005, http://news.com.com/Making+the+wrong+move+against+spyware/2010-1071_3-5690270.html (advocating a cautious approach to spyware regulation and allowing enforcement under existing regulatory authority to proceed).

223. *See* Spyware Control and Privacy Protection Act of 2000, S. 3180, 106th Cong., 2d Sess. (2000), *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:S.3180:.

224. Declan McCullagh, *Washington wakes up to spyware, adware*, CNET NEWS.COM, Apr. 28, 2004, http://news.com.com/Washington+wakes+up+to+spyware%2C+adware/2100-1023_3-5201819.html.

since been floated,[225] with Representative Mary Bono's Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) garnering the most attention and support.[226] The House of Representatives passed the SPY ACT on May 23, 2005.[227]

The SPY ACT would prohibit the following acts: (1) taking control of the computer by various specified means; (2) modifying computer settings related to use of the computer or to the computer's access to or use of the Internet by various means; (3) collecting personally identifiable information through the use of a keystroke logging function; (4) inducing the owner or authorized user of the computer to disclose personally identifiable information or install software through various deceptive means; and (5) removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer.[228] The Act prohibits collection of personal information without notice and consent, subject to various exceptions and limitations on liability for telecommunication entities.[229] The Act also delegates rulemaking authority to the FTC[230] and vests the agency with enforcement powers.[231]

Of most importance to the issues addressed in this Article, section 6 of the SPY ACT preempts state law regulating spyware:

> SEC. 6. EFFECT ON OTHER LAWS.
>
> (a) Preemption of State Law-
>
> (1) PREEMPTION OF SPYWARE LAWS- This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly regulates--
>
> (A) unfair or deceptive conduct with respect to computers similar to that described in section 2(a);
>
> (B) the transmission or execution of a computer program similar to that described in section 3; or

225. *See* Benjamin Edelman, *"Spyware": Research, Testing, Legislation, and Suits*, http://www.benedelman.org/spyware/#legislation (last visited July 13, 2005).

226. *See* H.R. 29, 109th Cong. (2005) (formerly H.R. 2929).

227. Roy Mark, *House Approves Anti-Spyware Bills*, INTERNET NEWS, May 23, 2005, http://www.internetnews.com/bus-news/article.php/3507211. A prior version of this bill passed in 2004. *See* Roy Mark, *House Passes Anti-Spyware Bill*, INTERNET NEWS, Oct. 6, 2004, http://www.internetnews.com/bus-news/article.php/3417891.

228. *See* SPY ACT, § 2.

229. *See id.*, § 3.

230. *See id.*, § 10.

231. *See id.*, § 4.

> (C) the use of computer software that displays advertising content based on the Web pages accessed using a computer.
>
> (2) ADDITIONAL PREEMPTION-
>
> (A) IN GENERAL- No person other than the Attorney General of a State may bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.
>
> (B) PROTECTION OF CONSUMER PROTECTION LAWS- This paragraph shall not be construed to limit the enforcement of any State consumer protection law by an Attorney General of a State.
>
> (3) PROTECTION OF CERTAIN STATE LAWS- This Act shall not be construed to preempt the applicability of--
>
> (A) State trespass, contract, or tort law; or
>
> (B) other State laws to the extent that those laws relate to acts of fraud.
>
> (b) Preservation of FTC Authority- Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law, including the authority to issue advisory opinions (under part 1 of volume 16 of the Code of Federal Regulations), policy statements, or guidance regarding this Act.

This provision serves the purpose of harmonizing governance of spyware. It accomplishes this goal on both the standard setting and enforcement levels. By preempting state enforcement and forgoing a private right of action, this provision may go too far. First, state regulators may well have resources and information that could complement federal enforcement. Second, such a restrictive enforcement regime risks underenforcement to the extent that interest groups opposing regulation unduly influence federal authorities. Nonetheless, exclusive federal enforcement has the virtue of ensuring a more cohesive and predictable regulatory environment.

V. GENERAL IMPLICATIONS FOR INTERNET GOVERNANCE

In little more than a decade, the Internet has revolutionized the way commerce and society function, becoming a critical means of communicating, transacting, and entertaining. At the same time, however, the Internet has spawned threats to personal and financial privacy, as well as a host of annoyances ranging from unsolicited e-mails to interferences with the

operation of end users' computers. Neither netiquette, market forces, nor technological fixes have adequately addressed several of these problems, prompting calls for government intervention. This Article has focused on which level of government—state or federal—is best suited for regulating Internet-related activities. In the framework suggested by Justice Brandeis, can states serve as laboratories of policy experimentation in cyberspace without jeopardizing the nation as a whole?

Using spyware and adware as a case study, this Article demonstrates that states cannot serve as independent laboratories of policy experimentation due to the inherent ubiquitous nature of the Internet. The experimentation of any one state creates national exposure, thereby making the policies of that state a national standard. State unfair competition law—encompassing both common law and state statutes—has this effect. Internet businesses can be hauled into court in any state and therefore must consider legal risks in every state. The problem is compounded by the amorphous character of unfair competition law.

This analysis can be generalized beyond the spyware area to almost all Internet-related activities. There are inherent technological limitations on the ability of states to experiment in spam, phishing, malware, privacy, or ecommerce policy without having significant effects on commerce outside of their borders.[232] The ubiquity of the Internet makes state borders largely irrelevant. Therefore, there should be a strong presumption in favor of at least national regulatory governance of most Internet-related activities.

The logic of the Article suggests that even the federal level may be too provincial for addressing Internet-related activities. Governance of many aspects of the Internet properly belongs on the global stage—whether private, public, or some combination thereof. As recognized in prior analyses

232. The doctrine of trespass to chattels is an exception to this rule because chattels will have a specific locus. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1067 (N.D. Cal. 2000); Steven Kam, *Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427 (2004). Thus, the California rule does not prevent Minnesota or Massachusetts from experimenting with their own rules without creating a national standard. Businesses have control over which servers from which they harvest data, thereby enabling them to avoid liability in any particular states by not targeting servers in those states. There may well be benefits to a national rule in this area, *cf.* Dan Burk, *The Trouble With Trespass*, 4 J. SMALL & EMERGING BUS. L. 27 (2000), but unlike with spyware, companies can limit their exposure to the rules of any state through the design of their code. For example, programmers can customize their automated bots to target servers in particular states in accordance with the applicable regulatory requirements and standards.

advocating global regulatory solutions to Internet-related activities,[233] regulation of Internet activities in any one country can have effects beyond the borders of that particular nation.[234] Therefore, global or at least coordinated or harmonized regulatory standards for Internet activities would serve to create a clear and consistent regulatory environment and avoid the de facto standards from becoming the most restrictive of any nation. The allocation of domain names, which were initially handled within the United States through a government contract with Network Solutions Inc. (NSI), now takes place under the auspices of the Internet Corporation for Assigned Names and Numbers (ICANN), an international entity.[235] This has alleviated the problem of conflicting standards in the assignment of domain names. On larger issues of Internet governance, however, the world is far from consensus.[236]

In some respects, however, nation-based regulation may provide some of the advantages of policy experimentation that Justice Brandeis endorsed. International jurisdiction, country codes, and language erect partial barriers that limit the extent to which legal regulation from one nation spills over into the governance of activities in other nations. In these circumstances, nations can obtain the benefits of seeing how particular regulatory constraints affect economic activities. We are seeing the effects of such experimentation in the areas of privacy,[237] database protection,[238] spyware,[239] and keyword advertising.[240] Nonetheless, there is some risk

---

233. *See* William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* (1997), http://www.ecommerce.gov/framewrk.htm (discussing the need for a set of globally recognized commercial law rules); Kalama Lui-Kwan & Kurt Opsahl, Symposium, *The Legal and Policy Framework for Global Electronic Commerce: A Progress Report*, 14 BERKELEY TECH. L.J. 503 (1999).

234. *Cf.* Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 261 (2002).

235. *See* Angela Proffitt, *Drop the Government, Keep the Law: New International Body for Domain Name Assignment Can Learn from United States Trademark Experience*, 19 LOY. L.A. ENT. L. REV. 601, 603 (1999); *cf.* A. Michael Froomkin, *Of Governments and Governance*, 14 BERKELEY TECH. L.J. 617 (1999).

236. *See* Irwin Arieff, *UN panel fails to agree on how to govern Internet*, REUTERS, July 14, 2005, *available at* http://www.wgig.org/docs/Reuters.htm.

237. *See* Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

238. *See* Stephen M. Maurer et al., *Europe's Database Experiment*, 294 SCI. 789-90 (2001); James Boyle, *A natural experiment*, FINANCIAL TIMES, Nov. 22, 2004, *available at* http://news.ft.com/cms/s/4cd4941e-3cab-11d9-bb7b-00000e2511c8.html.

239. *See* Dawn Kawamoto, *German court: Pop-ups need permission*, CNET NEWS.COM, Mar. 26, 2004, http://news.com.com/2100-1024-5180240.html; *Spyware Bill*

that such experiments will have undesirable spillover effects and that nations may use different constraints to serve protectionist goals.

Overall, the Internet's broad reach generally favors national and possibly global regulatory policies in order to promote a consistent regulatory environment. In some contexts, the locus of activity (as in the case of trespass to chattels) or practical constraints on activities (such as language and country codes) may create conditions in which sub-national or sub-global regulation is possible without spilling over into other jurisdictions. Policymakers should carefully consider the effects of such spillovers in allocating regulatory authority over Internet activities.

Pushes $10,000 Fine, AUSTRALIANIT, May 12, 2005, http://australianit.news.com.au/articles/0,7204,15262588%5E15331%5E%5Enbv%5E15306-15318,00.html.

240. *See Nanterre Court (TGI), emergency order, Hotels Méridien v. Google France* (Dec. 16, 2004), *available at* http://www.juriscom.net/jpt/visu.php?ID=631.

Chart I

Survey, State Spyware Legislation*		
State	**Status**	**Summary**
Alabama	Pending	S.B. 122 "Consumer Protection Against Computer Spyware Act" Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information; (3) take control of the consumer's computer; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce installation of spyware. **Enforcement**: Public. **Remedies**: Criminal penalties (Class B misdemeanor).
Alaska	Sent to Governor (as of 5/10/05)	S.B. 140 "An Act Relating to Spyware and Unsolicited Advertising" Prohibits certain popup ads displayed by spyware, including popups displayed in response to a specific web address or trademark without the consent of the site or mark owner; consumer consent is not a defense, and proof of trademark infringement is not a requirement. Exempts from liability distributors of software or services that remove spyware. **Enforcement**: Private right of action under existing unfair business practices statute.
Arizona	Enacted (4/18/05)	H.B. 2414; Chapter 136 Prohibits transmission, through intentionally deceptive means, of computer software that modifies certain settings, collects personally identifiable information, or takes control of the computer. **Enforcement**: Attorney General; a computer software provider or a website or trademark owner who is adversely affected. **Remedies**: Injunctive relief; greater of actual damages or $100,000 for each separate violation; treble damages for repeat violators; costs and attorney fees.
* Sources: National Conference of State Legislatures, *2005 State Legislation Relating to Internet Spyware or Adware*, http://www.ncsl.org/programs/lis/spyware05.htm (last visited Aug. 9, 2005); Ben Edelman, *State Spyware Legislation*, http://www.benedelman.org/spyware/legislation (last visited Jul. 20, 2005).		

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Arkansas	Enacted (4/13/05)	H.B. 2904; Act 2255 "Consumer Protection Against Computer Spyware Act" Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information; (3) take control of the consumer's computer; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce installation of spyware. **Enforcement**: Attorney General, under Deceptive Trade Practices Act. **Remedies**: Fines to be paid to "Spyware Monitoring Fund," which shall be used for enforcement and related expenses.
Arkansas	Enacted (4/14/05)	H.B. 2261; Act 2312 "An act to make an appropriation for expenses associated with spyware monitoring for the office of Attorney General" H.B. 2344; Act 2313 "An act to make an appropriation for expenses associated with spyware monitoring for the Department of Information Systems"
California	Enacted (9/28/04)	"Consumer Protection Against Computer Spyware Act" (Chapter 32 (§ 22947 et seq.); Division 8 of the Business and Professions Code) Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information; (3) take control of the consumer's computer; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce installation of spyware. **Enforcement**: Leaves open who may enforce prohibitions. **Remedies**: Unstated.

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
California	Pending	S.B. 92 Provides for enforcement and remedies for the "Consumer Protection Against Computer Spyware Act" **Enforcement**: Establishes a private right of action for recipients of spyware; public. **Remedies**: Allows parties to recover liquidated damages of $1,000 per violation, attorney's fees, and costs; makes violation of the prohibitions a crime, punishable as either a misdemeanor or felony.
California	Pending	S.B. 355 States that a purpose of the "Consumer Protection Against Computer Spyware Act" is to improve security on the Internet.
Delaware	Pending	S.B. 124 Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information; (3) take control of the consumer's computer; or (4) prevent an authorized user's reasonable efforts to block or disable spyware. **Enforcement**: Public enforcement. **Remedies**: Actual damages, attorney fees, and costs of at least $1,000 and up to $1,000,000; treble damages for willful violations.

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Florida	Pending	S.B. 2162 "Internet Computer Fraud" Prohibits a person or a business entity from using the Internet to solicit, request, or take any action to induce a computer user to provide personal identification information by fraudulently representing that the person or business is an online business; prohibits a business entity or person who is not the authorized user of a computer from committing certain specified deceptive acts or practices that involve the computer; prohibits a person or business entity from collecting certain information without notice to and the consent of the authorized user of the computer. **Enforcement**: Public enforcement; private right of action under deceptive and unfair trade statute; authorizes a computer user to file a civil action for violations of the act. **Remedies**: Actual damages and attorney fees; damages up to $5,000 per incident, or three times the amount of actual damages, whichever amount is greater.
Georgia	Enacted (5/10/05)	S.B. 127; Act 389 "Georgia Computer Security Act of 2005" Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information; (3) take control of the consumer's computer; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce installation of spyware. **Enforcement**: Public enforcement; private right of action for aggrieved consumers. **Remedies**: Criminal (felony: 1- 10 years; up to $3 million); civil—injunctive relief, damages (including statutory: $100 per violation, up to $1 million), and attorney fees and costs.

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Illinois	Passed House (2/8/05)	H.B. 380 "Spyware Prevention Initiative Act" Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information; (3) take control of the consumer's computer; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce installation of spyware. **Enforcement**: Public enforcement. **Remedies**: Criminal (Class B misdemeanor).
Indiana	Pending	H.B. 1714 Prohibits the unauthorized installation of a computer spyware program that monitors a computer's usage and: (1) transmits usage information to another computer; or (2) displays certain advertisements in response to the computer's usage. Permits the installation of spyware only if the computer owner consents after full disclosure of the spyware's purpose and there is a method of uninstalling the spyware. Authorizes a website owner, a trademark or copyright holder, or an authorized Internet advertiser harmed by spyware to bring a civil action against the person who unlawfully installed the spyware. **Enforcement**: Private right of action for adversely affected parties (including targeted websites); Attorney General to establish a complaint procedure. **Remedies**: Greater of actual damages or $10,000 per violation; judicial discretion to award treble damages if the violation is knowing or intentional; attorney's fees and costs.

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Iowa	Enacted (5/3/05)	H.F. 614 "Deceptive or Unauthorized Computer Software" Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information; (3) take control of the consumer's computer; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce installation of spyware. **Enforcement**: Authorizes private right of action by a provider of computer software, a website owner, or a trademark or copyright holder harmed by a prohibited use of spyware to bring a civil action. **Remedies**: Injunctive relief; greater of actual damages or $100,000 per violation.
Kansas	Pending	H.B. 2343 Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information; (3) take control of the consumer's computer; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce installation of spyware. **Enforcement**: Public. **Remedies**: Criminal (Class A misdemeanor).

