

Regulating Spyware: The Limitations of State “Laboratories” and the Case for Federal Preemption of State Unfair Competition Laws

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 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 Internet-related activities. The final section of the article extrapolates from this study of spyware regulation to the larger context of Internet governance.

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 attacks,³ spam,⁴ spIM,⁵ phishing,⁶ copyright infringement,⁷

* 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 Eric Goldman for comments and Richard Ronald and Carol Jones for research assistance on state unfair competition law. I also thank Ben Edelman for his website on spyware-related issues.

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 Ughetta Manzone, Trademark: Domain Name: Dilution - Panavision International, L.P. v. Toeppen, 13 Berkeley Tech. L.J. 249 (1998); 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).

² See George Smith, Billion-dollar virus economics, The Register (Apr. 29, 2002) http://www.theregister.co.uk/2002/04/29/billiondollar_virus_economics/; Eric J. Sinrod and 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); Michael Lee et al., Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, 14 Berkeley Tech. L.J. 839 (1999).

³ See id.

⁴ In its most expansive usage, spam refers to the sending of any unsolicited,

and spyware have dispelled an earlier cyber-libertarian hope that the Internet could adequately be governed through code or social norms (“netiquette”).⁸ 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 and the Federal Communications Commission), 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 have largely addressed concerns relating to cybersquatting. Technological fixes, enhanced security, and user vigilance have

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 web sites 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?,” *Chicago Tribune*, August 5, 1999.

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 web pages purporting to be operated by the company whose name is used in the message. The replica web page 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 Peter S. Menell, *Envisioning Copyright Law's Digital Future* 46 *N.Y. Law School Law Review* 63 (2003); Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models*, 22 *Cardozo Arts & Entertainment L.J.* 725 (2005).

⁸ See Vinton G. Cerf, *Building an Internet Free of Barriers*, *NY Times* § 3 p 12 (July 27, 1997); Thomas E. Weber, *The Internet (A Special Report): Debate: Does Anything Go? Limiting free speech on the Net*, *Wall Street J* (Dec 8, 1997); George Black, *Call for Controls: The Internet Must Regulate Itself*, *Fin Times* part 4 p 12 (Apr 1, 1998); Johnson and Post, *supra* n. __; 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.”); but cf. Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 *Chicago-Kent L. Rev.* 1257 (1998); Jack Goldsmith, *Against Cyberanarchy*, 65 *U. Chi. L. Rev.* 1199 (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 and Kristina McGrath, *Identifying and Evaluating the Business Impact of Network Risks and Liabilities*, 33 *WTR Brief* 18 (Winter 2004); U.S. Federal Trade Commission, *Safe at Any Speed: How to Stay Safe Online if You Use High-Speed Internet Access* (Sept. 2002) <http://www.ftc.gov/bcp/online/pubs/online/safeonline.pdf>.

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 fraudulent and pernicious ends.¹³ Spyware often operates in conjunction with other software that delivers advertisements (such as pop-up windows), harvests private information, and re-routes web traffic. Recent studies reveal that as many as 90 percent of home computers in the United States as well as many business computers are running spyware, 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

¹¹ See Lynch, *supra* n. __.

¹² See generally Menell, *supra* n. __; Hughes, *supra* n. __; Kristina Groenings, Costs and Benefits of the Recording Industry's Litigation Against Individuals, 20 Berkeley Tech. L.J. 571 (2005).

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

¹⁴ See John Borland, Dell Backs Spyware Education Drive, C/Net News.com (Oct. 15, 2004) (reporting findings of report from the Consumer Spyware Initiative, a joint project sponsored by Dell Computer and the Internet Education Foundation)
http://news.com.com/Dell+backs+spyware+education+drive/2100-1032_3-5410568.html; John Borland, Spike in "Spyware" Accelerates Arms Race, C/Net 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, C/Net News.com (Dec. 21, 2004) (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.")
http://news.com.com/Worst+spyware+queues+up/2100-7349_3-5499609.html

¹⁶ See Declan McCullagh, Few Solutions Pop Up at FTC Adware Workshop, C/Net News.com (Apr. 19, 2004) (noting that spyware concern have become the leading support problem for computer vendors and computer security companies)
http://news.com.com/Few+solutions+pop+up+at+FTC+adware+workshop/2100-1028_3-5195222.html; Stefanie Olsen, Revenge of the Pop-ups, C/Net News.com (Oct. 14, 2004) (characterizing the interplay between browser providers (who seek to block pop-up

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

Regulating spyware is complicated by the fact that some “spyware” or “adware” technology can offer benefits to consumers, advertisers, and web publishers by improving the targeting of advertising “vehicles.”¹⁸ Emerging “behavioral marketing” software-based business models¹⁹ 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

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.”)

http://news.com.com/Revenge+of+the+pop-ups/2100-1024_3-5408453.html

¹⁷ See Ilett, *supra* n. __ (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, C/Net News.com (Jul. 28, 2004) (describing software programs that reinstall even after a user removes it from their computer’s registry).

http://news.com.com/Google+feels+spyware+strains/2100-1024_3-5250383.html Some programs claiming to eliminate spyware actually install other forms of advertising software. See John Borland, Spyware Cures May Cause More Harm than Good, C/Net 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.” See Declan McCullagh, Adware’s Going Mainstream, Report Says, C/Net 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, C/Net News.com (Feb. 8, 2005) (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.”)

http://news.com.com/Catfight+in+the+spyware+corral/2100-1032_3-5567781.html

¹⁹ See, e.g., D. Reed Freeman, Jr., Privacy and the Future of Behavioral Marketing (written by Chief Privacy Officer for Claria Corporation)

http://www.claria.com/advertise/oas_archive/privacy.html?pub=imedia_module

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 A. Mitchell Polinsky and Steven Shavell (eds.) Handbook of Law and Economics (forthcoming 2005) (discussing the range of private and public institutions governing advertising).

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 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 characteristics of 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 cannot be targeted on a per viewer basis. The medium of traditional television distributes the same advertisement to all viewers in a particular market. 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 males watch some programming of particular interest to women. If advertisers could reach better defined market segments, or ideally particular individuals, more accurately and easily, 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.²⁴

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

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.”)

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 George J. Stigler, *The Economics of Information*, 69 *Journal of Political Economy* 213 (1961); P. Nelson, *Advertising as Information*, 82 *Journal of Political Economy* 729 (1974); P. Nelson, *The Economic Consequences of Advertising*, 48 *Journal of Business* 213 (1975).

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 at that time. For this reason, behavioral marketing software yields relatively high “click through” rates – i.e., the percentage of consumers clicking on advertisements to learn more about what is being offered – than randomly targeted pop-up advertisements.²⁵ 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.²⁶

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 web page 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.³⁰ Rather, it analyzes the proper jurisdiction or governmental level for

²⁵ 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? C/NET News.com (June 26, 2002) http://news.com.com/Reality+check+Does+adware+work/2009-1023_3-938263.html; see also Adam L. Penenberg, Ads That Annoy Also Succeed, *Wired* (Sept. 8, 2004) (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.") <http://www.wired.com/news/business/0,1367,64807,00.html>

²⁶ 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* n. __.

³⁰ See generally Kristen M. Beystehner, See Ya Later, Gator: Assessing Whether Placing Pop-Up Advertisements on Another Company's Website Violates Trademark 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).

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.³¹

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."³² 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 for personal jurisdiction,³³ 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.³⁴ Given the abstruse, vague, and uncertain contours of state unfair competition law, a

³¹ Most prior scholarship touching on federalism issues and the Internet have focused on jurisdiction and more abstract issues of governance. See Dan L. Burk, *Federalism in Cyberspace*, 28 *Conn L Rev* 1095 (1996); Joel R. Reidenberg, *Governing Networks and Rule-making in Cyberspace*, 45 *Emory L J* 911 (1996); David R. Johnson and David Post, *Law And Borders--The Rise of Law in Cyberspace*, 48 *Stan L Rev* 1367 (1996); Jack Goldsmith, *Against Cyberanarchy*, 65 *U. Chi. L. Rev.* 1199 (1998); Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 *U. Pa. L. Rev.* 311, 323 (2002).

³² *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., Richard W. Garnett, *The New Federalism, The Spending Power, and Federal Criminal Law* 89 *Cornell L. Rev.* 1, 18 (2003); Lucian Arye Bebchuck, *Federalism and the Corporation: The Desirable Limits on State Competition in Corporate Law*, 105 *Harv. L. Rev.* 1435 (1992); Eric Lamond Robinson, *The Oregon Basic Health Services Act: A Model for State Reform* 45 *Vand.L.Rev.* 977, 986-88 (1992); Deborah Jones Merritt, *The Guarantee Clause and State Autonomy: Federalism for a Third Century*, 88 *Colum. L. Rev.* 1, 3-10 (1988); Roberta Romano, *The State Competition Debate in Corporate Law*, 8 *Cardozo L. Rev.* 709 (1987); Lewis B. Kaden, *Politics, Money and State Sovereignty: The Judicial Role*, 79 *Colum. L. Rev.* 847, 853-55 (1979)

³³ See generally 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); Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 *Berkeley Tech. L.J.* 1345, 1352 (2001)..