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Maryland	Legislature adjourned (4/11/05)	S.B. 492, S.B. 801, H.B. 945, H.B. 780 "Unauthorized Computer Software Act" Prohibits specified persons under specified circumstances from causing computer software to be copied onto a consumer's computer that modifies specified Internet settings, collects specified personally identifying information, prevents an authorized user from blocking the installation of specified software, or prevents an authorized user from disabling specified software; prohibits specified persons from misleading authorized users as to the effect specified actions will have with respect to computer software. **Enforcement**: Private right of action for injured parties. **Remedies**: Greater of actual damages or $500 per violation; attorney's fees.
Massachusetts	Pending	S.B. 273 "An Act Prohibiting Spyware" Prohibits installation of software that monitors usage, sends information about usage to a remote computer or displays ads based on usage (with certain exemptions) when the software provider does not obtain clear consent to a license. **Enforcement**: Private right of action for website owners, trademark and copyright owners, and authorized advertisers on a website affected by spyware. **Remedies**: Injunctive relief; greater of actual damages or $10,000 per violation; treble damages for willful violation; attorney's fees and costs.
Massachusetts	Pending	S.B. 286 "Regulation of Unconsented Internet Advertising" Prohibits installing spyware or context-based triggering mechanisms to display advertisements that obscure a webpage absent express consent and uninstall directions. **Enforcement**: Unspecified. **Remedies**: Escalating fine ($500 for the first violation, $1,000 for a second violation, and $5,000 for a third and any subsequent violations).

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Massachusetts	Pending	H.B. 1444 "Consumer Protection Against Spyware Act" Prohibits transmitting and using, through intentionally deceptive means, computer software that changes certain settings, collects personally identifiable information, prevents a user's efforts to block installation, falsely claims that software will be disabled by the user's actions, removes or disables security software, or takes control of the computer. **Enforcement**: Public. **Remedies**: Fines.
Michigan	Passed Senate (3/9/05)	S.B. 151 "Spyware Control Act" Prohibits installation of software that sends protected information or displays advertisements unless the software meets specified notice (clear license terms, full-size exemplars of advertisements, and advertisement frequency) and consent requirements. **Enforcement**: Public (Attorney General); private right of action by an adversely affected authorized user, website owner or registrant, trademark or copyright owner, or authorized website advertiser; does not authorize class actions. **Remedies**: Injunctive relief; greater of actual damages or $10,000 per violation; treble damages for pattern of violation.
Michigan	Passed Senate (3/9/05)	S.B. 53, S.B. 54 Prohibits access to computers, computer systems, and computer networks for certain fraudulent purposes; prohibits intentional and unauthorized access, alteration, damage, and destruction of computers, computer systems, computer networks, computer software programs, and data; prohibits the sending of certain electronic messages. **Enforcement**: Public. **Remedies**: Criminal penalties (misdemeanor and felony); sentencing guidelines for the crime of installing spyware on another person's computer without consent (S.B. 53).

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Missouri	Pending	H.B. 902 "Consumer Protection Against Computer Spyware Act" Prohibits a person lacking authorization from intentionally modifying the settings of a computer belonging to a consumer, collecting personally identifiable information from the computer, preventing an authorized user's reasonable efforts to block the installation of or disable installed software, removing or disabling security software installed on the computer, or taking control of the consumer's computer by transmitted commercial electronic mail or a computer virus from the consumer's computer. **Enforcement**: Public (Attorney General). **Remedies**: Unspecified.
Nebraska	Pending	L.B. 316 "Consumer Protection Against Computer Spyware Act" Prohibits a person lacking authorization from intentionally modifying the settings of a computer belonging to a consumer, collecting personally identifiable information from the computer, preventing an authorized user's reasonable efforts to block the installation of or disable installed software, removing or disabling security software installed on the computer, or taking control of the consumer's computer by transmitted commercial electronic mail or a computer virus from the consumer's computer. Establishes a Task Force of Computer Technology and Privacy. **Enforcement**: Public. **Remedies**: Criminal (misdemeanor).

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
New Hampshire	Passed House (2/23/05)	H.B. 47 "Regulating Use of Spyware" Prohibits a person or entity, who is not an authorized user, from knowingly causing a computer program or spyware to be copied onto the computer of a consumer and using the program or spyware, through intentionally deceptive means, to: (1) take control of the consumer's computer; (2) modify specified settings; (3) collect personal information through keystroke logging; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce violation of the Act. **Enforcement**: Public; private right of action for aggrieved persons. **Remedies**: Criminal and civil (injunction, greater of actual damages or $1,000); up to treble damages for willful violation; attorney's fees and costs.
New York	Pending	A.B. 549 "Unlawful Use of Spyware and Malware"; see also A.B. 2682 Prohibits a person or entity, who is not an authorized user, from knowingly causing a computer program or spyware to be copied onto the computer of a consumer and using the program or spyware, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information through keystroke logging; (3) prevent an authorized user's reasonable efforts to block or disable spyware; (4) take control of the consumer's computer; or (5) induce violation of the Act. **Enforcement**: Public. **Remedies**: Criminal (Class A misdemeanor; Class E felony for repeat offenders within 5 years of prior conviction).
Oregon	Pending	H.B. 2302 Prohibits a person from installing or causing installation of spyware on a computer absent clear notice as specified in the statute and informed consent. **Enforcement**: Public (Attorney General). **Remedies**: As set forth in the state's unlawful trade practice statute.

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Pennsylvania	Pending	H.B. 574 Prohibits installation of adware or spyware without specified notice and consent. **Enforcement**: Public. **Remedies**: Criminal.
Rhode Island	Pending	H.B. 6211 "Software Fraud" Prohibits a person, who is not an authorized user, from knowingly causing a computer program or spyware to be copied onto the computer of a consumer and using the program or spyware, through intentionally deceptive means, to: (1) modify specified settings; (2) collect personal information through keystroke-logging; (3) prevent an authorized user's reasonable efforts to block or disable spyware; (4) take control of the consumer's computer; or (5) induce installation of spyware. **Enforcement**: Public (Attorney General); private right of action by aggrieved person. **Remedies**: Greater of actual damages or $1,000 per violation; treble damages for pattern of violations; attorney's fees and costs.
Tennessee	Pending	H.B. 1742, S.B. 2069 "Internet Spyware Control Act of 2005" Prohibits installation of spyware or adware (triggered by use of a trademark of another) without computer users' informed consent. **Enforcement**: Private right of action by website owner or registrant, trademark or copyright owner, or authorized website advertiser. **Remedies**: Injunction; greater of actual damages or $10,000 per violation; treble damages for willful violation; attorney's fees and costs.

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Texas	Passed House (4/26/05)	H.B. 1430, S.B. 958 "Consumer Protection Against Spyware Act Prohibits a person, who is not an authorized user, from knowingly causing a computer program, through intentionally deceptive means, to: (1) collect personal information; (2) modify specified settings; (3) take control of the consumer's computer; (4) prevent an authorized user's reasonable efforts to block or disable spyware; or (5) induce installation of spyware. **Enforcement**: Public (Attorney General); private right of action by a provider of computer software, owner of a webpage, or trademark owner who is adversely affected. **Remedies**: Injunction; greater of actual damages or $100,000 per violation; treble damages for pattern of violations; attorney's fees and costs.
Texas	Pending	S.B. 327 "Collection and Transmission of Certain Information by Computer" Prohibits installation of spyware without specified notice and informed consent. **Enforcement**: Public (Attorney General). **Remedies**: Injunction; $1,000 per violation; attorney's fees and costs.
Utah	Enacted (3/17/05)	H.B. 104 amends "Spyware Control Act" Prohibits display of popup advertisements in response to a mark without authorization and imposes liability upon an advertiser who receives actual notice from mark owners of the use of its mark to trigger advertisements and fails to take reasonable steps to stop violations. Exempts from liability those who request information about a user's state of residence prior to sending spyware or popup advertisements and the user indicates a residence outside Utah. **Enforcement**: Public (Attorney General); and private right of action by a mark owner who does business in Utah and is directly and adversely affected; no class actions. **Remedies**: Injunction, greater of actual damages or $500 per violation; treble damages for willful and knowing violation; attorney's fees and costs.

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Utah	Enacted (3/23/04) Enjoined by 3rd Judicial District Court (6/22/04)	H.B. 323 "Spyware Control Act" Prohibits installation of spyware or adware (triggered by use of a trademark of another) without computer user's informed consent. **Enforcement**: Private right of action by website owner or registrant, trademark or copyright owner, or authorized website advertiser. **Remedies**: Injunction; greater of actual damages or $10,000 per violation; treble damages for willful violation; attorney's fees and costs.
Virginia	Passed House (2/4/05)	H.B. 1729 amends "Computer Crimes Act" Prohibits any person who is not an owner or operator of a computer from transmitting computer software to such computer, with actual knowledge or with conscious avoidance of actual knowledge, and, through intentionally deceptive means, to use such software to: (1) modify specified settings; (2) collect personal information; (3) prevent an authorized user's reasonable efforts to block or disable spyware; (4) take control of the consumer's computer; or (5) induce installation of spyware. **Enforcement**: Public. **Remedies**: Criminal (Class 1 misdemeanor).
Virginia	Enacted (4/4/05)	H.B. 2215 amends Chapter 812 Expands definition of "computer trespass" to include unauthorized installation of software on the computer of another, disruption of another computer's ability to share or transfer information, and maliciously obtaining computer information without authority. **Enforcement**: Public. **Remedies**: Criminal (Class 1 misdemeanor).

Survey, State Spyware Legislation (cont.)		
State	**Status**	**Summary**
Washington	Enacted (5/17/05)	H.B. 1012 Prohibits any person who is not an owner or operator of a computer to transmit computer software to such computer, with actual knowledge or with conscious avoidance of actual knowledge, and, through intentionally deceptive means, to use such software to: (1) modify specified settings; (2) collect personal information; (3) prevent an authorized user's reasonable efforts to block or disable spyware; (4) take control of the consumer's computer; or (5) induce installation of spyware. **Enforcement**: Public (Attorney General); private right of action by a provider of computer software or owner of a website or trademark who is adversely affected. **Remedies**: Injunction; greater of actual damages or $100,000 per violation; attorney's fees and costs; liability cap of $2,000,000.
West Virginia	Pending	H.B. 3246 Augments West Virginia Computer Crime and Abuse Act to prohibit installation of spyware for fraudulent purposes and requires that persons or entities providing computer software which contains spyware to disclose certain information about the spyware. **Enforcement**: Public **Remedies**: Criminal (misdemeanor) - fine of not more than $500,000 or incarceration for not more than six months, or both.

FIRST DO NO HARM: THE PROBLEM OF SPYWARE

By Susan P. Crawford†

TABLE OF CONTENTS

I. INTRODUCTION

Online problems are popularly understood to be easily susceptible to offline legal categorizations and, thus, solutions.[1] "There is nothing new under the sun," we say to one another over and over again in the cyberlaw

---

† Assistant Professor, Cardozo School of Law. Thanks to Lorrie Cranor, David Johnson, David Post, Michael Steffen, Stewart Sterk, and participants in the University of Pittsburgh School of Law's "Where IP Meets IP: Technology and the Law" symposium convened by Michael Madison.

1. Jack Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998) (stating that no special problems are created by the Internet that have not been addressed by existing conflict of laws and jurisdiction concepts); Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119, 1121 (1998) (stating that the "Net is not a separate place, and Net users are not removed from our world").

arena. But spyware[2] appears to be an exception to this received world view. There is nothing quite like spyware in the "real" world. Unlike an infectious disease, some varieties of spyware can "phone home" enormous amounts of personal data. Unlike a fixed surveillance camera, some spyware can travel with you wherever you "go" online. And unlike a blackmail note, which is unambiguously bad, spyware is very difficult to define—there can be "good" and "bad" spyware applications that have the same essential characteristics. Spyware combines attributes of all three of these things. Like an infectious disease, it can be contracted without the user's knowledge and can have harmful, amplified effects inside the body of the user's computer. Like a surveillance camera, it can watch users across time without their knowledge. And like a blackmail note, some spyware installations may force users into involuntary relationships that feel oppressive.

Just as there is nothing quite like spyware in the "real" world, no existing offline legal or regulatory techniques are adequate to address this problem. We could legislatively require that users consent to particular installations of software that may watch (and report on) their activities; sue software providers under existing unfair trade practices or trespass laws;[3] or let the marketplace provide software applications that make it possible for users to protect themselves. This Article argues that only the last of these three sets of actions will have any real effect on spyware, and that software developers and major online companies have already responded to market demands for help by releasing useful spyware-combating products and services.

---

2. This Article focuses on the difficulty of defining "spyware." Spyware is generally understood as software that is installed on a user's computer (often without the user's knowledge) and monitors the activities of that computer, "phoning home" information about the user or the computer's activities, changing the user's web browsing settings (homepage, Internet connection settings), or prompting pop-up advertisements. Subsets of "spyware" include "adware" (software designed to generate advertising based on web use) and "malware" (software designed to do harm to a computer). State and federal legislators have defined "spyware" in various ways. For purposes of this Article, the term "spyware" is used to mean all of these things, except where otherwise specifically indicated. For a useful primer on the various meanings of "spyware," see CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT), GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM (Nov. 2003), http://www.cdt.org/privacy/031100spyware.pdf.

3. The Federal Trade Commission has taken this route successfully. *See infra* Part II.E.3.a. This Article is focused on the first and third of the three options that I describe, and it does not explore the various litigation routes that might be available to private litigants.

Proposed legislative cures now under discussion may be worse than the diseases they are designed to counteract. Several pending or enacted bills (1) assume that legislative design of software is appropriate and (2) embrace the notion that "notice" is an effective concept in the spyware context—two legislative directions that this Article explains are bound to have negative effects on lawful innovation.

I am not claiming that legislation in this area signals the end of the civilized world or will bring a halt to the progress of science. To the extent that draft bills focus on bad behaviors rather than software design and notice, their enactment will have little effect on innovation and may in fact be helpful. I am concerned, however, that the software design and notice elements of pending spyware legislation may be exploited in the future as part of the larger power struggle between people who want to constrain what software can do and people who want to write code.

Three great industries want to constrain the writing of software and the functioning of the Internet: law enforcement, the content industry, and telecommunications companies. Having early legislative design mandates for software focused on "spyware"—something most people agree is "bad," even if they cannot precisely define it—is useful for these industries.[4] Later design mandates aimed at making tappability easier for law enforcement or copyright policing easier for the content industry or taxation easier for telecom agencies will be able to take advantage of the spy-

---

4. For example, the content community draws specific links between peer-to-peer ("p2p") applications used to facilitate filesharing and spyware. *See The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer to Peer File Sharing Networks?: Hearing Before the S. Comm. on the Judiciary*, 108th Cong. (2003) (statement of Sen. Orrin Hatch). Senator Hatch's comments at the conclusion of the hearing have been summarized as follows:

> Sen. Orrin Hatch (R-UT), the Chairman of the Committee, also focused on copyright infringement on P2P networks, and suggested that if no other way can be found to protect copyrighted works from piracy, 'destroying computers' should be permitted. . . . [Sen. Hatch said that he was] also troubled that many P2P networks require their users to install so-called 'spyware' or 'adware'—programs that monitor, collect, and report information about the Internet 'browsing' habits of a particular user.

Senate Committee Holds Hearing on P2P Networks, TECH LAW JOURNAL, June 18, 2003, http://www.techlawjournal.com/home/newsbriefs/2003/06d.asp. Some very popular p2p applications, such as eDonkey, iMesh, Kazaa, and Morpheus, bundle optional installations or installations disclosed only in lengthy license agreements that are difficult to read. Benjamin Edelman, *Comparison of Unwanted Software Installed by P2P Programs*, Mar. 7, 2005, http://www.benedelman.org/spyware/p2p. It would be very helpful to the content community to be able to outlaw p2p networks by using laws facially addressed to spyware.

ware legislative example. We need to decide what threshold of pain suffered by code writers makes us jump up and down and say "don't legislate." This Article is designed to encourage legislators to pause and consider the larger power relationships implicated by these bills before launching into further fruitless legislative efforts to end "spyware."

Part II of this Article surveys the legislative landscape as of mid-2005. Prompted by concerns over pop-up ads that were launched by third parties when users visited particular sites, the Utah legislature passed a spyware bill in 2003 that has been widely imitated in other states. Although the initial Utah bill was successfully challenged as violative of the dormant Commerce Clause, as of May 8, 2005 at least twenty-seven states were considering or had passed spyware legislation—including Utah, which had taken another stab at a bill barring unauthorized pop-up advertising. Meanwhile, there has been a great deal of spyware-related legislative energy expended at the federal level. Two spyware bills overwhelmingly passed in the House in 2004, and combined versions of those bills are likely to be supported by both houses of Congress in 2005.

All of the state bills trigger substantial dormant Commerce Clause issues and are unlikely to be found to be constitutional.[5] More importantly, however, the legislative approaches taken at both the state and federal levels have three major problems. First, many of these bills are overly regulatory, setting forth detailed design mandates and notice requirements. Second, these legislative efforts are doomed to be unsuccessful in terms of producing a reduction in spyware—just as the CAN-SPAM Act of 2003 was unsuccessful in reducing the volume of spam.[6] Third, many legislators appear to view spyware as an assault on privacy interests, a view that does not illuminate the problem of spyware. In fact, people are upset by some forms of spyware because they create oppressive, unwanted relationships, not because they violate some preexisting idealized privacy interest. Existing law directed toward remediating oppressive relationships, including both prima facie tort claims and federal statutory schemes, may adequately address spyware.

---

5. Given the state laws' focus on software content, these laws may be unconstitutional under the First Amendment as well. *See* ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997) (invalidating a state law criminalizing Internet transmissions that falsely identify the sender and holding that a state may impose content-based restrictions only to promote a "compelling state interest" and only through use of "the least restrictive means to further the articulated interest"). These statutes may not be sufficiently narrowly tailored, may sweep protected speech within their scope, and are often vague in their use of terms. *See infra* Part II.D.1.

6. *See infra* Part II.D.2.

Part III provides concrete suggestions for addressing spyware. There is no one organization with sufficient knowledge to recognize and deal with "bad" spyware. Only a technical approach—and only a particular kind of technical approach at that—will work. Technical actors need to take an "immune system" approach to spyware, dividing their efforts and experimenting in the field the same way immunity networks do. If we think of the legal system as a medical expert operating on this difficult disease, our first priority must be to wait to allow these already-emerging immunity networks to take effect, and to "do no harm" in the interim. This is a time for patience, not for the knife.

Part IV asks: what is the legal role of these immunity networks? It may be time to recognize that individuals, and their unhappy relationships with spyware, will not always be the most important actors on the legal stage. We are part of a collective technical environment that has become too difficult for us to understand or deal with as people, and too difficult for any existing legal institutions to take on effectively. As a result, individuals may need to choose to cede some control over their machines to technical networks that will help in the constant fight against oppressive adware and malware. This is not a move towards enforced similarity, as in communism. Nor is this a move towards a voting, democratic approach to software, where software that is voted "bad" becomes illegal. Instead, we should recognize that there is already in the world a third way of governing that we need to embrace as we face difficult technical warfare: competing networks. Only by allowing these networks to "represent" and protect us will we survive the coming difficulties. Such networks will provide the benefits of connection as well as the technical protections on which the spyware debate focuses.

II. THE LEGISLATIVE LANDSCAPE

Because there is so much legislative activity on the spyware front, the most useful way to discuss U.S. spyware legislation is to tell the story of the initial Utah state statute and its constitutional problems, clump the rest of the pending (or enacted) state bills into three groups (bad acts bills, notice bills, and trademark bills), and spend some time on the implications of the federal bills that will likely pass before this Article is published. If nothing else, this discussion should signal that we have not settled on a central legislative metaphor for dealing with spyware. Is spyware a type of software that does things that would surprise a user (if the user knew what was happening)? Is spyware a type of software that is automatically installed on a "protected computer" without the user being given an oppor-

tunity to refuse? Is spyware a type of software that allows the unauthorized use of trademarks in search terms (or visits to particular websites) to prompt the display of unauthorized advertisements? Is spyware anything that tracks what a user does online, whether or not the technology collects personally identifiable information? Apparently it depends which legislator is talking.

A. The Initial Utah State Statute: The Spyware Control Act

Utah's 2004 Spyware Control Act[7] was a reaction to the success of WhenU's SaveNow program in presenting pop-up ads to computers browsing the web. The SaveNow program is downloaded by users in return for obtaining a piece of freeware—a popular, free piece of software.[8] The consumer is presented with a license agreement stating that SaveNow will generate "contextual" pop-up ads. After the user clicks "I agree," the SaveNow program is installed on the user's computer and causes a directory of search terms and URLs to be saved on the user's desktop. As the user browses, his/her use of search terms and web addresses causes the presentation of pop-up ads and coupons. Although ad impressions triggered by the software are reported back to central SaveNow servers, search terms and websites visited by the particular computer are not.

1-800 Contacts, a Utah company that was unhappy that competitors' ads were triggered by the SaveNow software to appear in windows over 1-800 Contacts' site, sued WhenU, the company behind SaveNow.[9] After 1-800 Contacts gained an early victory against WhenU in that lawsuit,[10]

---

7. H.B. 323, 2004 Gen. Sess. (codified at UTAH CODE ANN. § 13-39-101 et seq.).

8. Examples include MP3 players, screensavers, file sharing applications, online games, and shopping tools.

9. 1-800 Contacts sued WhenU in federal court in New York on the theory that WhenU's advertisements infringe 1-800 Contacts' trademark and copyrights and initially prevailed. 1-800 Contacts, Inc. v. WhenU.com, Inc., 309 F. Supp. 2d 467, 472 (S.D.N.Y. 2003) (granting preliminary injunction on trademark challenge but denying the copyright challenge). The Second Circuit reversed this decision in June 2005, ruling that WhenU does not "use" 1-800 Contact's trademarks within the meaning of the Lanham Act, 153 U.S.C. § 1127 (2000), when it (1) includes 1-800 Contact's website address in an unpublished directory of terms that trigger delivery of advertising or (2) causes branded pop-up ads to appear on a computer screen next to the 1-800 Contact's website window. 1-800 Contacts, Inc. v. WhenU.com, Inc., No. 04-0026(L), 2005 U.S. App. LEXIS 12711, at *5 (2d Cir. June 27, 2005).

10. *1-800 Contacts*, 309 F. Supp. at 467. The New York district court decision (now reversed) conflicted with two earlier decisions by federal district courts in Virginia and Michigan. *See* U-Haul Int'l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723 (E.D. Va. 2003) (holding that WhenU pop-up advertisements do not represent trademark infringement, unfair competition, trademark dilution, or copyright infringement); Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734 (E.D. Mich. 2003) (same). The

1-800-Contacts went the legislative route and urged the Utah legislature to pass a bill addressing SaveNow's tactics.[11] Although a large coalition of substantial online companies lobbied against the bill,[12] it was enacted into law in March 2004.[13] This Act barred any person from installing "spyware" on another person's computer or causing such installation.[14] Part of the bill appeared to be aimed directly at WhenU's business. The bill defined "Context Based Triggering Mechanisms" as "a software based trigger or program residing on a consumer's computer that displays an advertisement according to: (a) the current Internet website accessed by a user; or (b) the contents or characteristics of the current Internet website accessed by a user."[15] According to the bill, use of a Context Based Triggering Mechanism to display an advertisement "that partially or wholly covers or obscures paid advertising or other content on an Internet website in a way that interferes with a user's ability to view the Internet website" was

---

Gator Corporation, now owned by Claria Corp., has also been sued several times for similar actions. *See, e.g.*, *In re* Gator Corp., 259 F. Supp. 2d 1378, 1380-81 (J.P.M.L. 2003) (providing docket information for consolidated actions). *Washingtonpost. Newsweek Interactive Co., LLC. v. Gator Corp.* resulted in an injunction in favor of the website operators and eventually settled in 2003. No. 02-909-A, 2002 U.S. Dist. LEXIS 20879 (E.D. Va. July 16, 2002). The terms of the settlement have not been made public. Todd Weiss, *Online newspapers settle lawsuit with Gator Ad service*, COMPUTERWORLD, Nov. 2, 2003, http://www.computerworld.com.au/index.php/id;1502815315;relcomp;1.

11. *See Burns, Wyden Told to Focus Anti-Spyware Bill on Action, Not Technology*, 5 WASHINGTON INTERNET DAILY 57, Mar. 24, 2004 ("The Utah Bill resulted from WhenU triumphing in court over 1-800-Contacts, a Utah company that sued to stop WhenU ads from popping up over its web site.").

12. The Information Technology Association of America (ITAA), Google, Yahoo! Inc., Microsoft Corp., America Online, the Software & Information Industry Association, Oracle Corp., eBay, and Amazon.com formed an ad hoc coalition opposing the bill. *Utah Governor Mulls Spyware Bill, Industry opposes: Constitutional Issues Raised*, ECOMMERCE LAW DAILY, Mar. 12, 2004, http://subscript.bna.com/SAMPLES/ecd.nsf/0/4574a5cb36c6555985256e5500022a0b?OpenDocument.

13. The Spyware Control Act was passed by the Utah Legislature on March 3, 2004 after a twenty-six to zero vote in its favor. Utah State Legislature, H.B. 323 Fourth Substitute, http://www.le.state.ut.us/%7E2004/htmdoc/hbillhtm/HB0323S04.htm (last visited Aug. 19, 2005). The bill was signed into law by Governor Olene S. Walker on March 23, 2004. *Id.*

14. "Spyware" was defined as "software residing on a computer that monitors the computer's usage, sends information about the computer's usage to a remote computer or server, or displays or causes to be displayed an advertisement in response to the computer's usage." UTAH CODE ANN. § 13-40-102(4)(2), (b) (2004) (subsection indicators omitted).

15. *Id.* § 13-40-102(1).

illegal.[16] The bill provided for a private cause of action and set damages at $10,000 for each separate violation.[17]

Following a challenge by WhenU, a Utah state court on June 22, 2004 enjoined this Act from coming into force on dormant Commerce Clause grounds.[18] The court found that plaintiff had shown that compliance with the statute would be difficult and expensive, that the statute was vague, and that it created a risk of different penalties and mandates being applied to online companies from state to state.[19]

In early 2005, Utah introduced revisions to this Act that are driven by pop-up ad generation concerns.[20] The revised Act defines "spyware" as "software on the computer of a [Utah] user" that "collects information about an Internet website at the time the Internet website is being viewed in this state" and uses that information contemporaneously to display pop-up ads.[21] The key violation under the new Act is to display an ad in response to a particular trademark when that advertisement has been purchased by someone other than the mark owner.[22] Damages under the Act have been reduced from $10,000 per violation to $500 per each separate occurrence resulting in display of an unauthorized advertisement, plus a possibility of treble damages and attorneys' fees and costs.[23]

The revised Utah bill attempts to deal with the dormant Commerce Clause problem by applying its penalties only to spyware that is installed on the computer of a Utah resident that collects information "at the time [an] Internet website is being viewed in this state."[24] It provides a safe harbor for advertisers who "request[] information about the user's state of residence before sending the spyware or displaying a pop-up advertisement to the user" when the user says he/she does not live in Utah.[25]

---

16. *Id.* § 13-40-201.

17. *Id.* § 13-40-301(1), (2).

18. WhenU.com, Inc. v. State, No. 040907578 (3d Dist. Utah June 22, 2004), *available at* http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.

19. *Id.*

20. Spyware Control Act Revisions, H.B. 104, 2005 Leg., 56th Sess. (Utah 2005).

21. UTAH CODE ANN. § 13-40-102(8) (2005).

22. *Id.* § 13-40-201.

23. *Id.* §§ 13-40-301, 302.

24. It is not clear that this will be enough to solve the dormant Commerce Clause problem; after all, there is no requirement that the communication that is unlawful—here, the transmission of the software to Utah residents—take place entirely within Utah. *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169-170 (S.D.N.Y. 1997).

25. UTAH CODE ANN. §§ 13-40-201, 202 (2005).

B. Other State Bills

1. Bad Acts

Alabama, Arkansas, Arizona, California, Illinois, Maryland, Michigan, Nebraska, New York, Rhode Island, Virginia, and Washington are considering or have enacted "bad acts laundry list" bills.[26] The bills outlaw software that deceptively "takes control" of a computer by modifying home pages, changing bookmarks, changing modem or other Internet access settings, transmitting or relaying unauthorized e-mail messages, using the computer as part of a distributed denial of service attack, or "opening multiple, sequential, stand alone advertisements" in a browser that cannot be closed without turning off the computer or closing the browser. The collection of personally identifiable information through deceptive means is also illegal under these bills, which focus on the use of keystroke loggers as well as software that gathers information about the websites visited by a user. The bills make illegal the deceptive prevention of a user's efforts to block software installations, misrepresentations that software will be uninstalled or disabled by what the user does next, and deceptive actions to disable anti-spyware software. These bills prohibit misrepresentations that software is needed for security or privacy or in order to open, view, or play a particular type of content. And the state legislatures working on these "bad acts" bills intend to continue their work. For example, the preamble to the California act states bravely that "it is the intent of the Legislature to revise the provisions in this act as needed to fully protect consumers from additional unfair and deceptive practices and to address future innovations in computer technology and practices."[27]

2. Trademark Concerns

Alaska, Indiana, Massachusetts, New Hampshire, and Tennessee, like Utah, have focused on the use of software to trigger unauthorized adver-

---

26. S.B. 122, 2005 Leg. (Ala. 2005); S.B. 2904, 2005 Leg., Reg. Sess. (Ark. 2005); H.B. 2414, 47th Leg., 1st Reg. Sess. (Ariz. 2005); CAL. BUS. & PROF. CODE § 22947 (Deering 2005) (imposing a $1000 penalty per violation); H.B. 380, 94th Gen. Ass. (Ill. 2005); H.B. 945, 2005 Leg., Reg. Sess. (Md. 2005); S.B. 151, 2005 Leg. (Mich. 2005); L.B. 316, 99th Leg., 1st Sess. (Neb. 2005); A.B. 549, 2005-2006 Reg. Sess. (N.Y. 2005); H. 6211, Gen. Ass., Jan. Sess. (R.I. 2005); H.B. 2215, 2005 Leg., Gen. Ass. (Va. 2005); H.B. 1012, 59th Leg., 2005 Reg. Sess. (Wash. 2005). For updated status of state spyware bills, see National Conference of State Legislatures, 2005 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware05.htm (last visited Aug. 19, 2005).