³⁴ I do not mean to question the value of policy experimentation, but to recognize that

federal preemptive regulatory approach provides a better climate than decentralized state regimes for both regulating spyware and encouraging business and software innovation.

The article begins by developing 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. Part II 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, it 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 III reviews federal initiatives aimed at addressing spyware concerns. The concluding section extrapolates from this study of spyware regulation to the larger context of Internet governance.

I. 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 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.³⁵

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.³⁶

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.

³⁵ 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")

³⁶ See Richard O. Zerbe, *Optimal Environmental Jurisdictions*, 4 *Ecology L.Q.* 193 (1974); Richard B. Stewart, *Pyramids of Sacrifice? Problems of Federalism in Mandating State*

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’ metaphor draws upon a fundamental and powerful method of modern science – the idea of controlled experimentation. Science 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.”³⁷ In this way, the differing policies of the states could be examined essentially as independent experiments, producing valid, independent data for assessing alternative policies.³⁸ 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.

Implementation of National Environmental Policy, 86 Yale L.J. 1196 (1977); Daniel C. Esty, Revitalizing Environmental Federalism, 95 Mich. L. Rev. 570 (1996); but cf. Richard L. Revesz, Federalism and Environmental Regulation: A Public Choice Analysis, 115 Harv. L. Rev. 553 (2001).

³⁷ *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

³⁸ The state policy in question in *New States 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. There were arguably economies of scale. Justice Brandeis believed that allowing some experimentation in the regulation of such businesses could produce valuable information. Given the inherently local scale of ice manufacturing and distribution at the time, there is little reason to believe that state experiments would have any significant interstate effects.

Therefore, policy “experiments” can be implemented and studied in isolation.³⁹ In fact, land use has long been viewed as an area in which local authority remains paramount.⁴⁰ 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 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 nation at large.” The inherent architecture of the Internet – which make it difficult if not impossible to restrict Internet access to one or several states⁴¹ – in combination with the relatively liberal rules of personal jurisdiction⁴² mean that most substantial Internet-based commercial activities are subject to liability in many if not all of the 50 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

³⁹ Even land use policies can distort out-of-state communities to the extent that they influence interstate commerce.

⁴⁰ 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 and Eric T. Freyfogle, *Wildlife Law* 831-1099, 1164-1349 (2002).

⁴¹ 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 U.C.L.A. L. Rev. 925, 930-34 (2001); J.H. Saltzer et al., *End-to-End Arguments in System Design*, available at <http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf> (Apr. 8, 1981), reprinted in *Innovation in Networking* 195-206 (Craig Partridge ed., 1988); but cf. Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 Pa. L. Rev. 1951 (2005) (suggesting that innovations in information technology may afford states greater ability to enforce their regulatory policies electronically).

⁴² See supra n. ___; Reidenberg, supra n. ___.

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 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.⁴³ 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

⁴³ See Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (1971); James Buchanan & Gordon Tullock, *The Calculus of Consent* (1962); William Eskridge, Jr., *Politics Without Romance: Implications of Public Choice Theory for Statutory Interpretation*, 74 Va. L. Rev. 275, 285-88 (1988).

the extent that federal or state legislators are more 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.⁴⁵ 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.⁴⁶ 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 capture the legislature of only 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 of behavioral marketing is somewhat more complex due to the multiplicity of business interests. The battle appears to be between traditional web publishers⁴⁷ and emerging behavioral marketing companies.⁴⁸ 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.⁴⁹ It is not at all clear that federal

⁴⁵ See e.g., Stewart, *supra* n. __; Esty, *supra* n. __; but see Revesz, *supra* n. __.

⁴⁶ See Stewart, *supra* n. __ 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.”); Esty, *supra* n. __, at 597-98 (arguing that “asymmetries [among interest groups] may be more significant at the state and local levels” than the federal level).

⁴⁷ The Interactive Advertising Bureau (IAB) represents companies that sell interactive advertising, such a web publishers – companies that deliver banner and other advertisements to visitors of their websites. See Stefanie Olsen, Chorus of Gator Critics Grows C/Net News.com (Aug. 27, 2001) http://news.com.com/Chorus+of+Gator+critics+grows/2100-1023_3-272244.html

⁴⁸ See *infra* text accompanying n. __.

⁴⁹ The following organizations have mobilized around these issues: Center for Democracy and Technology (see Spyware page <<http://www.cdt.org/privacy/spyware/>>), Electronic Frontier Foundation (see Wendy Seltzer, Spitzer Suit Shows the Right Way to Fight Spyware (Apr. 28, 2005) <<http://www.eff.org/deeplinks/archives/003536.php>>), and Electronic Privacy Information Center (<http://www.epic.org>). A researcher at the Berkman Center for Internet and Society has long followed spyware and adware issues and served an active advocacy role. See <http://www.benedelman.org/>.

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.⁵⁰ 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 experiments with more restrictive policies.

At least on theoretical grounds, therefore, the case for federal preemption of state regulation of Internet activities appears quite strong.⁵¹ 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-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.⁵² 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

⁵⁰ See *infra* text accompanying n. ____.

⁵¹ 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? Wash. Post (May 7, 2005) (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) <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/07/AR2005050700597_pf.html>; Wendy Seltzer, Spitzer Suit Shows the Right Way to Fight Spyware (Apr. 28, 2005) <<http://www.eff.org/deeplinks/archives/003536.php>. 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.

⁵² See *infra* text accompanying note ____.

federal regulatory system would offer substantial advantages without jeopardizing consumer protection or fair business competition.

II. 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 I, 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 governed almost exclusively by federal law⁵³ and therefore does not require further consideration here.⁵⁴ 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

⁵³ See 17 U.S.C. § 301; see generally Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 1.01..

⁵⁴ 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, 309 F.Supp.2d 467, 484-88 (SDNY 2003); Wells Fargo, 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 Cal. L. Rev. 817 (2001).

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.”⁵⁵ 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.”⁵⁸ 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 coverage⁵⁹ and extend well beyond the task of assessing the allocation of governance responsibilities between federal and state authorities. Hence, I will focus 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 marks in commerce. An optional federal registration process complements this system. The latter approach, which took root in the Federal Trade Commission formed in 1914, relies principally on a regulatory/public enforcement model.

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

⁵⁵ *Ely-Norris Safe Co. v. Mosler Safe Co.*, 7 F.2d 603 (2d Cir. 1925), *rev'd on other grounds*, 273 U.S. 132 (1927).

⁵⁸ *American Safety Table Co. v. Schreiber*, 269 F.2d 255, 271 (2d Cir. 1959).

⁵⁹ See generally, Restatement (Third) of Unfair Competition; J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* (4th ed. 2005); Callmann on Unfair Competition, Trademark, and Monopolies (4th ed.)

As the mercantile economy developed in the early to mid 19th century, federal courts came to see trademark infringement as an actionable offense.⁶⁰ Justice Joseph Story granted the first injunction based on trademark infringement in 1844.⁶¹ 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 statute⁶² pursuant to the Intellectual Property Clause of the U.S. Constitution.⁶³ After the Supreme Court struck down the act as exceeding the scope of that clause (which authorizes Congress to enact laws promoting the progress of science and the useful arts),⁶⁴ Congress reenacted a more limited statute in 1881 pursuant to the Commerce Clause limiting protection to marks in foreign commerce.⁶⁵ 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 non-competing goods.⁶⁶

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.⁶⁷ 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 New Service v. Associated Press*⁶⁸ 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

⁶⁰ See generally Zechariah Chafee, Jr., *Unfair Competition*, 53 Harv. L. Rev. 1289 (1940); Rudolf Callmann, *What Is Unfair Competition?* 28 Geo. L.J. 585 (1940); Milton Handler, *Unfair Competition*, 21 Iowa L. Rev. 175 (1936).

⁶¹ *Taylor v. Carpenter*, 23 F. Cas. 742 (CCD Mass. 1844) (No. 13784).

⁶² Act of July 8, 1870, 16 Stat. at L 198, §§ 77-84, entitled “An Act to Revise, Consolidate and Amend the Statutes Relating to Patents and Copyrights.” Ch. 2, tit. 60, §§ 4937-4947, Revised Stats.

⁶³ Article I, Section 8, Clause 8.

⁶⁴ See *Trade-Mark Cases*, 100 U.S. 82, 94 (1879).

⁶⁵ Act of March 3, 1881, 21 Stat. 502.

⁶⁶ Act of Feb. 20, 1905, 33 Stat. 724, 15 U.S.C.S. §§ 81 et seq. “An Act to authorize the registration of trademarks used in commerce with foreign nations or among the several States or with Indian Tribes, and to protect the same.”