27. CAL. BUS. & PROF. CODE § 22947.

tisements.[28] To avoid a "spyware" categorization under these bills, software that triggers the display of ads must clearly identify the name of the entity responsible for delivering the advertisement in the body of the ad itself and the ad must not be triggered by an unauthorized trademark use. "Spyware" is defined to exclude "software or data that reports to an Internet web site only information previously stored by the Internet web site on the user's computer."[29]

These bills also require user consent for "spyware" to be installed legally. Consent will require user agreement to a full, detailed, plain language license agreement that, among other things, instructs the user how to distinguish the "spyware" advertisements from other advertisements.[30] Trademark owners and website operators have a private right of action under these bills, and can seek damages of $10,000 for each violation plus treble damages and attorneys fees.[31]

3. Notice Concerns

Michigan, Pennsylvania, Oregon, Tennessee, and Texas have enacted or are considering notice bills, under which "spyware," broadly defined,[32]

---

28. S.B. 140, 24th Leg. (Alaska 2005); H.B. 1714, 2005 Reg. Sess. (Ind. 2005) (section 2 provides that "'context based triggering mechanism' means a program or software based trigger that: (1) resides on a consumer's computer; and (2) displays an advertisement according to (A) the current Internet web site accessed by a user; or (B) the contents or characteristics of the current Internet web site accessed by a user"); S.B. 273, 184th Gen. Ct. (Mass. 2005) (defining spyware as follows: "software residing on a computer that monitors the computer's usage and either sends information about the computer's usage to a remote computer or server or causes to be displayed an advertisement in response to the computer's usage, or both"); H.B. 47 (N.H. 2005); H.B. 1742, 104th Gen. Ass. (Tenn. 2005).

29. H.B. 1714, § 2.

30. *Id.*

31. *Id.*

32. A draft Michigan spyware bill states: "Spyware" means computer instructions or software installed into a computer program, computer, computer system, or computer network for any of the following purposes:

> (a) monitoring the use of a computer program, computer, computer system, or computer network.
>
> (b) sending information about the use of a computer program, computer, computer system, or computer network to a remote computer or server or data collection site or point.
>
> (c) displaying an advertisement or causing an advertisement to be displayed in response to the use of a computer program, computer, computer system, or computer network.

S.B. 1315 (Mich. 2004) § 5a(5). The Pennsylvanian counterpart defines spyware as follows:

is illegal unless a consumer has a great deal of information supplied to him or her about the software: name and contact information of the person installing it (or on whose behalf it is being installed), notice of intent to install the software and a description of how it will affect its target, a full license agreement, and a method for refusing the installation and avoiding any further contact. Oregon provides that such notices "shall be in at least 10-point boldfaced type, in immediate proximity to the space reserved for the owner to agree to the installation."[33]

C. Overarching Commerce Clause Issues with Pending State Bills

All of the state bills pose substantial dormant Commerce Clause problems. Even where the bills provide a state nexus (such as, in the Utah bill, the scope limitation to Utah residents' computers and operating when those residents are in fact in Utah), the impact of these bills will not be limited to conduct occurring within the relevant state. "[P]urely intrastate communications over the Internet" do not exist.[34] Although these state bills and acts focus on spyware that has been installed on the computers of users inside the state, that installation requires a transmission that will

---

> An executable computer program that automatically and without the control of a computer user gathers and transmits to the provider of the program or to a third party either of the following types of information:
> (1) Personal information or data of a user.
> (2) Data regarding computer usage, including, but not limited to, which Internet sites are, or have been, visited . . . .

H.B. 574 § 2 (Penn. 2005) (introduced Feb. 16, 2005); *see also* H.B. 2302, 73rd Leg. Ass., 2005 Reg. Sess. (Ore. 2005). It is worth noting that much of the Pennsylvania bill is taken up with rules about commercial e-mail, all of which should, presumably, have been preempted by CAN-SPAM. The Tennessee and Texas bills contain both "notice" and "trademark" elements. H.B. 1742, 104th Gen. Ass. (Tenn. 2005); S.B. 327, 79th Leg. (Tex. 2005).

33. H.B. 2302, 73rd Leg. Ass., 2005 Reg. Sess. (Ore. 2005) § 2(3).

34. *See Am. Libraries Ass'n*, 969 F. Supp. at 171 (striking down a New York statute that prohibited online dissemination of harmful materials to minors because it did not require that the communication take place entirely within New York state and there was no way to limit the reach of the statute to New York); People v. Foley, 692 N.Y.S.2d 248, 256 (N.Y. App. Div. 1999) (holding that a New York statute criminalizing the dissemination of indecent material to minors through the Internet in order to lure minors to engage in sexual activity passed dormant commerce clause analysis); People v. Lipsitz, 663 N.Y.S.2d 468, 475 (N.Y. Sup. Ct. 1997) (holding that the application of New York consumer protection laws to New York business pursuant to Internet solicitations was proper under the dormant Commerce Clause). The Supreme Court has decided that state regulatory schemes that permit in-state wineries to ship alcohol to consumers but restrict the ability of out-of-state wineries to do the same are unconstitutional under the 21st Amendment and the dormant Commerce Clause. Granholm v. Heald, 125 S. Ct. 1885 (2005).

have come—necessarily—from out of state. Thus, because these statutes may impose burdens on out-of-state communications that are not necessarily unlawful, their constitutionality is suspect.[35] Web publishers and software developers cannot effectively prevent the flow of information to any given state.[36] State regulations may burden interstate commerce "when a statute . . . has the practical effect of requiring out-of-state commerce to be conducted at the regulating state's direction,"[37] and these state statutes have precisely this effect. Moreover, and perhaps more importantly, imposing state regulations in this area will subject the Internet to inconsistent regulations, something that is likely to make a reviewing court uncomfortable.[38]

---

35. *See* Am. Booksellers Found. v. Dean, 342 F.3d 96, 104 (2d Cir. 2003) (holding a state statute concerning dissemination of material harmful to minors unconstitutional under the dormant Commerce Clause and First Amendment); ACLU v. Johnson, 194 F.3d 1149, 1160-63 (10th Cir. 1999) (same); PSINet v. Chapman, 167 F. Supp. 2d 878, 882, 891 (W.D. Va. 2001) (same); Cyberspace Commc'ns, Inc. v. Engler, 55 F. Supp. 2d 737, 739-40, 751-52 (E.D. Mich. 1999) (same), *aff'd*, 238 F.3d 420 (6th Cir. 2000); *cf.* People v. Hsu, 99 Cal. Rptr. 2d 184 (Cal. Ct. App. 2000) (finding a state statute criminalizing pedophile activity constitutional because it included an intent requirement and prohibiting transmission of harmful material to seduce minors would not burden any legitimate commerce).

36. It is a matter of scholarly dispute whether technology now exists that could enable websites to determine, in an accurate and cost-effective fashion, where their visitors are coming from. *Compare* Joel Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. (forthcoming 2005) ("Commercial pressures and the dynamic nature of the Internet have resulted in geolocation and the re-creation of geographic origin and destination."), *and* Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1401 (2001) (pointing to the efficacy of geolocation technologies), *with* Andrea M. Matwyshyn, *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy*, 98 NW. U. L. REV. 493, 520 (2004) ("Geolocation technologies, while demonstrating relatively high levels of accuracy for marketing purposes, are still imperfect, both for the Internet and other forms of Network Communications; they do not offer adequate levels of certainty for jurisdiction purposes to be mandated as the tool of choice for jurisdictional determinations. For example, the European Union believes that geolocation technologies are inadequate tools for the purpose of assessing value-added tax on e-commerce." (citations omitted)). I consider the best-regarded free geolocation service, NetGeo, out of date and increasingly inaccurate, while the services that are more accurate (Akamai Edgescape, Digital Envoy, and Quova Geopoint) cater to large enterprises and charge steep monthly subscription fees.

37. Brown & Williamson Tobacco Corp. v. Pataki, 320 F.3d 200, 208-09 (2d Cir. 2003) (citations omitted).

38. *See Am. Booksellers Found.*, 342 F.3d at 104 ("[A]t the same time that the internet's geographic reach increases Vermont's interest in regulating out-of-state conduct, it makes state regulation impracticable. We think it likely that the internet will soon be seen as falling within the class of subjects that are protected from State

D. Federal Bills

The 108th Congress was a time of great legislative activity on the subject of spyware, and the 109th is proving to be a similarly active period. Although no bills have passed in either the House or the Senate as of the time of the preparation of this Article, it is very likely that spyware legislation will pass later this year. Bills on the list, each of which is discussed below, include the SPY ACT, the I-SPY ACT, and the SPY-BLOCK Act.

1. SPY ACT

The House bill in the lead as of May 2005, H.R.29 (The Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)), which preempts state legislation on these issues, is both a "laundry list of bad acts" bill and a notice bill.[39] The SPY ACT, which passed in the House on May 23, 2005, contains a list of "bad acts" that is very similar to the lists set forth in the Alabama, Arkansas, Arizona, California, Illinois, Michigan, Ne-

---

regulation because they 'imperatively demand[ ] a single uniform rule.'") (quoting Cooley v. Bd. of Wardens, 53 U.S. 299, 319 (1851)). On the other hand, *Pike v. Bruce Church, Inc.*, requires that "[w]here the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits". 397 U.S. 137, 142 (1970). Some commentators have argued that the Pataki approach to dormant Commerce Clause issues is overreaching and insufficiently nuanced. *See generally* Jack L. Goldsmith and Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L. J. 785, 787 (2001) ("The dormant Commerce Clause, properly understood, leaves states with much more flexibility to regulate Internet transactions than is commonly thought."); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1212 (1998) (spillover effects of local regulations are "a commonplace consequence of the unilateral application of any particular law to transnational activity in our increasingly interconnected world"); Michael W. Loudenslager, *Allowing Another Policeman on the Information Superhighway: State Interests and Federalism on the Internet in the Face of the Dormant Commerce Clause*, 17 BYU J. PUB. L. 191 (2003) (stating that deference to state police powers requires narrower reading of dormant Commerce Clause).

39. A 2004 version of the The SPY ACT passed the House in October 2004 by a vote of 399-1. Andrew Noyes, *Spyware Bill OK'd by House Commerce Committee*, 6 WASHINGTON INTERNET DAILY 47, Mar. 10, 2005. Its sponsor, Representative Mary Bono of California, reintroduced the SPY ACT in January 2005. The Subcommittee on Commerce, Trade, and Consumer Protection reported out H.R. 29 on Feb. 16, 2005. On March 4, 2005, an amended version of the bill was proposed by the Commerce Committee, and on May 23, 2005, the bill passed in the House. GovTrack.us, 109th Congress: Securely Protect Yourself Against Cyber Trespass Act, http://www.govtrack.us/congress/bill.xpd?bill=h109-29 (last visited Aug. 29, 2005). Chairman Barton of Texas has vowed to get H.R. 29 to the President's desk during 2005. *See* Michael Grebb, *Revised Spyware Bill Moves Ahead*, WIRED NEWS, Mar. 10, 2005, http://www.wired.com/news/politics/0,1283,66848,00.html.

braska, New York, Rhode Island, Virginia, and Washington proposed (or passed) bills: unauthorized "taking control" of the computer, modifying settings of the computer without authorization, modem hijacking, using the computer as part of a network of computers to cause damage, delivering uncloseable advertisements, collecting personally identifiable information by keystroke logging, phishing, and rendering security software inoperable.[40]

The SPY ACT "notice" provisions are far more complicated than those found in most of the state level bills.[41] The Act begins by creating the term Information Collection Program (ICP). According to the Act, an ICP is computer software that collects personally identifiable information and sends it on to anyone else, or uses it to show an advertisement. The bill contains a list of specific information that is considered "personally identifiable."[42] Next, the Act goes on to include in the definition of an ICP computer software that collects information about webpages accessed by a computer[43] (whether or not personally identifiable) and uses it to show advertisements. This is potentially a very broad category of code. HTML code, Java script, noncommercial applications, and very localized search functions that show ads based on pages visited within a site or search terms employed within a particular application might all fall within this definition.[44]

To this broad category of software, the SPY ACT applies an opt-in notice and consent provision, making it illegal to transmit an ICP to or execute an ICP on a computer unless the ICP (1) provides notice (including

---

40. *See supra* note 26.

41. Florida has introduced S.B. 2162, 2005 Leg., Reg. Sess. (Fla. 2005), and Georgia has introduced S.B. 127, 2004-05 Reg. Sess. (Ga. 2005), both of which appear to be very closely modeled on the SPY ACT.

42. SPY ACT § 10 (including specific information, like name, physical address, e-mail address, phone number, SSN, tax ID number, passport number, driver's license number, credit card number, access code, password, and date of birth).

43. The SPY ACT potentially covers all devices that compute around the world. *See infra* note 50.

44. Section 3(b)(2) of the SPY ACT states that computer software that would otherwise be considered an ICP will not be if the only information collected has to do with pages within a particular site and the information is not made available to people other than (i) the provider of the website accessed or (ii) a party authorized to facilitate the display or functionality of webpages within the site accessed. The only permitted advertising delivered to or displayed on the computer using this information is advertising on pages within that particular site. It is not clear how the SPY ACT will deal with information feeds or new technologies (including communication clients of various kinds) whose outputs do not map clearly onto "websites" or "pages."

specific English-language disclosures) and (2) includes functions listed in the bill.

The notice provisions in the SPY ACT require that ICP notices be clearly distinguished from any other information visually presented at the same time on the computer, and that they contain particular required texts in English, for example, "This program will collect and transmit information about you. Do you accept?" or "This program will collect information about Webpages you access and will use that information to display advertising on your computer. Do you accept?"[45] The notice also must provide a description of the types of information to be collected and sent by the ICP, an explanation of the purpose for these actions, and identify the ICP by name. After the user has consented to execution of the ICP, if the program is used to collect or transmit materially different information, a second notice must be sent and a second consent must be obtained. The Federal Trade Commission (FTC) is commanded to issue regulations on these notice subjects.[46] The FTC is not, however, provided with additional funding for this drafting work.[47]

---

45. The required notices may not communicate effectively to the 10 percent of Americans who do not speak English. US CENSUS BUREAU, LANGUAGE USE AND ENGLISH-SPEAKING ABILITY: 2000, Oct. 2003, http://www.census.gov/prod/2003pubs/c2kbr-29.pdf. Moreover, because the SPY ACT potentially affects devices around the globe, *see infra* note 50, Chinese notices may be more appropriate.

46. The SPY ACT is under the jurisdiction of the House Commerce Committee, which has been fiercely fighting for control over Internet-related issues with the Committee on the Judiciary for several years. *See, e.g.*, *House Commerce and Judiciary Committees Vie for High Tech Leadership*, TECH LAW JOURNAL, June 15, 1999, http://www.techlawjournal.com/intelpro/19990616a.htm. The Commerce Committee has jurisdiction over the FTC, and thus is interested in making spyware a deception issue subject to FTC rulemaking. Rep. Barton of Texas, who chairs the House Commerce Committee, has made clear that spyware legislation is his top priority. Because Rep. Barton is also in charge of rewriting the Telecommunications Act, it would be politically unwise for large online companies to challenge his spyware agenda, as it may adversely effect their telecommunications interests as well. For an exploration of the implications of the turf war between the Judiciary and Commerce committees, see John M. deFigueiredo, *Committee Jurisdiction and Internet Intellectual Property Protection*, May 2002, http://itc.mit.edu/itel/docs/2002/defigueiredo_0502.pdf (describing jurisdictional turf wars between committees over continuing and new issues can have a profound impact on the behavior of legislators and the outcomes of policies).

47. The SPY ACT's anointing of the FTC as the drafter of spyware rules is reminiscent of the FTC's adventures in children's online privacy under the Children's Online Privacy Protection Act (COPPA) of 2000. I have noted that despite expending enormous energy drafting rules under that statute, the FTC has brought very few cases. There is evidence that some providers of legitimate interactive services for children went out of business rather than attempt to comply with the burdensome consent requirements of the rules. *See* Ben Charny, *The Cost of COPPA: Kids' Site Stops Talking*, ZDNET,

Under the SPY ACT, all ICPs must allow the program to be disabled easily by a user, and they must ensure that any triggered advertisement is accompanied by the name or logo of the ICP. "Embedded advertisements" (an undefined term) are excepted from the latter requirement. The FTC may make rules about these functions, but is not required to do so. The SPY ACT provides for fines of up to $3 million for "patterns or practices" that violate the "bad acts" provisions, and sunsets at the end of 2010.

2. I-SPY ACT of 2005

The House Judiciary Committee introduced its own bill, H.R. 744 or the Internet Spyware (I-SPY) Prevention Act of 2005, which passed in the House on May 23, 2005. The bill avoids the regulatory approach of the SPY ACT, instead focusing on penalties for actual harm to computers.[48] It imposes up to a two-year prison sentence on anyone who uses spyware to intentionally break into a computer and either alter the computer's security settings, or obtain personal information with the intent to defraud or injure a person or with the intent to damage a computer. Additionally, it imposes up to a five-year prison sentence on anyone who uses software to intentionally break into a computer and uses that software in furtherance of another federal crime.

3. SPY BLOCK Act

The Senate is considering S. 687, or the Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK Act), co-

---

Sept. 12, 2000, http://news.zdnet.com/2100-9595_22-523848.html?legacy=zdnn; Carrie Kirby, *Youth Privacy Net Law Takes Effect, Many Web Site Operators Worry They'll Lose Money on Children's Market*, SAN FRANCISCO CHRONICLE, Apr. 21, 2000, at B1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/04/21/BU102542.DTL; Electronic Privacy Information Center, *The Children's Online Privacy Protection Act*, http://www.epic.org/privacy/kids (last visited Aug. 19, 2005) (stating that critics have claimed that the methods outlined by the FTC for verification—sending/faxing printed forms, supplement of credit card numbers, calling toll-free numbers, and forwarding digital signatures through e-mail—are inadequate to protect personal information, as well as prohibitively costly and cumbersome. Consequently, children may manipulate information to access these websites, and that online businesses may eliminate children-focused sites).

48. I-SPY uses the same broad definition of protected computers found in the SPY ACT—any "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device . . . which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C.A. § 1030(e) (West 2005).

sponsored by Senator Burns of Montana and Senator Wyden of Oregon. This bill has "bad act" elements, but goes beyond the bad acts explored by state legislation to outlaw very general deceptive software acts: it is unlawful under the SPY BLOCK Act to cause the installation of software[49] on a computer[50] in a manner that conceals the fact of the installation of the software from the user, prevents the user from having an opportunity to grant or withhold consent to the installation, or is the result of inducing the user to consent to the installation by means of a misrepresentation; it is also unlawful to cause the installation of software that prevents uninstall efforts. Given the definitions of "software" and "computer" under the SPY BLOCK Act, it could potentially cover software associated with routing communications across the Internet.

The SPY BLOCK Act states that ads prompted by software are unlawful if they are displayed "without a label or other reasonable means of identifying to the user of the computer, each time such an advertisement is displayed, which software caused the advertisement's delivery."[51] The Act also contains some language that appears to be trying to make unlawful any software installation that would surprise an end user:

> (a) It is unlawful for a person . . . to— (1) cause the installation on that computer of software that includes a surreptitious information collection feature; . . .
>
> (c). . . the term "surreptitious information collection feature" means a feature of software that—
>
> (1) collects information about a user of a protected computer or the use of a protected computer by that user, and transmits such information to any other person or computer—
>
> (A) [automatically]
>
> (B) [invisibly] and
>
> (C) for purposes other than—(i) facilitating the proper technical functioning of a capability, function, or service that an authorized user of the computer has knowingly used, executed, or enabled . . .
>
> (2)…without prior notification that—(A) clearly and conspicuously discloses to an authorized user of the computer the type of information the software will collect and the types of ways the

49. Under the SPY BLOCK Act, "the term 'software' means any program designed to cause a computer to perform a desired function or functions." S. 687, 109th Cong. § 13(9) (2005).

50. As in the other federal pieces of legislation, "computer" is defined very broadly to include all computers around the world. *Id.* § 12(8).

51. *Id.* § 4(a).

> information may be used and distributed" has not been provided.[52]

The FTC is given authority to promulgate rules for notifications that software will have to provide in order to avoid being categorized as a "surreptitious information collection feature."[53] Preemption provided by the SPY BLOCK Act is narrower than in the other federal bills, and covers only state legislation or regulation that deals with software installed or used to collect information or present ads, or prescribes specific methods for providing notification before the installation of software on a computer.[54]

It is likely that the Senate will pass the SPY BLOCK Act with a criminal amendment. The differences among the SPY BLOCK, I-SPY, and SPY ACT bills will be worked out in conference committee meetings. These bills are marching towards passage with virtually no opposition, which is not surprising because it is difficult to lobby against a bill labeled as fixing the problem of "spyware."

E. Implications of Pending Legislation

1. Implication One: Design Mandates

To the extent these bills deal with deceptive "bad acts" that are widely viewed as harmful spying, they are likely duplicative of existing unfair trade practices laws and unlikely to pose problems for future innovation. The I-SPY ACT falls within this category, as do the "bad acts" bills (including the first section of the SPY ACT) that focus on software that deceptively "takes control" of a computer or uses keystroke loggers. Because the deceptive use of software is outlawed under these bills, not the software itself, they may have the salutary effect of pushing the FTC to bring cases against clearly bad actors. But bills that broaden the definition of "spyware" to include software that gathers information about the websites visited by a user, or software that somehow surprises a user (as in the pending SPY BLOCK Act), or software that triggers contextual ads or web content based on user activity or use of unauthorized search terms (as in the revised Utah bill and the other state "trademark" bills), and require "notice" to be given to consumers before such software can be legally used, constitute technical design mandates focused on the software itself rather than legislation about deceptive behavior.

---

52. *Id.* § 3.
53. *Id.* § 7(b).
54. *Id.* § 10.

For example, under the proposed SPY ACT, all "information collection programs" must provide "notice" and include required functions in order to be considered lawful.[55] Information collection programs are broadly defined to include software that "collects information regarding the Web pages accessed using the computer" and "uses such information to deliver advertising to, or display advertising on, the computer."[56] In order to avoid falling into the hole of "spyware" liability, software meeting these broad definitions must provide elaborate disclosures in English and obtain consent from users. Similarly, the SPY BLOCK Act makes illegal "surreptitious information collection features" that without notice to the user collect information and use it for purposes that might surprise the user, and outlaws software that causes ads to be displayed without labels of various kinds. All of the "trademark" state bills and "notice" bills require notices and labels for liability to be avoided. Broadly stated, because these pending bills require functions, labels, and notices to be applied to software, whether or not the software coder feels it is a good idea to have such notices in place or the advertiser wants a label plastered on its ad, they are design mandates.

In conversation, people will say clearly that they think "spyware" is bad. We can all agree that the kinds of bad acts addressed by these bills constitute behavior that should be punished. Deceptive hijacking of the browser function, deceptive phishing, and deceptive installation of software are all things we can be confident are wrong. These provisions will not slow the course of innovation. But defining "spyware" in terms of broad categories of functions plus absence of "notice" (and clickthrough "assent") is a step legislatures should not take lightly, for several reasons.

First, the definition could be over-inclusive. Many of these broadly defined functions are in fact things that users now and in the future may want to have happen invisibly. For example, Yahoo! is offering a deeply contextual search function—Y!Q—that users can place on their own websites.[57] When text is highlighted on that page, and the search function is triggered, the search results respond to the text in context on the page. What if Y!Q also included ad results in exchange for the free service? Would that be "spyware" under one of these bills? Would users then have to see only labeled ads, or respond to notices in order to get the search function at all?

---

55. SPY ACT, 108th Cong. § 3 (2004).

56. *Id.*

57. *See* Yahoo! Search Help: Y!Q Search, http://help.yahoo.com/help/us/ysearch-/yq/index.html (last visited Aug. 30, 2005).

Similarly, Google is now offering an updated version of the popular Google Toolbar that allows users to highlight text on any webpage and be sent directly to another site—even though the author of the webpage did not insert a link in the underlying text.[58] In effect, Google is adding its own links to pages, starting initially with U.S. addresses as the highlighted text that goes to Google-chosen maps. Google tracks and logs the information gathered through this process, including pages visited, searches chosen, form information filled-in, and the IP address of the visitor, and can link that information to whatever a Google registrant has done with his or her Gmail account. Google can then use this information to trigger highly-focused ads that are presented to the user in Gmail or other contextually relevant places.[59] Would a user be surprised by this functionality? Should the Google Toolbar-generated ads be accompanied by various labels that make it clear what software triggered these ads? What if the user's use of the Google Toolbar generated just a drop of data in an ocean of other Google-gathered information that triggered these ads?[60]

SideStep, which bills itself as "the traveler's search engine," accompanies users as they shop for travel services online. When a user is about to

---

58. Anita Hamilton, *Google Tricks*, TIME MAGAZINE, Mar. 7, 2005, http://www.time.com/time/archive/preview/0,10987,1032364,00.html.

59. In 2004, Google filed a declaratory judgment action against American Blind based on American Blind's threats of suit arising out of Google's keyword advertising practices. Google, Inc. v. Am. Blind & Wallpaper Factory, Inc., No. C03-5340, 2004 U.S. Dist. LEXIS 27601 (N.D. Cal. Apr. 8, 2004). In March 2005, the Northern District refused to grant Google's motion to dismiss American Blind's trademark infringement and dilution claims, stating that American Blind might be able to show actionable trademark "use" based on purchase of keywords by Google advertisers. Google, Inc. v. Am. Blind & Wallpaper Factory, Inc., No. C 03-05340 JF, 2005 U.S. Dist. LEXIS 6228 (March 30, 2005). Judge Brinkema of the Eastern District of Virginia recently issued a decision concerning Google's use of keywords to trigger advertisements. Geico v. Google, Inc., No. 1:04cv507 (E.D. Va. Aug. 8, 2005) (holding that while mere use of keywords to trigger advertisements does not constitute trademark infringement, advertisements that reference trademarks in their headings or text may infringement trademarks).

60. eBay also has a toolbar that knows where you are on the eBay network of sites (including PayPal) at all times, and where you are when you have left that network. The eBay toolbar also includes an "Account Guard" feature that warns users (using colors) when they are on potentially fraudulent—spoofed—eBay or PayPal sites, and when they are on non-eBay sites. Users can report sites that they believe to be spoof sites, and that information will be reviewed by eBay and made part of the toolbar functioning if the tip is found to be accurate. Regarding this issue, eBay's Frequently Asked Questions states that the eBay toolbar is not spyware. eBay Frequently Asked Questions, eBay Toolbar With Account Guard, http://pages.ebay.com/help/announcement/4.html (last visited Aug. 30, 2005).

purchase a plane ticket, a narrow SideStep box slides out from the side of the user's screen, letting the user know that better deals on the same trip are available from different companies.[61] Many more SideStep-like applications will emerge in the months and years to come, accompanying users to provide comparison shopping and trust/verification services. Some of these services may not provide notices of any kind, and may be installed invisibly when a user elects a particular network of relationships or chooses a particular provider of online access. These applications will help users understand and organize the overwhelming wealth of information available online. They will certainly be tracking what users see and what users' preferences are, and they will have extensive information about users' offline activities. Will we call these applications "spyware," and claim that they are unlawful if they do not communicate particular prescribed notices and labels? Many of these applications are or will be free, and users want to continue having access to helpful free software.[62]

Cookies, text files that are sent by a webserver to a user's browser, are generally not considered spyware because they can only be read by the site that sent them. Thus, cookies do not track user activity across their entire web experience. But many major websites allow network advertisers, like DoubleClick and AvenueA, to place cookies on users' browsers and collate the information gathered for purposes of targeted advertising. The more sites that are served by these network advertisers, the richer and more sophisticated their databases of user activities become. Are these so-called "third party cookies" spyware that should be unlawful without notices and labels? Are users (or computers) harmed by well-targeted ads?[63]

Second, requiring these broad categories of sometimes-helpful software to provide notices (and obtain traceable consent to these notices) and include required functions, such as uninstallation features and readily-available information links, will greatly constrain the freedom of software designers. I am not arguing that facially unlawful software that does nothing but perform intrusive bad acts (like spreading viruses, or installing

---

61. *See* SideStep: The Traveler's Search Engine, http://www.SideStep.com/html/about_SideStep/main.html (last visited Aug. 19, 2005).

62. *See* 2005 Spyware Study, May 12, 2005, http://www.networkadvertising.org/spyware-forum/2005_Consumer_Spyware_Survey_NAI_051205.pdf (reporting national survey of 2000 Internet users and showing most people download free software and do not want new anti-spyware laws to prevent them from being able to download such software).

63. Updating virus control requires "spyware," and parental controls (settings that a user can alter to block particular kinds of content from being accessed by members of a household) raise some of the same concerns. Both require "monitoring" of the use of a computer; both might surprise users; neither is malicious.

Trojan horses, or changing a PC's settings) should be legal. I am saying, however, that new software applications with both "spying" and "serving" elements may be developed. Right now, enhanced search toolbars and third-party cookies both spy and serve. It is unclear what will happen next in the world of legitimate software development—and requiring particular features and the provision and tracking of "notice" will inevitably constrain some developers from doing inventive things that users might like.[64]

Indeed, it may be that laws mandating particular forms of code (and the application of labels and notices to this code) are unconstitutional. We can *protect* code (from copyright and patent infringement and from circumvention),[65] and *prevent* code by law from being exported (if it uses an encryption algorithm that exceeds certain limits),[66] but only when the government is acting as a customer (or funder) can it *mandate* that code have particular attributes.[67] Otherwise, design mandates become government-facilitated upstream censorship—something that is inconsistent with free speech values.

Requiring the use of particular labels and notices is arguably a violation of the First Amendment right "to refrain from speaking at all."[68] As the Supreme Court put it in *Riley v. National Federation of the Blind of North Carolina*, "Mandating speech that a speaker would not otherwise make necessarily alters the content of the speech. We therefore consider

64. The use of voluntary privacy notices has had good effects on data practices in the U.S., because such statements give the FTC and its state counterparts ways to attack data practices that do not match the promises made in these privacy notices. Professor Pam Samuelson has suggested that, similarly, mandatory notices for digital rights management (DRM) might have good effects for consumers. Pam Samuelson, A Notice Requirement for DMCA Anti-Circumvention Rules, paper presented at Modest Proposals 2.0 Conference at Cardozo Law School (Feb. 24-25, 2005). But mandatory notices, either for DRM or for software that some legislatures would consider "spyware" would raise constitutional concerns as well as pose threats to innovation. *See supra* II.D.i.

65. Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205 (2005); Dennis S. Karjala, *Distinguishing Patent and Copyright Subject Matter*, 35 CONN. L. REV. 439 (2003).

66. Export controls on commercial encryption products are administered by the Bureau of Industry and Security of the U.S. Department of Commerce. 15 C.F.R. pts. 730-74 (2004).

67. *Compare* U.S. v. Am. Library Ass'n, 539 U.S. 194 (2003) (discussing Children's Internet Protection Act, requiring public libraries to use Internet filters as a condition of receiving federal funding, not violative of First Amendment), *with* Ashcroft v. ACLU, 124 S. Ct. 2783 (2004) (discussing the Child Online Protection Act and holding that imposing fines and prison terms for knowingly posting web content that is harmful to minors for "commercial purposes" is likely unconstitutional because it is not the least restrictive means available to protect children).