⁶⁷ See *McCarthy on Trademarks*, supra n. ___, at § 1.12.

⁶⁸ 248 U.S. 215 (1918).

of a lawful business is as much entitled to protection as the right to guard property already acquired.”⁶⁹ 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.”⁷⁰ 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.⁷¹

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 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.⁷²

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.⁷³ 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 Federal Trade Commission. In 1914, Congress enacted the Federal Trade Commission Act for the primary purpose of enforcing federal anti-trust laws by preventing “unfair methods of competition.” In addition to pursuing anti-competitive 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 1922.⁷⁴ In 1938, Congress clarified that the FTC’s jurisdiction extends to

⁶⁹ Id. at 236.

⁷⁰ Id. at 240.

⁷¹ Id. at 246-48.

⁷² *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).

⁷³ See *Washboard Co. v. Saginaw Mfg. Co.*, 103 Fed. 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).

⁷⁴ See *Federal Trade Commission v. Winsted Hosiery Co.*, 258 U.S. 483 (1922).

deceptive practices without regard to evidence of competitive harm.⁷⁵ The Commission must, however, establish that its actions respond to specific and substantial harm to the public interest.⁷⁶

ii. 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*,⁷⁷ 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.⁷⁸ 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.⁷⁹ 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.⁸⁰ The 1988 revision of § 43(a) removed any doubt that the

Commentators came to see the FTC as “the Magna Carta of truth in interstate trade of incalculable service to both industry and the public at large.” See Ely, *The Work of the Federal Trade Commission*, 7 Wis. L. Rev. 195, 209-10 (1932).

⁷⁵ Wheeler-Lea Amendment of 1938, ch. 49, § 3, 52 Stat. 111 (codified at 15 U.S.C. § 45(a) (2000)).

⁷⁶ *Federal Trade Commission v. Klesner*, 280 U.S. 19 (1929).

⁷⁷ 304 U.S. 64 (1938).

⁷⁸ Act of July 5, 1946, ch. 540, 60 Stat. 427 (1946) (codified as amended at 15 U.S.C. §§1051-1127 (2004)).

⁷⁹ See *Samson Crane Co. v. Union National 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 *Washboard Co. v. Saginaw Mfg. Co.*, 103 Fed. 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); *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).

⁸⁰ See *U-Haul Intern., Inc. v. Jartran, Inc.*, 681 F.2d 1159, 1162 (9th Cir. 1982); *Procter & Gamble Co. v. Chesebrough-Pond's Inc.*, 747 F.2d 114 (2d Cir. 1984); *Coca-Cola Co. v.*

Lanham Act extends to both misrepresentations of source and other deceptive representations made in connection with the marketing of goods and services⁸¹ and does away with the single source limitation on recovery.⁸² The plaintiff must, however, establish some likelihood of harm to itself in order to have standing to bring an action under the Lanham Act.⁸³ Congress has since expanded the federal unfair competition regime to provide causes of action against dilution of famous marks⁸⁴ and registration of trademarks as domain names in bad faith.⁸⁵

Procter & Gamble Co., 822 F.2d 28 (6th Cir. 1987).

⁸¹ Pub. L. 100-667, 102 Stat. 3935 (1988). As revised, trademark liability extends to:

(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.

⁸² See *Forschner Group, Inc. v. Arrow Trading Co., Inc.*, 833 F. Supp. 385 (S.D.N.Y. 1993), *order vacated*, 30 F.3d 348 (2d Cir. 1994) (allowing one of two sellers of genuine product to sustain an action for false advertising without the other); *Pacamor Bearings, Inc. v. Minebea Co., Ltd.*, 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); *ALPO Petfoods, Inc. v. Ralston Purina Co.*, 913 F.2d 958, 964, 16 U.S.P.Q.2d (BNA) 1081 (D.C. Cir. 1990).

⁸³ See *Ortho Pharmaceutical Corp. v. Cosprophar, Inc.*, 32 F.3d 690 (2d Cir. 1994); *PDK Labs, Inc. v. Friedlander*, 37 U.S.P.Q.2d (BNA) 1195 (S.D. N.Y. 1995), *aff'd*, 103 F.3d 1105 (2d Cir. 1997) (denying standing to sue under § 43(a) to one who is not yet a competitor of the alleged false advertiser). 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), *aff'd*, 129 F.3d 1252 (1st Cir. 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).

⁸⁴ See Federal Anti-Dilution Act, Pub. L. 104-98, 109 Stat. 985 (1996) (codified at 15 U.S.C. §§ 1125(c); 1127 (definition of "dilution"))

⁸⁵ See Anti-cybersquatting 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)).

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 development of such laws, the FTC drafted a model act in the late 1960s – the Unfair Trade Practices and Consumer Protection Law (UTPCPL).⁸⁶ Like the FTC Act, the model state law authorized the creation of state agencies to promulgate standards to combat unfair and deceptive practices⁸⁷ 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.⁸⁸ This provision – focusing on

⁸⁶ See Unfair Trade Practices and Consumer Protection Law (contained in Council of State Governments, 26 Suggested State Legislation 141-52 (1970)).

⁸⁷ Section 2 of the model Act offered states three formulations for their laws: Alternative Form No. 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, false advertising – as well as a general bar against “any act or practice which is unfair or deceptive to the consumer.”

⁸⁸ 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 if 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

persons who suffer ascertainable 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.

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.⁸⁹ 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 established by statutes, the common law, or otherwise - whether, in other words, it is within at least the penumbra of some common-

and costs.

(e) Any permanent injunction, judgment or order of the court made under Section 5 [providing for the Attorney General to bring 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.

⁸⁹ See H.R. Conf. Rep. No. 1142, 63d Cong., 2d Sess., at 19 (1914) (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”).

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).⁹⁰ 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.⁹¹

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.*,⁹² 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.”⁹³ 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, to the consumer’s detriment.”⁹⁴ This standard was ratified a year later in *In re Cliffdale Associates*.⁹⁵ By focusing upon whether an act or practice is likely to mislead consumers acting reasonably in the circumstances to their detriment, the 1983 standard

⁹⁰ Statement of Basis and Purpose, 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. 223, 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).

⁹¹ FTC’s Policy Statement on Fairness, which was published in a letter from the Commission to members of the Consumer Subcommittee of the Committee on Commerce, Science, and Transportation of the U.S. House of Representatives on December 17, 1980 (footnotes omitted). <<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.

⁹² 291 U.S. 67, 81 (1934).

⁹³ *Charles of the Ritz Distrib. Corp. v. FTC*, 143 F.2d 676 (2d Cir. 1944) (concerning an advertisement claiming that “Rejuvenescence Cream will rejuvenate and restore youth or the appearance of youth to the skin, regardless of the condition of the skin”). Quoting the Supreme Court’s decision in *Federal Trade Commission 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 Gellhorn, Proof of Consumer Deception before the Federal Trade Commission, 17 U. Kan. L. Rev. 559 (1969).

⁹⁴ Federal Trade Commission Policy Statement on Deception (Oct. 14, 1983).

⁹⁵ 103 F.T.C. 110 (1984); see generally Jack E. Cairns, State Regulation of Deceptive Trade Practices Under “Little FTC Acts”: Should Federal Standards Control?, 94 Dickinson L. Rev. 373 (1990).

narrowed the reach of the FTC Act.⁹⁶

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* decision⁹⁷ 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.⁹⁸ In the false advertising area, they have retained the single source limitation as a barrier to recovery;⁹⁹ although many state legislatures have abolished this restriction through legislation. The misappropriation tort articulated by the Supreme Court in *International New Service v. Associated Press*¹⁰⁰ has been elaborated to some extent, but has not been expanded.¹⁰¹

⁹⁶ See Bailey & 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).

⁹⁷ *Erie R.R. Co. v. Tompkins*, 304 U.S. 64 (1938).

⁹⁸ See generally, Restatement (Third) Unfair Competition.

⁹⁹ See e.g., *California Apparel Creators v. Wieder of Cal.*, 162 F.2d 893 (2d Cir. 1947). See generally 1A Callmann on Unfair Competition, Trademark, and Monopolies, § 5:2 (4th Ed.). “[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. Products, Inc.*, 242 F. Supp. 302 (N.D. Ill. 1965); followed in *Julie Research Laboratories, Inc. v. General Resistance, Inc.*, 25 A.D.2d 634, 635, 268 N.Y.S.2d 187 (1st Dep’t 1966), *order aff’d*, 19 N.Y.2d 906, 281 N.Y.S.2d 96, 227 N.E.2d 892 (1967); followed in *Magnus Organ Corp. v. Robbins Music Corp.*, 163 U.S.P.Q. (BNA) 695 (N.Y. Sup 1969): “While 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.” *Nordictrack, Inc. v. Soloflex, Inc.*, 31 U.S.P.Q.2d (BNA) 1732, 1734 (D. Or. 1994): (“to prevail under Minnesota [common] law, [plaintiff] must establish that it lost sales through [defendant’s] false advertising.”); *Multi-Tech Systems, Inc. v. Hayes Microcomputer Products, Inc.*, 800 F. Supp. 825, 848 (D. Minn. 1992); *Ortho Pharmaceutical Corp. v. Cosprophar, Inc.*, 32 F.3d 690 (2d Cir. 1994) (no standing to sue for false advertising without a showing of harm to the plaintiff).

¹⁰⁰ 248 U.S. 215 (1918).

¹⁰¹ See, e.g., *United States Golf Ass’n v. St. Andrews Sys., Data-Max, Inc.*, 749 F.2d 1028 (3d Cir. 1984); *Nat’l Basketball Ass’n v. Motorola, Inc.*, 105 F.3d 841, 847 (2d Cir. 1997); but see *United States Golf Ass’n v. Arroyo Software Corp.*, 81 Cal. Rptr. 708, 714 (Ct. App. 1999). See generally Edmund J. Sease, *Misappropriation: Is Seventy-Five Years Old; Should We Bury It or Revive It?*, 70 N.D. L. Rev. 781 (1994); Richard A. Posner, *Misappropriation: A Dirge*, 40 Hous. L. Rev. 621 (2003); Leo J. Raskind, *The Misappropriation Doctrine as a Competitive Norm of Intellectual Property Law*, 75 Minn. L. Rev. 875 (1991); cf. 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)

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 effects. 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.

i. 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.¹⁰² Following the abrupt elimination of federal common law in 1938, litigants continued to invoke state common law where their claims did 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 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.”¹⁰³ He called for the adoption of either a preemptive federal statute or a uniform state law to govern unfair competition.¹⁰⁴

The American Bar Association's Section of Patents, Trademark and Copyright Law also took note of the problem. In its 1958 report,¹⁰⁵ a special committee concluded that with the exception of California unfair competition law,¹⁰⁶ which was codified in statute, all state unfair

(arguing that flexible and evolving common law norms are an effective means for addressing the dynamism brought about by technological change).

¹⁰² See Keller, “It Keeps Going and Going and Going”: The Expansion of False Advertising Litigation Under the Lanham Act, 59 *Law & Contemp. Probs.* 131 (1996).

¹⁰³ *American Safety Table Co. v. Schreiber*, 269 F.2d 255, 271 (2d Cir. 1959).

¹⁰⁴ 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* n. __.

¹⁰⁵ See Prefatory Note, National Conference of Commissioners of Uniform State Laws, Uniform Deceptive Trade Practices Act (1966) (referencing 1958 ABA Report)

<http://www.law.upenn.edu/bll/ulc/fnact99/1920_69/rudtpa66.htm>

¹⁰⁶ See Cal. Civil Code § 3369; *Netterville*, California Law of Unfair Competition:

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.”¹⁰⁷ 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 1964.¹⁰⁸

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.¹⁰⁹ The uniform law was modeled roughly after California law.¹¹⁰ 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 various forms of false advertising.¹¹¹ The UDPTA 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.¹¹²

The UDTPA affords business enterprises a cause of action against other businesses which obtain a competitive advantage by deceiving consumers. After being adopted by 14 states¹¹³ 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.¹¹⁵ 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.¹¹⁷ Nonetheless, the dozen or so state statutes modeled after the UDPTA remain in effect

Unprivileged Imitation, 28 So Cal. L. Rev. 240 (1955).

¹⁰⁷ See supra n. ___.

¹⁰⁸ Id. NCCUSL amended this report in 1966 to provide for the award of reasonable attorney fees in some circumstances.

¹⁰⁹ Id.

¹¹⁰ See Cal. Civ. Code § 3369

¹¹¹ UDPTA, Section 2.

¹¹² UDTPA, Section 3.

¹¹³ Colorado, Delaware, Georgia, Hawaii, Illinois, Kansas, Minnesota, Nebraska, Nevada, New Mexico, Ohio, Oklahoma, Oregon, and Utah. See Uniform Business and Financial Laws Locator <<http://www.law.cornell.edu/uniform/vol7.html#dectr>>

¹¹⁵ See supra n. ___.

¹¹⁷ See The National Conference of Commissioners on Uniform State Laws Drafts of Uniform and Model Acts <http://www.law.upenn.edu/bll/ulc/ulc_frame.htm>.

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.

ii. 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.¹¹⁸ These causes of action impose relatively high burdens of proof upon plaintiffs.¹¹⁹ Since most consumers suffer relatively 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 (UTPCPL). Fourteen states¹²⁰ adopted some variation on Alternative 1 of the FTC model act.¹²¹ 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 states¹²² adopted some version of Alternative 3, which

¹¹⁸ 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).

¹¹⁹ 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 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 by the exercise of reasonable care could not have ascertained their falsity." *Coffin v. Dodge*, 146 Me. 3, 5-6, 76 A.2d 541, 543 (1950); *Inman v. Ken Hyatt Chrysler Plymouth*, 294 S.C. 240, 242, 363 S.E.2d 691, 692 (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 Rice, *Exemplary Damages in Private Consumer Actions*, 55 Iowa L. Rev. 307 (1969).

¹²⁰ 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."

¹²¹ See Note, *Consumer Protection: The Practical Effectiveness of State Deceptive Practices Legislation*, 59 Tul. L. Rev. 427 (1984).

¹²² Alabama, Alaska, Georgia, Idaho, Maryland, Mississippi, New Hampshire, Pennsylvania, Rhode Island, and Tennessee.

enumerates 12 (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.¹²³

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.¹²⁴ Variation in the substantive provisions of 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.”¹²⁵ 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.¹²⁶ 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.¹²⁷ 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, in fact, require that private litigants meet a “public interest” standard, as required under the FTC Act.¹²⁸ States also vary in terms of whether

¹²³ 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.

¹²⁴ See generally Jonathan Sheldon and Carolyn L. Carter, *Unfair and Deceptive Acts and Practices* (National Consumer Law Center, 4th ed. 1997, 2000 cumulative supplement).

¹²⁵ See Edmund W. Kitch and Harvey S. Perlman, *Intellectual Property and Unfair Competition* 144 (5th ed. 1998).

¹²⁶ 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.”)

¹²⁷ See UTPCPL, § 3.

¹²⁸ Of the 42 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 Leaffer & 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).

they follow the pre or post-*Cliffdale Associates* test¹²⁹ for deception. State laws also vary in terms of remedies, 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 may inhibit some forms of innovation. Due to the relative ease of hauling Internet businesses into court in just about any state,¹³⁰ 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.¹³¹ The first generation of Internet advertising utilized banner advertisements. Such advertisements could be delivered to web surfers visiting a particular website. Early efforts to customize advertising delivery mimicked traditional media advertising by using relatively crude sampling techniques to map demographic characteristics.¹³² 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 2000.¹³³ During this time, online advertisers developed more sophisticated techniques for customizing advertisements, such as 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

¹²⁹ 103 F.T.C. 110 (1984). See supra n. ___ <discussing evolution of federal "deception" standard>.

¹³⁰ See supra n. ___ <footnote citing articles relating to Internet jurisdiction>

¹³¹ See Doubleclick, *The Decade in Online Advertising 1994-2004* (Apr. 2005) <http://www.doubleclick.com/us/knowledge_central/documents/RESEARCH/dc_decaderinonline_0504.pdf>

¹³² See Advertising as a science, CNET News.com (Oct. 4, 1996) (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 .5 percent to .75 percent response rate)

<http://news.com.com/Advertising+as+a+science/2100-1001_3-235158.html>

¹³³ See DoubleClick, supra n. ___, at 4.

that can be used to track surfing activity).¹³⁴ They also used response information to tie advertising pricing to various measures of performance, such as click through rates and revenues attributable to online advertisements.¹³⁵

Web advertising lost some of its luster in the late 1990s, with revenues leveling and then declining as the dot com bubble burst.¹³⁶ In addition, some of the more aggressive modes of online advertising, such as e-mail spam, came to be seen 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 offline information databases to develop detailed consumer profiles.¹³⁷ In response to pressure from privacy organizations, the Federal Trade Commission, and members of Congress, DoubleClick scaled back its plans and instituted a privacy policy and review board.¹³⁸

Behavioral marketing took root in the wake of these events. In 1999, The Gator

¹³⁴ See Ads find strength in numbers, CNET News.com (Nov. 4, 1996) <http://news.com.com/Ads+find+strength+in+numbers/2009-1001_3-243757.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>; 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>; 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>; In re DoubleClick Inc. Privacy Litigation, 154 F.Supp.2d 497, 502-06 (S.D.N.Y. Mar 28, 2001) (describing DoubleClick's "Dynamic Advertising Reporting & Targeting" (DART) technology).