68. Wooley v. Maynard, 430 U.S. 705, 714 (1977).

[such legislation] as a content-based regulation of speech."[69] Although it is true that commercial speech receives less protection than noncommercial speech,[70] and that disclosures can be required to keep commercial speech from being deceptive,[71] it is not at all clear that software is commercial speech.

The Supreme Court provided three factors that identify commercial speech when existing in combination: (1) advertisement; (2) mentioning a specific product by name; and (3) economically-motivated speech.[72] Software transmitted to users and networks does not necessarily meet this standard. Source code has been held to be expressive and thus protected by the First Amendment.[73] Sweeping online "notice" and "consent" laws do not seem adequately tailored to address problems with data privacy when offline data practices are left untouched—under either the intermediate scrutiny applied to commercial speech or the strict scrutiny applied to pure speech.[74] And even if software is commercial speech, spyware is not necessarily misleading or part of an illegal activity—the threshold inquiry for regulation of commercial speech under *Central Hudson Gas & Electric Corp. v. Public Service Commission*.[75] As the Court has said, "Our recent decisions involving commercial speech have been grounded in the faith that the free flow of commercial information is valuable enough to justify imposing on would-be regulators the costs of distinguishing the truthful from the false, the helpful from the misleading, and the harmless from the harmful."[76]

---

69. 487 U.S. 781, 795 (1988); *see also* Eugene Volokh, *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).

70. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978).

71. Zauderer v. Office of Disciplinary Counsel, 471 U.S. 626, 651 (1985).

72. Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 66-67 (1983) (striking down ban on mailings of contraceptive ads).

73. Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000).

74. Boos v. Barry, 485 U.S. 312, 321 (1988) (applying the strict scrutiny standard, which requires the government to show a compelling interest in restricting the speech and that the restriction is necessary and narrowly tailored to achieve that end); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Commc'n, 447 U.S. 557, 564 (1980) (stating that under intermediate scrutiny, regulation must not be more extensive than necessary to serve that interest).

75. 447 U.S. at 564.

76. *Zauderer*, 471 U.S. at 646.

Third, users[77] may not actually want to know everything that their machines are doing. Since the demise of the command line, the graphical user interface has been piling abstractions on top of abstractions and hiding more and more functionality from the user.[78] HTML, after all, is itself an invisible function of computer software, telling the browser how to render particular code visible to the user. It is code transmitted to and executed within the user's browser without the user's permission or knowledge. JavaScript, similarly, is used by web designers to make HTML pages more dynamic. It is also sent to the client as text and executed in the browser without the user's permission or knowledge. Several of the pending bills (including the SPY ACT) suggest that computer software that collects information about webpages accessed by the computer, or that is executed or installed without the user's knowledge, is potentially spyware that requires notice and consent. How much of this approval process do users want to be involved in? Would users like to know every time something "happens" inside their computer, and give approval to it?[79] Probably not. Users who set their browsers to "not accept cookies without permission" end up having terrible usage experiences, because they have to click to agree over and over again in order to sustain a single session on a single website.

Fourth, insisting on "notice and consent" for broadly-defined "spyware" will lead to a hopelessly impoverished and meaningless regime. No one will understand what a "yes" click means, and most people will simply click through as much as possible in order to be allowed to continue the session. If a "yes" is answered to the question "do you consent to the collection of information about your web browsing session," then that "yes" does not signal that the user understands how that collected informa-

---

77. Although policy discussions surrounding the spyware bills concern "users" and "consumers," the bills deal with electronic devices generally (worldwide) and "authorized users" of those devices. These "authorized users" could be systems administrators or network operators.

78. *See generally* M. MITCHELL WALDROP, THE DREAM MACHINE: J.C.R. LICKLIDER AND THE REVOLUTION THAT MADE COMPUTING PERSONAL (2001).

79. Perhaps for this reason, a recent revision of the SPY ACT exempts particular kinds of "computer software" from the notice provisions of the bill. If the software is (a) only collecting information about what pages have been accessed inside a particular website, (b) does not send information to someone other than the website operator, and (c) does not prompt advertising other than ads on the webpages within that particular website, it will not be considered an ICP. E-mail from David Cavicke, General Counsel and Chief Counsel for Commerce Trade and Consumer Protection, House Committee on Energy and Commerce (Mar. 11, 2005, 17:46:26) (on file with the author). This language is designed to exempt "HTML and Java when either performs ordinary functions like constructing Web pages," according to House staff. *Id.*

tion may be used from that moment to the end of time. It would be impossible to explain the consequences of a single "yes" without writing a novel and sending it for approval to the user. To the extent these "yes" clicks represent assent to a contract of adhesion, that contract will rise and fall based on its reasonableness, not on the presence or absence of a user's click.[80] In effect, the government will be requiring users to click helplessly along, assenting to something they do not understand over and over again.[81] This is more like forced speech ("CLICK! CLICK!") than consumer protection. Labeling generated ads to signal what software generated them is also a largely meaningless pursuit. Why will this information make any difference to the consumer? Wouldn't the consumer be happier managing his/her own user experience by using tools that block pop-ups, rather than gathering over and over again the empty knowledge of the ad's origin?

In sum, these design mandate elements of the pending legislative efforts should be understood for what they really are: reflections of an overall desire to control the online world. Although this set of issues is coming up in a context that many find "easy"—as there are few lobbyists for spyware—enacting these technical mandates should not be easy steps for legislators to take. There is in the world today an enormous push for control over the Internet generally[82] that uses fear of online threats to fuel its progress. In the copyright wars, we see a drive for technical mandates constraining devices (the broadcast flag) and requiring notices and redesigns of general purpose software that might be used for copyright infringement.[83] Staff to senators have said that software should be subject to a regime similar to products liability law, and be redesigned to avoid the risk of infringement and labeled to warn users of the potential for such risks.[84]

---

80. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (holding that a software licensor can bind purchasers by: (1) providing notice of a license to a consumer at the moment of licensing, and (2) providing the license terms and conditions following the moment of license); M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1 (1972); Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 595 (1991).

81. And if software manufacturers are providing notice and collecting consent, how will they know who consented to what without collecting and maintaining a great deal of personally-identifiable information? The privacy implications of these bills have not been explored—at least not publicly.

82. *See* Susan P. Crawford, *The Biology of the Broadcast Flag*, 25 HASTINGS COMM. & ENT. L.J. 603 (2003); Susan P. Crawford, *Shortness of Vision: Regulatory Ambition in the Digital Age*, FORDHAM L. REV. (forthcoming 2005).

83. *See* MGM Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2780-81 (2005).

84. Tom Sydnor, S. Comm. on the Judiciary staff member for Sen. Orrin Hatch, Public Statement at The Modest Proposals 2.0 Conference at Cardozo Law School (Feb. 25, 2005).

Similarly, the FBI would like to subject new online applications to pre-approval regimes, to ensure that they are easily tappable by law enforcement (and redesigned if they are not).[85] And the telecommunications industry would like to see broad application of "consumer privacy" mandates to IP-enabled services,[86] including required notices, labels, and all the rest. Notices, labels, and design mandates for software designated as "spyware" fit into this larger desire by incumbents for control over the high-tech industry, and represent a first crucial step down this path.

This may sound like an overstatement. "Why, no," you say to yourself. "There are no black helicopters here. All we're trying to do is lessen the scourge of spyware. Surely you can't suggest that great incumbent industries—law enforcement, content, and telecommunications—are behind this legislative effort so as to gain further control over software development."

I agree that consumer protection is a key goal for lawmaking, and I am confident that most legislators are being pushed by their relatives to do something about spyware. But this spyware battle presents an opportunity for specific design power to be asserted over code in a way we have not yet seen.[87] I would not be concerned if the legislation under consideration dealt only with "bad acts" that most people agree constitute spying. Taking this step seems wholly appropriate, and not worth an alarmist response. The insertion of notice and labeling mandates, by contrast, raises red flags and signals a shift in our understanding of what code is.

If code needs notice and labeling, it must be something that otherwise could be subject to product liability claims for failure to warn.[88] But because direct physical injury is not caused by software, it should not be

85. Joint Reply Comments of Industry and Public Interest, *In re* Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295 (FCC Dec. 21, 2004).

86. In re IP-Enabled Servs., 19 F.C.C.R. 4863 (proposed Feb. 12, 2004).

87. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and The Constitution*, 143 U. PA. L. REV. 709, 718-34 (1995) (describing uses of encryption technology to protect communications and provide data security).

88. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (1998) breaks down the definition into three distinct areas: (1) Manufacturing Defects—when the product departs from its intended design, even if all possible care was exercised; (2) Design Defects—when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design, and failure to use the alternative design renders the product not reasonably safe; and (3) Inadequate Instructions or Warnings Defects—when the foreseeable risks of harm posed by the product could have been reduced or avoided by reasonable instructions or warnings, and their omission renders the product not reasonably safe. The design defects approach seems to have been adopted with respect to code, at least in dicta, by Judge Posner in the *Aimster* decision. In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).

treated under a products liability regime—which traditionally focuses on tangible rather than intangible products. When we think of "products" whose manufacturers should be liable for "failure to warn," we think of chairs, or power tools, and so does the Restatement (Second) of Torts.[89] Software is much more like speech than it is a product.[90] It is not clear that rendering code subject to "failure to warn" standards would improve the quality of software.[91] And it would undoubtedly constrain what new code is allowed to do, limit user experiences, and lead to a flurry of inexplicable notices and labels[92] that might drive people away from the online world.

Because legislation is primarily a one-way ratchet,[93] should "spyware" notice and labeling bills pass legislatures will be in the business of demanding more and different notices and labels: "This software may permit copies to be made. WARNING." or "This software allows you to meet

89. RESTATEMENT (SECOND) OF TORTS § 402A (1979) (providing the framework for products liability law); *see also* Winter v. G.P. Putnam's Sons, 938 F.2d 1033, 1034 (9th Cir. 1991) ("The purposes served by products liability law . . . are focused on the tangible world . . . .").

90. The Magnuson-Moss Warranty—Federal Trade Commission Improvements Act, 15 U.S.C. §§ 2301-2312 (2000), which establishes minimum standards for consumer product warranties, may apply to software sold to consumers. I attended an FTC workshop in October 2000 at which the applicability of Magnuson-Moss to software was discussed, and there was no answer as to whether it did or did not.

91. *See* Jeffrey Neuberger & Maureen Garde, *Information Security Vulnerabilities: Should We Litigate or Mitigate?*, 21 Andrews Computer & Internet Litig. Rep. 13 (Mar. 2004) ("On the face of events, it appears that limiting liability for software defects may have been part of the solution to the Y2K problem. . . . Perhaps the economic resources that would have been devoted to litigating Y2K issues went instead to mitigating Y2K problems.").

92. Compare the experience of consumers with required financial privacy notices under Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2000). That Act requires that financial institutions provide certain disclosures regarding their privacy policies and provide opt-out opportunities before releasing information about individuals to third parties. Most experts agree that these notices are viewed by consumers as meaningless, and there is no evidence that the existence of these notices has led to increased privacy. And at least one "readability consultant" has concluded that consumers are unable to read and understand these notices. Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, PRIVACY RIGHTS CLEARINGHOUSE, July 2001, http://www.privacyrights.org/ar/GLB-Reading.htm.

93. For example, in the Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272, Congress made substantial changes to the 1978 Foreign Intelligence Surveillance Act (FISA), Pub. L. No. 95-511, 92 Stat. 1783. Although there is a sunset provision for these FISA changes in § 224 of the Patriot Act scheduled for December 31, 2005, it is very unlikely that we will return to pre-9/11 standards for foreign intelligence surveillance.

strangers and converse with them. Do you REALLY WANT TO DO THIS?"

2. Implication Two: Lack of Efficacy

Even with all the elements of the previously discussed approaches addressing spyware—notices, design mandates, and bad acts—written into legislative language, will federal spyware legislation work? The clear answer is "no." Although legitimate software distributors who routinely comply with law will provide notices and constrain their design efforts, rogue spyware sources will simply move offshore and continue their deceptive work, or stay in the U.S. and design around the rules. This has been our experience to date with the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)[94] legislation of mid-December 2003.[95]

The most important element of CAN-SPAM, like the pending federal spyware bills, is that it preempts state anti-spam measures that are not directly related to fraud or deception.[96] Several states (most notably, California, with an "opt-in" bill that was scheduled to take effect on January 1, 2004) had enacted statutes that were extremely restrictive, and CAN-SPAM was designed to avoid the complexities of complying with fifty different state laws.

CAN-SPAM does not outlaw the sending of unsolicited commercial e-mail. Instead, it prohibits some fraudulent and misleading practices (such as misleading header information), requires senders to label their messages as commercial, and requires that senders give recipients a means to opt out of communications.[97] The labeling scheme of CAN-SPAM requires that senders provide in each message a "clear and conspicuous identification that the message is an advertisement or solicitation."[98] The Act is enforced by the FTC,[99] criminal prosecutions (with penalties ranging up to five

94. Pub. L. No. 108-187, 117 Stat. 2699.

95. *See* Press Release, The White House, Fact Sheet: President Bush Signs Anti-Spam Law (Dec. 16, 2003), http://www.whitehouse.gov/news/releases/2003/12/20031216-4.html; Tom Zeller, *Law Barring Junk E-Mail Allows a Flood Instead*, N.Y. TIMES, Feb. 1, 2005, at A2.

96. *See* 15 U.S.C. § 7708(b) (Supp. 2004).

97. CAN-SPAM Act, § 5(a)(3).

98. *Id.* § 5(a)(5)(A)(i).

99. *Id.* § 7(a).

years in prison),[100] actions by state attorneys general,[101] and suits by ISPs.[102]

Unsolicited e-mail on the Internet has actually increased since the passage of CAN-SPAM, and now amounts to 80 percent or more of all e-mail sent, up from 60 percent during the period before the law went into effect.[103] It appears that the greatest impact of CAN-SPAM has been to cause legitimate businesses heartaches as they try to avoid falling into some of the ambiguous traps that statute creates. Spammers, meanwhile, have changed their tactics since CAN-SPAM was enacted, and are now using "zombies networks" (computers hijacked with trojan horse programs, according to PC World) to send spam.[104] Nearly half of the world's spam is said to come from the U.S.[105] CAN-SPAM has neither made it easier to find spammers nor decreased the amount of spam.

Some may argue that CAN-SPAM was a toothless alternative to state opt-in bills, such as the California measure that CAN-SPAM was designed to preempt, and that federal spyware legislation could be made more effective than CAN-SPAM.[106] Spyware relationships leave a direct money trail that can be more easily followed than spam operations, making it potentially easier to police than spam. But both CAN-SPAM and the spyware bills attempt to do the same thing: control the flow of bits through law, in a world in which it is very difficult both to tell who is responsible for which bits and to locate these sources physically for enforcement purposes.

---

100. *See, e.g.*, Associated Press, *Spam senders convicted in first felony case*, Nov. 3, 2004, http://www.msnbc.msn.com/id/6401091 (noting that the court sentenced spammers to nine years in prison plus fines).

101. CAN-SPAM Act, § 7(f).

102. *Id.* § 7(g).

103. Zeller, *supra* note 95; Grant Gross, *Is CAN-SPAM Working? One year After it Went Into Effect, Many Say The Nation's Antispam Law is Ineffective*, PC WORLD, Dec. 28, 2004, http://www.pcworld.com/news/Article/0,aid,119058,00.asp (reporting Postini claim that legitimate nonspam e-mail was down to 12 percent in December 2004 and MX Logic claim that 25 percent of all e-mail was legitimate as of November 2004).

104. Gross, *supra* note 103.

105. Dan Ilet, *U.S. Leads the Dirty Dozen Spammers*, CNET NEWS.COM, Dec. 24, 2004, http://news.com.com/U.S.+leads+the+dirty+dozen+spammers/2100-7349_3-5503344.html.