¹³⁵ 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>

¹³⁶ See DoubleClick, supra n. __, at 4.

¹³⁷ See 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>; In re DoubleClick Inc. Privacy Litigation, 154 F.Supp.2d 497 (S.D.N.Y. Mar 28, 2001).

¹³⁸ 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>; 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>; 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>

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 advertisements delivered by the website that a consumer was visiting. With venture capital backing from Garage.com and founders of Sun Microsystems, Symantec, and Intuit,¹³⁹ 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 of such products consenting to receive contextual advertising.¹⁴⁰ Gator earned revenue principally from advertisers who purchase advertisements on its contextual advertising platform. This system enables 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 entering agreements with emerging peer-to-peer distributors to bundle Gator software with downloads of peer-to-peer software.¹⁴¹

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, FTC.com, NetFlix, Orbitz, Priceline, Sun Microsystems, Target, Verizon DSL, and Target.¹⁴² Gator was also able to serve as a conduit for Overture, an online advertising company that charges clients on a "cost-per-click" basis.¹⁴³ 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 and poached visitors to their websites.¹⁴⁴ Consumers and privacy organizations also became

¹³⁹ See Brian McWilliams, Gator Branded A Trojan Horse Despite Security, Newsbytes Mar. 7, 2002) <<http://www.newsbytes.com/news/02/175046.html>>; reproduced at <<http://seclists.org/lists/isn/2002/Mar/0045.html>>

¹⁴⁰ See Corporate Overview, Claria Corp. web site <<http://www.claria.com/companyinfo/>>

¹⁴¹ In 2003, Gator paid \$19.3 million on such distribution agreements, approximately 43 cents per active user. See Sharon Wienbar, The Spyware Inferno, News.com (Aug. 13, 2004) <http://news.com.com/The+spyware+inferno/2100-1032_3-5307831.html>; FTC Spyware Report at p.5.

¹⁴² See Benjamin Edelman, Documentation of Gator Advertising and Targeting <<http://cyber.law.harvard.edu/people/edelman/ads/gator/gator-customers.html>>; PC Pitstop, Gator's Advertisers <<http://www.pcpitstop.com/gator/advertisers.asp>>.

¹⁴³ See Wienbar, supra n. __. 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>

¹⁴⁴ 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) (noting that Gator's software "might display a Federal Express ad to people viewing UPS.com").

concerned about the means by which adware was being loaded onto their computers and the difficulty of removing it.¹⁴⁵

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.¹⁴⁶ 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. The first wave of litigation has been brought by web publishers who have sought 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 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.¹⁴⁷ 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.¹⁴⁸ WhenU was sued in Michigan, New York, Utah, and

<http://news.com.com/UPS+sues+Gator+for+wrongful+delivery/2100-1023_3-960535.html >

¹⁴⁵ See Center for Democracy and Technology, 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, BusinessWeek (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_3-877568.html

¹⁴⁶ 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>;

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>

¹⁴⁷ See

¹⁴⁸ Hertz Corp. v. The Gator Corp., Civ. No. 03-444 (D. N.J. 200_); United Parcel Service of Am. v. The Gator Corp., Case No. 1:02-CV-2639-BBM (N.D. Ga. Sept. 26, 2002);

Virginia.¹⁴⁹ 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.

i. California

California's unfair competition regime is set forth rather tersely in its Business & Professions Code: "unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising. . . ."¹⁵⁰ This provision can be traced back to a 1930's enactment inspired by the enlargement of the Federal Trade Commission's regulatory jurisdiction to include unfair business practices that harmed not merely the interests of business competitors but also those of the general public.¹⁵¹ As such, 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,¹⁵² the statute affords only injunctive relief (including restitution where monies have been paid) but does not

The Gator Corp. v. Extended Stay America, Case No. C-02-5226- CRB (N.D. Cal. Oct. 29, 2002); Six Continents Hotels v. The Gator Corp., Case No. 1:02-CV- 3065-JOF (N.D. Ga. Nov. 12, 2002); Extended Stay Am., Inc. v. The Gator Corp., Case no. 7:02- 3845-20 (D.S.C. Nov. 14, 2002); Lendingtree, Inc. v. The Gator Corp., Case No.3:02-CV-519-V (W.D.N.C. Dec. 11, 2002); The Gator Corp. v. PriceGrabber, Inc., Case No. C-02-5875-BZ (N.D. Cal. Dec. 16, 2002); The Gator Corp. v. TigerDirect, Inc., Case No. C-02-5875-BZ (Dec. 19, 2002); Tigerdirect, Inc. v. The Gator Corp., Case No. C-02-23615 (S.D. Fla. Dec. 20, 2002); Washington Post.Newsweek Interactive Co., v. The Gator Corp., Case. No. CV 02-909-A (E.D. Va. June 25, 2002). <<http://lawlibrary.rutgers.edu/fed/html/ca03-444-1.html#Footnote1>> The Hertz Corp. lawsuit brought in New Jersey does not allege violations of any state deception or unfair competition statutes.

¹⁴⁹ Overstock.com v. WhenU.com, Case No. 2:03-CV-00570 (D. Ut. Jun. 25, 2003); Louis Vuitton Malletier v WhenU.com, Case No. 1:05-CV-01325 (S.D.N.Y. Feb. 3, 2005); Louis Vuitton Malletier v WhenU.com, Case No. 1:04-CV-03249 (S.D.N.Y. Apr. 28, 2004); U-Haul Int'l v. WhenU, Case No. 1:02-CV-01469 (E.D. Va. Oct. 2, 2002); 1-800-Contacts, Inc. v. WhenU.com, Case No. 1:03-CV-09043 (S.D.N.Y. Nov. 7, 2003); Vision Direct, Inc. v. WhenU.com, Case No. 1:02-CV-09788 (S.D.N.Y. Dec. 11, 2002); Tiger Direct, Inc. v. WhenU.com, Case No. 1:02-CV-23306 (S.D. Fla.. Nov. 12, 2002); Wells Fargo Co. v. WhenU.com, Case No. 2:03-CV-71906 (E.D. Mich. May 16, 2003).

¹⁵⁰ Cal. Bus. & Profs. Code §17200, et seq.

¹⁵¹ See *Gregory v. Albertson's, Inc.*, 104 Cal. App. 4th 845, 128 Cal. Rptr. 2d 389 (1st Dist. 2002).

¹⁵² See Cal. Bus. & Profs. Code §17204; see also *Gregory v. Albertson's, Inc.*, 104 Cal. App. 4th 845, 128 Cal. Rptr. 2d 389 (1st Dist. 2002).

authorize the award of civil damages.¹⁵³

California's unfair competition regime prohibits "any unlawful, unfair, or fraudulent business act or practice." 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.¹⁵⁴ As such, the unfairness standard is quite broad, thus 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.¹⁵⁵

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 could possibly have broader reach based on somewhat different legal standards. At a minimum, the California regime creates some added uncertainty regarding the boundaries of liability.

ii. Florida

Florida has both statutory and common law restraints on unfair competition. Florida's Deceptive and Unfair Trade Practices Act (FDUTPA),¹⁵⁶ enacted in 1973, follows Alternative Form #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."¹⁵⁷ 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."¹⁵⁸ Although court decisions frequently applied the FTC's pre-1983 standards for determining what

¹⁵³ See Cal. Bus. & Profs. Code §17203. Cf. *People v. Thomas Shelton Powers, M.D., Inc.*, 2 Cal. App. 4th 330 (1992) (ordering disgorgement of profits under 17200); but see *Kraus v. Trinity Management Services, Inc.*, 23 Cal. 4th 116, 137-38 (2000) (overruling disgorgement in *People v. Thomas Shelton Powers, M.D., Inc.*, in part). Public enforcers, however, may recover civil damages. Cal. Bus. & Profs. Code §§17206, 17206-1. A successful plaintiff may seek attorney fees where the action has been brought as a "private attorney general" action. See Cal. Code of Civil Procedure §1021.5.

¹⁵⁴ *Gregory v. Albertson's, Inc.*, 104 Cal. App. 4th 845, 128 Cal. Rptr. 2d 389 (1st Dist. 2002).

¹⁵⁵ See *People ex rel. Bill Lockyer v. Fremont Life Ins. Co.*, 104 Cal. App. 4th 508, 128 Cal. Rptr. 2d 463 (2d Dist. 2002), *opinion modified on denial of reh'g*, *People ex rel. Lockyer v. Fremont Life Ins. Co.*, 105 Cal. App. 4th 270, 2003 WL 125447 (2d Dist. 2003).

¹⁵⁶ See § 501.201, et seq.

¹⁵⁷ FDUTPA § 501.204.