106. Chris Hoofnagle of the Electronic Privacy Information Center made this point at a February 19, 2005 conference, "Real Law and Online Rights," sponsored by the Virginia Journal of Law and Technology at the University of Virginia. Hoofnagle has argued that the past decade of self-regulation has led to the spyware epidemic. Chris Jay Hoofnagle, *Privacy Self-Regulation: A Decade of Disappointment*, EPIC.ORG, Mar. 4, 2005, http://www.epic.org/reports/decadedisappoint.html.

Additionally, none of the spyware bills that are under consideration create any new funding for agency enforcement of their mandates. Real spyware—the truly harmful kind, not the broadly defined kind—comes from people who are completely dedicated to breaking the law. Without enforcement funding, and with the real difficulties involved in finding and prosecuting spyware sources, the spyware picture is unlikely to be changed by new federal laws. And international spyware sources will, of course, be completely unaffected.

3. Implication Three: A Complicated Relationship With Existing Laws

In response to the spyware epidemic, some have strongly suggested that spyware be addressed as a privacy issue.[107] In connection with pending federal spyware bills, and at the urging of legislators, public advocacy groups have testified in favor of "baseline" privacy legislation, whereby fair information practices[108] (including notice, consent, access, and security) would be required of all U.S. online participants.[109]

---

107. *See* Editorial, *The Spies in Your Computer*, N.Y. TIMES, February 18, 2004, at A1 (arguing that "Congress will miss the point [in spyware legislation] if it regulates specific varieties of spyware, only to watch the programs mutate into forms that evade a narrowly tailored law. A better solution, as proposed recently by the Center for Democracy and Technology, is to develop privacy standards that protect computer users from all programs that covertly collect information that rightfully belongs to the user").

108. An exhaustive discussion of the history and meaning of the phrase "fair information practices" is beyond the scope of this Article. *See generally* Secretary's Advisory Comm. on Automated Personal Data Systems, U.S. Dep't. of Health, Educ. & Welfare, *Records, Computers, and the Rights of Citizens* viii (1973) (stating five principles of fair information practices: no data record-keeping systems should be secret; access should be by subject; information obtained for one purpose should not be used for another purpose without consent; correction should be by subject; reliability and security of data is required); ORGANISATION FOR ECONOMIC CO-OPERATION AND DEV., RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, Sept. 23, 1980, O.E.C.D. Doc. C(80)58 Final, *reprinted in* 20 I.L.M. 422 (1981) (stating eight similar principles); Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (granting right of access to personal data, right to know where data originated, right for inaccurate data to be rectified, right of recourse in the event of unlawful processing, and right to withhold permission to use data in certain circumstances).

109. *See, e.g.*, *Combating Spyware: H.R. 29, the SPY ACT: Hearing Before the H. Comm. on Energy and Commerce*, 109th Cong. (2005) (testimony of Ari Schwartz, Associate Director, CDT), *available at* http://www.cdt.org/testimony/20050126 schwartz.pdf; *Spyware: Hearing Before the S. Subcomm. on Communications of the Comm. on Commerce, Science, and Transportation*, 108th Cong. (2004) (prepared

This approach looks at spyware from the wrong end of the telescope. Although the scope of any constitutional "right to privacy" is hotly disputed,[110] such rights are fundamentally grounded in notions of property.[111] People have a right to privacy in their houses and effects, because a man's home is his castle.[112] When the subject for "privacy" is data about interactions between a user and his/her computer, or interactions between a computer and online resources,[113] it is very difficult to define the "property"

---

statement of Jerry Berman, President, CDT), *available at* http://www.cdt.org/testimony/20040323berman.pdf ("Fundamental to the issue of spyware is the overarching concern about online Internet privacy. Legislation to address the collection and sharing of information on the Internet would resolve many of the privacy issues raised by spyware.").

110. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (stating that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant"); Village of Belle Terre v. Boraas, 416 U.S. 1, 13 (1974) (Marshall, J., dissenting) (holding that an ordinance restricting "single-family" houses to those in which "persons related by blood, adoption, or marriage" live infringes upon "fundamental" First Amendment rights of privacy and freedom of association); Katz v. United States, 389 U.S. 347, 351-52 (1967) (overruling *Olmstead* and stating that "the Fourth Amendment protects people not places. . . . [W]hat [an individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (identifying a right of privacy and describing it as "the right to be let alone" in response to majority opinion that held that the government's use of wiretap without a search warrant did not violate the Fourth Amendment because no physical intrusion into the home where the calls were made); Louis Brandeis & Samuel Warren, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890) (stating that the law should create a right to privacy protecting private facts).

111. Brandeis and Warren explored this right of property:

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. . . . Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. . . . Gradually, the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to compromise every form of possession—intangible, as well as tangible.

Brandeis & Warren, *supra* note 110, at 193.

112. *Id.*; *Kyllo*, 533 U.S. at 40; *Olmstead*, 277 U.S. at 478.

113. Although the preceding discussion should make clear that not all of the pending sypware bills are the same, or even similar, many of them go far beyond requiring

that is being impinged on and should be protected as "private,"[114] either through constitutional protection or common law tort claims. The key, defining characteristics of property are exclusive ownership and the ability to exclude (or invite) others. Do you "own" streams of data (created by your interactions by others) about your online transactions and experiences? Do you expect to be able to consent to, correct, and "remove" these streams of data that you "own"? Physically separable personal information is very different to conceptualize, much less protect.

More importantly, focusing on notions of inevitably property-based privacy misses the forest for the trees. The reason people are upset by spyware is that it creates oppressive, unwanted relationships through, for example, hijacking their browsers, or using their PC for an attack on others, or flashing unwanted pop-up ads. Users' instinctive worry is not that spyware violates some preexisting idealized control over particular pieces of data they "own" or could possibly define in advance in some clean, sterile way. As soon as a user goes online, he or she is thrust into an interactive data flow experience that is largely invisible to them. There is no castle; there are no walls; there is nothing to draw a line around and say "this is private." Users want many of these data flows to be invisible to them (or would want this if they suddenly had to control and authorize every data exchange). What is troublesome is bad interactions—oppressive, unreasonable relationships that bother the user.

Now that we have identified users' actual concerns about spyware, we discover that existing federal and state laws and court-created doctrines directed toward addressing oppressive relationships may already adequately address users' legal issues.

a) Federal Law

There are several federal laws addressing computer privacy. The federal Computer Fraud and Abuse Act (CFAA) already makes unauthorized

---

restraints on the use or collection of personally identifiable information to constraining the use or collection of use data generally. *E.g.*, SPY ACT, H.R. 29, 109th Cong. § 3(B)(1)(b) (2005) (covering "computer software that. . . (2)(A) collects information regarding the Web pages accessed using the computer; and (B) uses such information to deliver advertising to, or display advertising on, the computer").

114. *But see* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000) (stating that meaningful autonomy requires a degree of freedom from monitoring, scrutiny, and categorization by others); Daniel Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1091-92 (2002) (discussing need for ad hoc, contextual conceptions of privacy).

computer intrusions illegal.[115] The CFAA has proven to be a broad and flexible statute, under which anyone who obtains information from a computer or causes damage or obtains anything of value can be sued.[116] All spyware could potentially be reached by a claim under the CFAA, as long as the code caused (or would have caused) aggregated losses over a one-year period of at least $5,000.[117] Repeated, intentional spyware activity is likely to meet this threshold.[118]

The Electronic Communications Privacy Act (ECPA)[119] made it a crime and a statutory tort to intercept electronic communications, to disclose intercepted communications, or to use intercepted communications.[120] ECPA also made criminal (and tortious) any unauthorized access to "stored electronic communications."[121] To the extent that spyware is installed without user consent—which is often the case—ECPA may provide a cause of action against its source.

The FTC has already brought litigation against spyware sources under Section 5 of the Federal Trade Commission Act, which outlaws unfair or deceptive trade practices.[122] In October 2004, the FTC sought and obtained a federal court injunction against Seismic Entertainment Produc-

115. 18 U.S.C. § 1030 (2000). The central offense under the CFAA is the abuse of a computer to obtain information. Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1128-29 (W.D. Wash. 2000) (involving an employer who sued a competitor under the CFAA for hiring away employees to improperly gain information).

116. Civil causes of action under the CFAA are available against the violator for compensatory damages and injunctive relief. 18 U.S.C. § 1030(g) (2000); *see* Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003) (stating that employers "are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system").

117. 18 U.S.C. § 1030(g).

118. *See, e.g.*, Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268 (S.D. Fla. 2003) (holding that a hotel licensee violated the CFAA by intentionally attempting to access the licensor's protected computers without authorization, spoofing the licensor's computers, causing congestion on the licensor's VPN device, and obtaining information of value in the form of confidential customer and financial data).

119. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

120. 18 U.S.C. § 2510 (1994).

121. *Id.* §§ 2701-10.

122. These provisions prohibit unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45(a) (2000).

tions, Inc., Smartbot.net, Inc., and Sanford Wallace,[123] after alleging that these actors had installed software code onto users' computers without authorization that changed those users' home pages, downloaded and installed various other programs, caused an incessant stream of pop-up messages to be displayed, and triggered ads for defendants' "anti-spyware" programs. Defendants did not contest the agency's factual allegations, but argued that their actions were "accepted marketing practices used by reputable companies."[124] The FTC alleged that defendants' actions were "unfair."[125] The court agreed with this assessment and granted an injunction—adding that it thought defendants' actions were "deceptive" as well as "unfair."[126] Thus, the FTC been successful proceeding against "spyware" purveyors under its existing powers.

b) State law

Deceptive trade practices acts based on the Uniform Deceptive Trade Practices Act model have been adopted in many states.[127] California's unfair competition law imposes civil liability for "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising,"[128] and provides standing for citizens that can show harm by such unfair practices to bring claims even where the conduct alleged is a violation of a statute that does not provide for a private right of action.[129] These acts broadly prohibit unfair or deceptive conduct in commerce, and thus could be used by states in connection with spyware activities in just the same way that the FTC has used its authority.

---

123. FTC v. Seismic Entm't Prods., Inc., No. 04-337-JD, 2004 U.S. Dist. LEXIS 2278 (D.N.H. Oct. 21, 2004), *available at* http://www.cdt.org/privacy/spyware/spywiper/20041021seismicruling.pdf.

124. *Id.* at *11.

125. Under the FTC Act, an act or practice is unfair if it: (1) causes or is likely to cause substantial injury to consumers; (2) the injury to consumers is not outweighed by any countervailing benefits; and (3) the injury is not reasonably avoidable by consumers. *See* 15 U.S.C. § 45(n) (2000).

126. "The affected users were not notified of the defendants' activities and did not know what had caused the problems with their computers, making the defendants' activities both deceptive and unfair." *Seismic Entm't Prods., Inc.*, 2004 U.S. Dist. LEXIS at *9-*10.

127. For example, Colorado, Delaware, Georgia, Hawaii, Illinois, Maine, Minnesota, Nebraska, New Mexico, Ohio, Oklahoma, Oregon. *See* Legal Information Institute, Uniform Business and Financial Laws Locator, http://www.law.cornell.edu/uniform/vol7.html#dectr (last visited Aug. 29, 2005).

128. CAL. BUS. & PROF. CODE § 17200 (Deering 2005).

129. *See* CAL. BUS. & PROF. CODE §17204 (Deering 2005); Barquis v. Merchants Collection Ass'n of Oakland, Inc., 496 P.2d 817, 828 (Cal. 1972).

If deception is difficult to prove, there is an even broader state law approach to spyware that captures the essence of the spyware violation: prima facie tort. Although not widely used (and in fact often denigrated), this tort addresses unjustified actions that are intended to harm another—or, in other words, the creation of an oppressive relationship.[130] The prima facie tort requires (1) an injury to another and (2) culpable conduct on the part of the actor that is (3) unjustifiable under the circumstances.[131] All other specific intentional torts are instantiations of the general principle stated in the prima facie tort.[132] In the absence of a mature, specific, clearly-delineated "spyware" intentional tort (or even an intentional tort that clearly applies to spyware), the prima facie tort will provide courts with a role in redressing oppressive relationships created by code.[133] Involving courts in creating a common law of spyware—deciding which oppressive relationships are harmful enough to merit judicial censure—will allow for a much more nuanced approach to spyware than is possible through legislation.

As outlined in the previous two subsections, both federal and state legal frameworks already exist that address the concerns that are driving the current push for spyware legislation. Litigation based on these existing

---

130. *See* RESTATEMENT (SECOND) OF TORTS § 870 (1979) ("One who intentionally causes injury to another is subject to liability to the other for that injury, if his conduct is generally culpable and not justifiable under the circumstances. This liability may be imposed although the actor's conduct does not come within a traditional category of tort liability."). Prima facie tort is recognized in Missouri, New Mexico, and New York. *See* Bandag of Springfield, Inc. v. Bandag, Inc., 662 S.W.2d 546, 553 (Mo. Ct. App. 1983); Schmitz v. Smentowski, 785 P.2d 726, 739 (N.M. 1990); Beavers v. Johnson Controls World Servs., Inc, 901 P.2d 761 (N.M. Ct. App. 1995); Curiano v. Suozzi, 469 N.E.2d 1324, 1327 (N.Y. 1984); Bd. of Educ. v. Farmingdale Classroom Teachers Ass'n, 343 N.E.2d 278 (N.Y. 1975).

131. ATI, Inc. v. Ruder & Finn, Inc., 368 N.E.2d 1230, 1232 (N.Y. 1977).

132. As for conduct intentionally causing harm, however, it has traditionally been assumed that the several established intentional torts developed separately and independently and not in accordance with any unifying principle. This Section purports to supply that unifying principle and to explain the basis for the development of the more recently created intentional torts. More than that, it is intended to serve as a guide for determining when liability should be imposed for harm that was intentionally inflicted, even though the conduct does not come within the requirements of one of the well established and named intentional torts.

RESTATEMENT (SECOND) OF TORTS § 870 cmt. a.

133. *See* Porter v. Crawford & Co., 611 S.W.2d 265, 269 (Mo. Ct. App. 1980) (noting that Justice Holmes introduced the prima facie tort doctrine in this country).

laws may be a better solution to spyware than legislation—particularly "notice" and "labeling" legislation.

But even litigation's effect on spyware will be greatly constrained by interdependencies, jurisdictional tangles, and technical realities that are beyond the scope of any court. Spyware purveyors are certainly not necessarily based in the U.S., and spyware often reaches consumers through highly complex chains of affiliates whose relationships are very difficult to parse.[134] Without an attorney's-fee recovery mechanism, many lawyers are unwilling to take on the expense of litigating against spyware sources, and prosecutors often lack the resources to investigate technical spyware cases.

III. THE TECHNICAL LANDSCAPE

Given that both legislation and litigation are unlikely to be up to the task of definitively solving the spyware problem, what should we do? There is no one legal institution with sufficient knowledge to recognize and fix the infinite varieties and functionalities of "bad" spyware in advance. Legal minds simply cannot design a sufficient attack on spyware. This Part suggests that legal systems can instead encourage deference to the development of technical immune networks, and points to areas for possible future work.

The informational properties of the immune system are remarkable. Although the networks that make up the human immune system are distributed throughout the body, the system is able to distinguish between "self" and "nonself" quickly and retain this information in "memory." It can thus tell the difference between harmful microbes (foreign materials or "antigens") and the body. Special types of white blood cells (lymphocytes) recognize foreign material by forming molecular bonds between these foreign materials and receptors on the surface of the lymphocyte. In effect, immune system detectors bind to particular (foreign) short chains of amino acids—thus recognizing the pattern encoded by these short chains.[135] These detectors are highly specific, so each recognizes only a limited

134. *Combating Spyware: H.R. 29, the SPY ACT: Hearing Before the H. Comm. on Energy and Commerce*, 109th Cong. (2005) (testimony of Ari Schwartz, Associate Director, CDT), *available at* http://www.cdt.org/testimony/20050126schwartz.pdf (noting that spyware download process is "sustained through a nearly impenetrable web of affiliate relationships that is used to deflect accountability and frustrate law enforcement").