¹⁵⁸ *Id.* at

constitutes an “unfair” or “deceptive” trade practice, more recent decision take into consideration the modern interpretations of these terms by the FTC.¹⁵⁹ The Florida statute confers broad standing upon “anyone aggrieved by a violation” of the Act, extending to consumers and competitors.¹⁶⁰ 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.¹⁶¹ 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.¹⁶²

iii. 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 enjoy a wide range of deceptive practices.¹⁶³ A separate statute prohibits false advertising.¹⁶⁴ Georgia’s Unfair Competition Act,¹⁶⁵ dating back well over a century, prohibits the tort of passing off.¹⁶⁶ Federal courts have

¹⁵⁹ See David J. Federbush, Obtaining Relief for Deceptive Practices Under FDUTPA, 75 Fla. Bar Journal 22 (November 2001); David J. Federbush, The Unexplored Territory of Unfairness in Florida’s Deceptive and Unfair Trade Practices, 73 Fla. Bar Journal 26 (May 1999).

¹⁶⁰ See generally David J. Federbush, Obtaining Relief for Deceptive Practices Under FDUTPA, 75 Fla. Bar Journal 22 (November 2001).

¹⁶¹ FDUTPA § 501.211.

¹⁶² See *Investacorp, Inc. v. Arabian Inv. Banking Corp. (Investcorp) E.C.*, 931 F.2d 1519, 521 (11th Cir. 1991); *Gift of Learning Foundation, Inc. v. TGC, Inc.*, 329 F.3d 792, (11th Cir. 2003); *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 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 Southern Bank v. First Southern Bank*, 625 So.2d 463 (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.)”).

¹⁶³ See Deceptive Trade Practices Act O.C.G.A. § 10-1-370 et seq.

¹⁶⁴ See O.C.G.A. § 10-1-420-27.

¹⁶⁵ See O.C.G.A. §23-2-55.

held that the substantive standards of liability under § 23-2-55 “mirror” the standards of liability applicable under the Lanham Act.¹⁶⁷ The Fair Business Practices Act (FBPA),¹⁶⁸ enacted in 1975, combines Alternative Forms #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,”¹⁶⁹ and therefore denies standing to competitors.¹⁷⁰ Georgia’s common law of unfair competition, although evolving beyond pre-*Erie* jurisprudential restraints,¹⁷¹ does not appear to reach beyond the modern 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.¹⁷²

iv. Michigan

Michigan protects consumers and competitors against unfair competition under its Consumer Protection Act (MCPA),¹⁷³ 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 (such as 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).¹⁷⁴ The MCPA does, however, incorporate the FTC Act’s standards by authorizing

¹⁶⁶ See *Sofate of America, Inc. v. Brown*, 171 Ga.App. 39, 318 S.E.2d 771 (1984).

¹⁶⁷ See *University of Georgia Athletic Ass’n v. Laite*, 756 F.2d 1525, 1539 n.11 (11th Cir. 1985) (observing that standards under §23-2-55 “are similar, if not identical to those under the Lanham Act”).

¹⁶⁸ See OGCA § 10-1-390 et seq.

¹⁶⁹ OGCA § 10-1-___ (emphasis added).

¹⁷⁰ See *Friedlander v. PDK Labs, Inc.*, 266 Ga. 180, 465 S.E.2d 670 (Ga. S. Ct.1996).

¹⁷¹ See *Kay Jewelry Co. v. v. Kapiloff*, 204 Ga. 209, 49 S.E.2d 19, 81 U.S.P.Q. 293 (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 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.”)

¹⁷² 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”).

¹⁷³ MCPA § 445.901, et seq.

¹⁷⁴ MCPA § 445.903. 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 Michigan Consumer Protection Act, is the same confusion as to source standard applicable to trademark violations under the Lanham Act. See *Microsoft*

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.¹⁷⁵ Although initially focused on consumer harm,¹⁷⁶ recent decisions have expanded standing under the MCPA to include competitors.¹⁷⁷

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.¹⁷⁸ 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.¹⁷⁹ 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.¹⁸⁰ Thus, Michigan courts have followed the general law of unfair competition.¹⁸¹

Corp. v. Compusource Distributors, Inc., 115 F. Supp.2d 800 (E.D. Mich.2000); Schreiber Mfg. Co. v. Saft America, 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).

¹⁷⁵ MCPA § 445.911(b)(3)(c).

¹⁷⁶ See *Noggles v. Battle Creek Wrecking, Inc.*, 153 Mich.App. 363, 367, 395 N.W.2d 322, 324 (1986); *Wynn Oil Co. v. American Way Service 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). 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).

¹⁷⁷ See *Action Auto Glass v. Auto Glass Specialists*, 134 F.Supp.2d 897 (W.D. Mich.2001); *Florists' Transworld Delivery, Inc. v. Fleurop-Interflora*, 261 F.Supp.2d 837, 848 (E.D. Mich. 2003); *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 personal, family, or household purposes"; but see *Cosmetic Dermatology and Vein Centers of Downriver, P.C. v. New Faces Skin Care Centers, 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").

¹⁷⁸ See *Clairol, Inc. v. Boston Discount Center of Berkley, Inc.*, 608 F.2d 1114, 118 (6th Cir. 1979).

¹⁷⁹ See *James Heddon's Sons v. Millsite Steel & Wire Works*, 128 F.2d 6 (6th Cir. 1942); *Moon Bros. v. Moon*, 300 Mich. 150, 1 N.W.2d 488 (1942); *Carbonated Beverages v. Wisko*, 297 Mich. 80, 297 N.W. 79 (1941); *Schwannecke v. Genesee Coal & Ice Co.*, 262 Mich. 624, 247 N.W. 761 (1933).

¹⁸⁰ See *Williams v. Farrand*, 88 Mich. 473, 50 N.W. 446 (1891); *James Heddon's Sons v.*

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 confusion¹⁸² and has languished in 1930s era constraints.¹⁸³ 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.

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 produce different conclusions.

v. North Carolina

The North Carolina Unfair Trade Practices Act (NCUTPA),¹⁸⁴ enacted in 1969, adopts Alternative #1 of the FTC's proposed Unfair Trade Practices and Consumer Protection. It does not expressly tie interpretation of its terms to interpretations given by the Federal Trade Commission, although courts have borrowed the expansive definition of "deception" that the federal courts have traditionally employed in interpreting the FTC Act.¹⁸⁵ The statute expressly provides for a broad private right of action extending to both consumers and businesses (including competitors).¹⁸⁶ It also affords victorious plaintiffs treble damages.¹⁸⁷ Courts may, in

Millsite Steel & Wire Works, 128 F.2d 6 (C.C.A. 6th Cir. 1942); Carbonated Beverages v. Wisko, 297 Mich. 80, 297 N.W. 79 (1941).

¹⁸¹ See A & M Records, Inc. v. MVC Distributing 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).

¹⁸² See generally 54A Am. Jur. 2d, Monopolies, Restraints of Trade and Unfair Trade Practices, § 1107 et seq., pp. 361-384; see also In re MCI Telecommunications Corp. Complaint, 612 N.W.2d 826 (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").

¹⁸³ See, e.g., Burns v. Schotz, 343 Mich. 153, 72 N.W.2d 149 (1955); Good Housekeeping Shop v. Smither, 254 Mich. 592, 236 N.W. 872 (1931); but cf. Boron Oil Co. v. Callanan, 50 Mich. App. 580, 213 N.W.2d 836 (1973) (loosening the competition requirement).

¹⁸⁴ See N.C.G.S. § 75-1.1, et seq.

¹⁸⁵ See Hageman v. Twin City Chrysler-Plymouth Inc., 681 F. Supp. 3030 (M.D.N.C. 1988); cf. State ex rel. Edmisten v. J.C. Penney Co., 292 N.C. 311, 233 S.E.2d 895 (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); Eastern Roofing & Aluminum Co. v. Brock, 70 N.C. App. 431, 320 S.E.2d 22 (1984) (same)

¹⁸⁶ See Harrington Mfg. Co. v. Powell Mfg. Co., 38 N.C. App. 393, 248 S.E.2d 739 (1978) (holding that the statute applies to disputes between competitors, and not only to dealings between buyers and sellers), *cert. denied*, 296 N.C. 411, 251 S.E.2d 469 (1979); McDonald v. Scarborough, 91 N.C. App. 13, 370 S.E.2d 680, *cert. denied*, 323 N.C. 476, 373 S.E.2d 864 (1988).

¹⁸⁷ See N.C.G.S. § 75-16. See generally Robert Morgan. "The People's Advocate in the Marketplace -- The Role of North Carolina's Attorney General in the Field of Consumer

their discretion, award attorney fees.¹⁸⁸

The statute was enacted to provide a private cause of action for aggrieved consumers with recognition that common law remedies were ineffective.¹⁸⁹ 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”¹⁹⁰ 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 offends established public policy as well as when the practice is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.¹⁹¹

Litigation under North Carolina’s UTPA statute involving competitors has been particularly brisk.¹⁹² In *Polo Fashions, Inc. v. Craftex, Inc.*,¹⁹³ 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. §111 requires the statutory notice or registration before damages are permitted, damages were available (and trebled) under the state statute.¹⁹⁴ Thus, the North Carolina unfair competition statute may well impose broader liability than federal law.

vi. South Carolina

The South Carolina Unfair Trade Practices Act (SCUPTA) was initially enacted in 1962 and was amended in 1972 in light of the FTC proposed act.¹⁹⁵ In its amended form, the SCUPTA adopts Alternative #1 of the FTC’s proposal, but provides a much more open-ended standing. Under the Act, “[a]ny person who suffers any ascertainable loss of money or

Protection” 6 Wake Forest Intramural L. Rev. 1, 20 (1969).

¹⁸⁸ See N.C.G.S. § 75-16.1; *Canady v. Crestar Mtg. Corp.*, 109 F.3d 969 (4th Cir. 1997).

¹⁸⁹ See *Bhatti v. Buckland*, 328 N.C. 240, 400 S.E.2d 440 (1991).

¹⁹⁰ See *Cash v. State Farm Mutual Auto. Ins. Co.*, 137 N.C.App. 192, 197, 528 S.E.2d 372, 375 (N.C.Ct.App. 2000).

¹⁹¹ See *Huff v. Autos Unlimited, Inc.*, 477 S.E.2d 86, 124 N.C.App. 410 (1996), *writ denied, review denied*, 487 S.E.2d 546, 346 N.C. 279.

¹⁹² See Edmund W. Kitch and Harvey S. Perlman, *Intellectual Property and Unfair Competition* 153 (5th ed. 1998).

¹⁹³ 816 F.2d 145 (4th Cir. 1987).

¹⁹⁴ But see *Sideshow, Inc. v. Mammoth Records, Inc.*, 751 F.Supp. 78 (E.D.N.C. 1990) (limiting *Polo Fashions* to intentional infringement and holding 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”).

¹⁹⁵ See S.C. Code § 39-5-10 et seq.

property,”¹⁹⁶ not merely consumers purchasing for personal use, may bring a private action under this statute. Thus, competitors have standing under this statute.¹⁹⁷ 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,¹⁹⁸ although only the Attorney General may obtain injunctive relief under the statute.¹⁹⁹

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 result 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.²⁰⁰ 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),”²⁰¹ 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.²⁰² An act is “unfair” when it is offensive to public policy or when it is immoral, unethical, or oppressive.²⁰³ 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.²⁰⁴ 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.²⁰⁵

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.²⁰⁶ Second, as noted above, the

¹⁹⁶ S.C. Code § 39-5-140.

¹⁹⁷ See *Global Protection Corp. v. Halbersberg*, 332 S.C. 149, 503 S.E.2d 483 (S.C. App. 1998).

¹⁹⁸ S.C. Code § 39-5-140.

¹⁹⁹ S.C. Code § 39-5-50.

²⁰⁰ See *Havird Oil Co., Inc. v. Marathon Oil Co., Inc.*, 149 F.3d 283 (4th Cir. 1998).

²⁰¹ S.C. Code § 39-5-20(b).

²⁰² See *Johnson v. Collins Entertainment Co., Inc.*, 349 S.C. 613, 564 S.E.2d 653 (S.C. 2002); *Williams- Garrett v. Murphy*, 106 F. Supp. 2d 834 (D.S.C. 2000).

²⁰³ See *id.*

²⁰⁴ See *Daisy Outdoor Advertising Company, Inc., v. Abbott*, 322 S.C. 489, 473 S.E.2d 47 (S.C. S. Ct. 1996); *Noack Enters., Inc. v. Country Corner Interiors*, 290 S.C. 475, 351 S.E.2d 347 (Ct.App.1986), *cert. dismissed*, 294 S.C. 235, 363 S.E.2d 688 (1987).

²⁰⁵ See *Liberty Mut. Ins. Co. v. Employee Resource Management, Inc.*, 176 F.Supp.2d 510 (D.S.C. 2001).

²⁰⁶ See *State ex rel. Medlock v. Nest Egg Soc. Today, Inc.*, 290 S.C. 124, 348 S. E. 2d

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*²⁰⁷ involved two fiercely 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 the 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.²⁰⁸ "For Sale" signs were exempted from the state statute regulating placement of billboards.²⁰⁹ 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 "public interest" requirement, applying a more stringent standard.²¹⁰ The South Carolina Supreme Court reversed, reinstating the trial court's decision.²¹¹

iii. State Legislative Spyware 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.

Chart I

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 adware software removal), restrictions on specific practices (e.g., 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,

381 (Ct. App. 1986) (A "willful" violation occurs when the party committing the violation knew or should have known that his conduct violated the Act.)

²⁰⁷ 322 S.C. 489, 473 S.E.2d 47 (S.C. S. Ct. 1996).

²⁰⁸ 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.

²⁰⁹ See § 57-25-40(A)(5) and (D).

²¹⁰ 317 S.C. 14, 451 S.E.2d 394 (S.C. App. 1994).

²¹¹ 322 S.C. 489, 473 S.E.2d 47 (S.C. S. Ct. 1996).

Chart I

Survey State Spyware Legislation*		
State	Status	Summary
Alabama	pending	<p>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.</p> <p>Enforcement: Public Remedies: criminal penalties (Class B misdemeanor)</p>
Alaska	Sent to Governor (as of 5/10/05)	<p>S.B. 140 “An Act relating to spyware and unsolicited advertising” Prohibits certain pop-up 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. Exempts from liability distributors of software or services that remove spyware.</p> <p>Enforcement: Private right of action under existing unfair business practices statute.</p>
Arizona	Enacted (4/18/05)	<p>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.</p> <p>Enforcement: Attorney General; a computer software provider or a web site or trademark owner who is adversely affected Remedies: Injunctive relief; greater of actual damages or one hundred thousand dollars for each separate violation; treble damages for repeat violators; costs and attorney fees</p>

Survey State Spyware Legislation*		
State	Status	Summary
Arkansas	Enacted (4/13/05)	<p>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.</p> <p>Enforcement: by Attorney General under Deceptive Trade Practices Act.</p> <p>Remedies: Fines to be paid to “Spyware Monitoring Fund,” which shall be used for enforcement and related expenses.</p>
	Enacted (4/14/05)	<p>H.B. 2261; Act 2312 “An act to make an appropriation for expenses associated with spyware monitoring for the office of Attorney General”</p> <p>H.B. 2344; Act 2313 “An act to make an appropriation for expenses associated with spyware monitoring for the Department of Information Systems”</p>
California	Enacted (9/28/04)	<p>“Consumer Protection Against Computer Spyware Act”(Chapter 32 (§22947 et seq.); Division 8 of the Business and Professions Code)</p> <p>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.</p> <p>Enforcement: leaves open who may enforce prohibitions</p> <p>Remedies: unstated</p>
	pending	<p>S.B. 92 provides for enforcement and remedies for the “Consumer Protection Against Computer Spyware Act”</p> <p>Enforcement: establishes a private right of action for recipients of spyware; and public</p> <p>Remedies: allows parties to recover liquidated damages of \$1,000 per violation, attorney’s fees, and costs; makes violation the prohibitions a crime, punishable as either a misdemeanor or felony.</p>

Survey State Spyware Legislation*		
State	Status	Summary
	pending	S.B. 355 states that a purpose of the “Consumer Protection Against Computer Spyware Act” is to improve security on the Internet
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 on-line business; prohibiting 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; prohibiting 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; and 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; and 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*

State	Status	Summary
Illinois	Passed House (2/8/05)	<p>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)</p>
Indiana	pending	<p>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 a method of uninstalling the spyware. Authorizes a web site 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</p>

Survey State Spyware Legislation*

State	Status	Summary
Iowa	Enacted (5/3/05)	<p>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 web site 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</p>
Kansas	pending	<p>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)</p>
Maryland	Legislature adjourned (4/11/05)	<p>S.B.492, S.B.801, H.B.945, H.B.780 “Unauthorized Computer Software Act” Prohibiting specified persons from causing computer software 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 to be copied onto a consumer’s computer under specified circumstances; prohibiting 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</p>

Survey State Spyware Legislation*		
State	Status	Summary
Massachusetts	pending	<p>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), and 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 for each separate violation; treble damages for willful violation; attorney's fees and costs</p>
	pending	<p>S.B. 286 "Regulation of Unconsented Internet Advertising" Prohibits installing spyware or context-based triggering mechanisms to display advertisements that obscure a web page absent express consent and uninstall directions. Enforcement: Remedies: escalating fine (\$500 for the first violation, \$1,000 for a second violation, and \$5,000 for a third and any subsequent violations).</p>
	pending	<p>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</p>