135. Stephanie Forrest & Steven Hofmeyr, *Immunology as Information Processing*, *in* DESIGN PRINCIPLES FOR IMMUNE SYSTEM & OTHER DISTRIBUTED AUTONOMOUS SYSTEMS (L.A. Segal & I.R. Cohen eds. 2000).

number of foreign chains.[136] Some lymphocytes (those that mature in the thymus gland) actually attack and destroy cells that are recognized as foreign; others mark the foreign cells for destruction. This distributed system is error-tolerant, dynamic, self-protecting, and adaptable.[137] Lymphocytes that bind too strongly with "self" cells are selected out, so that the remaining cells will be able to recognize abnormal peptides. Once lymphocytes have encountered and destroyed a particular organism, they carry out resistance to that organism for some time—they remember their enemies. They also "learn" new foreign materials through the development of new receptors. Through a complex interaction among decentralized molecules, cells, and organs, acting independently but communicating, the system is able to protect individuals from outside and internal enemies.

Because it is able to respond in a fine-grained, highly parallel, distributed, decentralized, and coordinated way to enormous varieties of foreign materials, the idea of the human immune system provides a fascinating analogous physiological solution to the spyware problem.[138] Like antigens, spyware comes in a multitude of forms. No centralized command-and-control "inoculation" system could ever deal with spyware, because the learning/feedback loops would be simply too slow and too clumsy, and it would fail to deal with intruders it had never seen before.[139] An immune system can "learn" about particular foreign patterns—invading bits—and then remember what it learns.[140] It solves by swarming.

---

136. Stephanie Forrest & Steven Hofmeyr, *John Holland's Invisible Hand: An Artificial Immune System* (1999), http://www.cs.unm.edu/~steveah (presented at the Festschrift held in honor of John Holland).

137. *Id.*

138. Computer scientists know this well, and have been working comfortably with this metaphor for some time. *See* Forrest & Hofmeyr, *supra* note 136. The idea of an immunity network rather than a legal structure as a solution for a hard problem is new to lawyers, however. We are more used to hierarchies.

139. An FTC Report states, "Because the digital fingerprint [used by spyware scanner programs to identify spyware] is only developed after a spyware program is discovered and analyzed, there is a lag time between the distribution of a spyware program and the ability of anti-spyware programs to detect it." FTC, SPYWARE WORKSHOP REPORT, MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 14 (March 2005), http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

140. When the immune system encounters a new pathogen, it might take three weeks or so to clear the initial infection. Steven Hofmeyr, An Immunological Model of Distributed Detection and Its Application to Computer Security 30 (1999) (unpublished Ph.D. dissertation, University of New Mexico) (on file with author). But later invasions by the same pathogen will be reacted to much more quickly—indeed, there may be no evidence of a re-infection. *Id.* A classic example of immune system memory is the system's reaction to measles. *Id.*

A network built like an immune system would allow for a great deal of redundancy and simultaneously reduce local complexity, leaving less for individual machines/users to know. It would observe user-network interactions; learn the code paths that each application uses during its normal operations ("self"); develop a profile of each application's behavior and then block anything that falls outside that profile and is likely to do serious harm ("harmful non-self");[141] tell the human later what has been blocked (which, as "good" spam filters have taught us, is much better than simply blocking the material invisibly); log the event; minimize harm to the rest of the life going on inside the network; and allow creation of metainformation that will help other users. It would also operate in a completely decentralized fashion. The immune system, after all, is made up of millions of agents that act completely locally.

As just one existing example, Sana Security, founded by Steven Hofmeyr, is building computer security schemes that are based on immunity ideas.[142] Sana's software can "learn and take care of itself."[143] It "installs on the operating system and takes a snapshot of how the uninfected machine normally works."[144] Then "it waits and watches for anomalies to normal computing behavior and takes action against any deviation that could harm the PC or alter its normal operation."[145] The operation of this

---

141. Not all pathogens are harmful, and eliminating non-harmful pathogens might actually harm the human body. *Id.* at 1. The same is likely true of code.

142. *See* Sana Security, http://www.sanasecurity.com (last visited Aug. 19, 2005). Computer scientists have been talking about software in biological terms for some time. *See, e.g.*, Stephanie Forrest et. al, *Computation in the Wild*, *in* THE INTERNET AS A LARGE-SCALE COMPLEX SYSTEM (K. Park & W. Willinger eds. forthcoming), *available at* http://crypto.stanford.edu/portia/pubs/articles/FBGA1917099772.html (claiming that networked computer systems can be better understood, controlled, and developed when viewed from the perspective of living systems).

143. John Verity, *Computing*, MIT TECH. REV., Oct. 2003, http://www.techreview.com/Articles/03/10/tr100computing1003.asp; Dan Neel, *Sana Gives Desktop PCs Autoimmunity*, SECURITYPIPELINE.COM, Oct. 25, 2004, http://www.securitypipeline.com/news/51200074.

144. Neel, *supra* note 143.

145. *Id.* A recent article about watching botnets (networks of compromised machines that can be instructed remotely by an attacker) described the creation of "honeypots" that perform many of the same functions. THE HONEYNET PROJECT AND RESEARCH ALLIANCE, *Know Your Enemy: Tracking Botnets*: *Using Honeynets to Learn More About Bots*, Mar. 13, 2005, http://www.honeynet.org/papers/bots. These honeypots "actively participate in networks (e.g. by crawling the web, idling in IRC channels, or using P2P-networks) or modify honeypots so that they capture malware and send it to anti-virus vendors for further analysis." *Id.* There are, however, also legal risks of monitoring networks:

software may initially be annoying, until we teach it what we want it to allow. Like a young student, it may begin with many questions.

If Sana can do this, any other company can too. It is very likely that "immunity networks" will soon be available to us (either on our own desktops or within our own networks) that will learn our hard drives and watch for anomalies.[146] In small ways, these networks are already developing. Some excellent tools are already available to combat spyware, including Microsoft Anti-Spyware, Spybot Search and Destroy, Lavasoft's AdAware, CounterSpy from Sunbelt Software, and Computer Associate's eTrust PestPatrol. Sites like spywarewarrior.com and securitypipeline.com will help us figure out which networks to join or adopt.[147]

Very early versions of immunity networks already exist, in the form of updated Symantec or Norton client applications. To some extent, these applications learn from their environment and watch for events to which they should respond. But I suggest that these applications are primitives. They are not decentralized or peer-created. They rely on updated authoritative blacklists of undesirable bits and applications. Significantly, ISPs

---

> For honeynet deployments in the U.S., consider three legal issues: first, ensure that you are in compliance with the laws that restrict your right to monitor the activities of users on your system. Second, recognize and address the risk that attackers will misuse your honeynet to commit crimes, or store and distribute contraband. Third, consider the possibility that your honeynet will be used to attack other systems, and the potential liability you could face for resulting damage. Your lawyer may identify other legal issues as well. If you deploy a honeynet outside the U.S., look to the applicable laws of the jurisdiction in which you will operate. Designing and implementing your honeynet with attention to these concerns can help you stay out of legal trouble.

THE HONEYNET PROJECT, KNOW YOUR ENEMY 252 (2004).

146. Cisco is already doing this. *See Core Elements of the Cisco Self-Defending Network Strategy* (Cisco Self-Defending Network, White Paper 2005), http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_white_paper0900aecd80247914.shtml. It has introduced its own "adaptive security" program, which relies on "network-based, multi-layered, application-oriented, IP-dependent, worm mitigation, dynamic trust" elements. *Id.* Its plan is for all network hardware and software on the backbone and within enterprises to be coordinated to provide security against spyware and other security threats. *Id.* Although enterprise network security is a classic subject, Cisco may have larger plans for "the Internet" itself.

147. Microsoft recently introduced its own anti-spyware program, available to Windows XP and Windows 2000 users for free download through July 2005. Microsoft Windows AntiSpyware (Beta), http://www.microsoft.com/athome/security/spyware/software/default.mspx (last visited Aug. 19, 2005). This event marks an enormous step forward because Windows operating systems run on more than 90 percent of computers worldwide.

like Earthlink and AOL are already competing on the basis of their ability to protect users from spyware,[148] and many ISPs spend up to 40 percent of their customer service resources responding to spyware-related inquiries.[149]

All of these things, taken together, will provide a solution to oppressive spyware. They will take the self-conscious form of immunity networks when users affirmatively tie their online access and communications to the use by themselves *and others they communicate with* of spyware protections that learn. We will eventually leave the ISP model of "membership" (which is based only on commodity connectivity rather than valuable learning/reaction services provided by network administrators) and move towards participation in immunity networks.[150] (These networks may map to the outlines of current ISPs for the foreseeable future, but with the rise of wireless mesh services ISPs as a business category may diminish in importance as the years go by.)[151] Groups of machines and people will cluster together, looking for companionship as well as security, and to join one of these networks will be to buy into a set of practices governing many different kinds of interactions.

We should wait for these steps to take effect, rather than plunging towards legislative solutions that are likely to cause more troubles than they solve. Law should now look at technology problems the way modern doctors look at health care: "do no harm," "do not give antibiotics when you

148. EarthLink offers a free software suite to its users that blocks spyware, spam, and viruses. Earthlink TotalAccess, http://www.earthlink.net/software (last visited Aug. 19, 2005). AOL claims it is the first ISP to offer automated spyware detection. Paul Roberts, *AOL Goes After Spyware*, PC WORLD, Jan. 6, 2004, http://www.pcworld.com/news/Article/0,aid,114106,00.asp.

149. Jim Thompson, *Malware Returns*, ISP-PLANET, May 27, 2005, http://www.isp-planet.com/business/2005/spyware.html.

150. I believe that the ISP intermediary business model, under which ISPs provide commodity connectivity to upstream networks, is already under enormous pressure, and that in the coming years, we will see great consolidation in the ISP marketplace. This is already happening in India. *See* Joji Thomas Philip, *80% ISPs fall off infobahn*, BUSINESS STANDARD, June 14, 2005, http://www.business-standard.com/iceworld/storypage.php?hpFlag=Y&chklogin=N&autono=191508&leftnm=lmnu9&leftindx=9&lselect=0 (reporting that 80 percent of India's 700 private ISPs have gone out of business in the last four years). Surviving ISPs will have to reinvent themselves as much more meaningful businesses, and immunity provisions may provide a useful path towards solvency.

151. *See* Microsoft Networking Research Group, *Self-Organizing Neighborhood Wireless Mesh Networks*, http://www.research.microsoft.com/mesh (last visited Aug. 19, 2005) (describing the topology of "community-based multi-hop wireless networks," in which every member of the network contributes packet-routing resources). Traditional broadband providers (DSL, cable, satellite, T1) will still be needed to get these packets to the public Internet, but the intermediary role of the local ISP may disappear in time.

are only dealing with a virus," and "help the body develop its own defenses." Congress, like an HMO, should approve (or defer to) treatments, fund research, regulate use of highly, facially dangerous substances, and otherwise get out of the way. Much is already being done without legislative involvement.

IV. THE IMPLICATIONS OF TECHNICAL IMMUNITY NETWORKS

The set of problems that we lump together as "spyware" (a set that is itself full of ever-increasing variety) is a particular expression of the world's complexity. We have opened ourselves to communication, and it is too much for us (or at least for our relatives) to deal with. No human being, and no legal institution, can single-handedly take on this problem.

I have suggested in this Article that the only real solutions to spyware are technical in nature, and that these technical solutions will come in the form of immunity networks. This suggestion leads me to guess that our focus on individual privacy and our obsession with global interconnectivity may both become inappropriate or irrelevant as the Internet changes. It may be time to recognize that individuals, and their unhappy relationships with spyware, will not always be the most important actors in this technical environment. It may be that individuals need to choose to cede some control over their individual machines to networks that will help in the constant fight against oppressive spyware and malware.[152]

I am emphatically not suggesting that membership in an immunity network be mandated by statute. Rather, it may be that some of the ultimate connectivity providers (the entities that make it possible to reach the public Internet) will mandate as a condition of service that individuals sign up for one of several immunity providers. It may become more expensive for individuals who have not joined such a network to be online.

This is not a move towards enforced similarity, as in communism. Nor is this a move towards a voting, democratic approach to software, where software that is voted "bad" becomes illegal. Instead, we need to recog-

152. The P3P lesson tells us that even with some controls ceded, users can be given opportunities to reverse or override decisions made by (and defaults set by) machines and networks. P3P, or Platform for Privacy Preferences, automatically compares a consumer's privacy preferences with a website's privacy policy and alerts the consumer to any discrepancies. *See* Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P (last visited Aug. 19, 2005). Of course, even if we cede some of our autonomy to immunity networks, and establish clear boundaries between them, we will never, ever win the battle against "spyware." We will experience local emergencies, great ups and downs, and periods of calm, but we will never be completely at peace.

nize that there is already in the world a third way of governing that we need to begin to embrace as we face difficult technical warfare: competing networks. Such networks may be more flexible than any presumptively uniform law, although such flexibility will be possible only if: (1) exit from and entry into these networks is truly voluntary, and (2) adequate competition among networks exists.

Only by allowing these networks to "represent" and protect us technically will we survive the coming malware difficulties. Laws and litigation will not shield us, because the rate of change is too great and the varieties of attack too diverse. What the body does with overwhelming flows of sensory data is to "chunk" it, creating metainformation that can be dealt with. Similarly, these new networks will have a real role in collecting data about information flows, chunking it, and using the patterns that are revealed to protect their subscribers. The network will know when it is under attack and will pay attention. We, as individuals acting alone, are no longer capable of protecting ourselves from electronic attack. (Of course, individuals who have access to peer-created shields will be protected. I am talking about individuals trying to decide on the acceptability of every electronic message.)

The boundaries between these immunity networks will need to be real as well. Where these boundaries are unclear, dangerous electronic conditions may exist. Voluntary separation, with well-policed gateways that open deliberately, may be the best alternative to violence. I am troubled by this suggestion, because I am loath to create gatekeepers that have power over my or anyone else's communications. But even the co-inventor of the TCP/IP protocol, Vint Cerf, said recently that he wished that end-to-end authentication had been part of the protocol's original design.[153] Gateways between networks could check for communications that were adequately credentialed, and could perhaps do so in a lightweight fashion. To the extent we are at the beginning of a cataclysmic series of malware invasions, we may need to support good fences in order to keep communications flowing at all.[154]

The legal status of immunity networks raises fascinating questions that range far beyond the scope of this initial, exploratory study of the relatively narrow subject of spyware legislation. It may be that we have come into an era in which we need governments and hierarchies for atom-based

153. Vint Cerf, General Comments at The Freedom To Connect Conference, Silver Spring, Maryland (March 30, 2005).

154. *See* David R. Johnson, Susan P. Crawford & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 9 (2004).

issues—when to put someone in prison, when to settle a property dispute—but that networks of various kinds, chosen by us, can best deal with the problems of digital bits. We may need to tell terrestrial governments that they are in charge of atoms—food and chemicals—but not in charge of minds or culture. This may happen as a matter of course, without explicit statements on anyone's part, as governments and prosecutors come to recognize the need to defer to networks that are solving problems for citizens. Until this recognition dawns, the only appropriate governmental initiative should be to do no harm.