Survey State Spyware Legislation*		
State	Status	Summary
Michigan	Passed Senate (3/9/05)	<p>S.B. 151 "Spyware Control Act"</p> <p>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.</p> <p>Enforcement: public (attorney general) and 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.</p> <p>Remedies: injunctive relief; greater of actual damages or \$10,000 per violation; treble damages for pattern of violation..</p>
	Passed Senate (3/9/05)	<p>S.B. 54, S.B. 53</p> <p>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.</p> <p>Enforcement: public</p> <p>Remedies: criminal penalties (misdemeanor and felony); sentencing guidelines for the crime of installing spyware on another person's computer without consent (S.B. 53).</p>
Missouri	pending	<p>H.B. 902 "Consumer Protection Against Computer Spyware Act"</p> <p>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.</p> <p>Enforcement: public (attorney general)</p> <p>Remedies:</p>

Survey State Spyware Legislation*		
State	Status	Summary
Nebraska	pending	<p>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.</p> <p>Enforcement: public Remedies: criminal (misdemeanor)</p>
New Hampshire	Passed House (2/23/05)	<p>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 use the program or spyware to, 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; and (5) induce violation of the Act.</p> <p>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)</p>

Survey State Spyware Legislation*		
State	Status	Summary
New York	pending	<p>A.B. 549 "Unlawful Use of Spyware and Malware"; see also A.B. 2682</p> <p>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 use the program or spyware to, 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.</p> <p>Enforcement: Public</p> <p>Remedies: Criminal (class A misdemeanor; class E felony for repeat offenders (within 5 years of prior conviction)</p>
Oregon	pending	<p>H.B. 2302</p> <p>Prohibits a person from installing or causing installation of spyware on a computer absent clear notice as specified in the statute and informed consent.</p> <p>Enforcement: public (attorney general)</p> <p>Remedies: unlawful trade practice</p>
Pennsylvania	pending	<p>H.B. 574</p> <p>Prohibits provision of adware or spyware without specified notice and consent.</p> <p>Enforcement: public</p> <p>Remedies: criminal</p>

Survey State Spyware Legislation*

State	Status	Summary
Rhode Island	Pending	<p>H.B. 6211 "Software Fraud"</p> <p>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 use the program or spyware to, 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.</p> <p>Enforcement: public (attorney general); and private right of action by aggrieved person</p> <p>Remedies: greater of actual damages and \$1,000 per violation; treble damages for pattern of violations; attorney's fees and costs</p>
Tennessee	pending	<p>H.B. 1742, S.B. 2069 "Internet Spyware Control Act of 2005"</p> <p>Prohibits installation of spyware or adware (triggered by use of a trademark of another) without computer user's informed consent.</p> <p>Enforcement: private right of action by website owner or registrant, trademark or copyright owner, or authorized website advertiser.</p> <p>Remedies: injunction; greater of actual damages and \$10,000 per violation; treble damages for willful violation; attorney's fees and costs</p>
Texas	Passed House (4/26/05)	<p>H.B. 1430, S.B. 958 "Consumer Protection Against Spyware Act"</p> <p>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.</p> <p>Enforcement: public (attorney general); private right of action by a provider of computer software, owner of a web page, or trademark owner who is adversely affected</p> <p>Remedies: injunction; greater of actual damages and \$100,000 per violation; treble damages for pattern of violations; attorney's fees and costs</p>

Survey State Spyware Legislation*		
State	Status	Summary
Utah	pending	<p>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</p>
Utah	Enacted (3/17/05)	<p>H.B. 104 amends "Spyware Control Act" Prohibits display of pop-up 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 user's state of residence prior to sending spyware or pop-up 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 and \$500 per violation; treble damages for willful and knowing violation; attorney's fees and costs</p>
Utah	Enacted (3/23/04) Enjoined by 3rd Judicial District Court (6/22/04)	<p>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 and \$10,000 per violation; treble damages for willful violation; attorney's fees and costs</p>

Survey State Spyware Legislation*

State	Status	Summary
Virginia	Passed House (2/4/05)	<p>H.B. 1729 amends "Computer Crimes Act" 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.</p> <p>Enforcement: public Remedies: criminal (Class 1 misdemeanor)</p>
	Enacted (4/4/05)	<p>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.</p> <p>Enforcement: public Remedies: criminal (Class 1 misdemeanor)</p>
Washington	Enacted (5/17/05)	<p>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.</p> <p>Enforcement: public (attorney general); private right of action by a provider of computer software or owner of a web site or trademark who is adversely affected. Remedies: injunction; greater of actual damages and \$100,000 per violation; attorney's fees and costs; liability cap of \$2,000,000.</p>

Survey State Spyware Legislation*

State	Status	Summary
West Virginia	pending	<p>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) - shall be fined not more than \$500,000 or confined in jail for not more than six months, or both</p>
<p>* Sources: National Conference of State Legislatures, 2005 State Legislation Relating to Internet Spyware or Adware (updated as of May 17, 2005) <http://www.ncsl.org/programs/its/spyware05.htm>; Ben Edelman, State Spyware Legislation <http://www.benedelman.org/spyware/legislation/>; state legislation websites</p>		

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 lobbied for strong notice, consent, and removal requirements.²¹² 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 Net.²¹³ Many of the pending bills (Alabama, Arizona, Arkansas, California, 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 Utah, have favored stronger regulation.

Utah became the first state to enact spyware legislation in March 2004.²¹⁴ 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. Within days of passage, 1-800-Contacts brought suit against Coastal Contacts, a competitor that sponsored advertisements on WhenU.com's advertising platform targeting 1-800-Contacts' website.²¹⁵ Shortly thereafter,

²¹² See "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," Red Herring (Sept. 17, 2004)

<<http://www.redherring.com/article.aspx?a=10859&hed=Should+spyware+be+a+crime?>>; 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>>; Memorandum in Support of Plaintiff WhenU.com Inc.'s Application for a Temporary Restraining Order and Motion for Preliminary Injunction at 7, n.6 (Apr. 12, 2004) (noting lobbying efforts by 1-800 Contacts) <http://www.benedelman.org/spyware/whenu-utah/whenu-memo-tro_pi.pdf>; John Borland, States join spyware battle, CNet New.com (Mar. 4, 2004) <http://news.com.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>>.

²¹³ See Stefanie Olsen, Utah judge freezes anti-spyware law, CNet New.com (Jun. 22, 2004) <http://news.com.com/Utah+judge+freezes+anti-spyware+law/2100-1024_3-5244151.html>.

²¹⁴ See Utah Spyware Control Act, H.B. 323; Brice Wallace, Spyware Act has detractors, Deseret Morning News (Mar. 19, 2004) <<http://deseretnews.com/dn/print/1,1442,595050017,00.html>>

²¹⁵ See Draper firm files lawsuit over pop-up ads, Deseret Morning News (Mar. 19, 2004) <<http://deseretnews.com/dn/print/1,1442,595050012,00.html>> A second Utah retailer, Overstock.com, 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 in May 2004. This lawsuit also alleged common law causes of action based on unfair competition and interference with prospective economic advantage. See Janis Mara and Ron Miller, Lawsuit

WhenU.com brought an action seeking to have the legislation declared invalid under the Commerce Clause. In June 2004, the state court granted a preliminary injunction blocking the Act from taking effect.²¹⁶

In March 2005, Utah amended its Spyware Control Act in an attempt to circumvent the Commerce Clause bar.²¹⁷ 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 of the 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 faced.²¹⁹ The range of states in which these cases were brought supports the nationwide exposure that Internet-based businesses face under

Filed Under Utah's Challenged Anti-Spyware Act: Massachusetts based companies fighting it out in Utah, Internet News (May 19, 2004) <internetnews.com/ec-news/article.php/3356441>.

²¹⁶ See Stefanie Olsen, Utah judge freezes anti-spyware law, CNET News.com (Jun. 22, 2004) <http://news.com.com/Utah+judge+freezes+anti-spyware+law/2100-1024_3-5244151.html>

²¹⁷ See H.B. 104 (2005), <<http://www.le.state.ut.us/~2005/bills/hbillenr/hb0104.htm>>;

²¹⁹ 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>

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' 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. Thus, 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 preempted.

III. Federal Spyware Initiatives and Federalism Implications

The rapidity with which the Internet evolves creates unprecedented challenges for already overworked deliberative bodies like legislatures and courts. 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 that the protection of copyrighted works in the digital environment,²²⁰ 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 (Federal Trade Commission) and the federal legislature to address the public policy concerns raised by spyware? Furthermore, do these reasons override the advantages of national uniformity and coordinated policy development? This section reviews the actions of the Federal Trade Commission 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.

²²⁰ See S. Rep. No. 105-190, at 8 (1988); see also H. Rep. No. 105-551, pt. 2 at 23 (1998).

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 14 cases relating to spyware.²²¹ 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. It promoted the software by sending consumers by exploiting a feature within Microsoft's Windows operating system that allows network administrators notify users about critical maintenance to bombard consumers with pop-up advertisements promoting its software.²²² 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.²²³

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.²²⁴ 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. Although some critics have complained that the FTC has not been sufficiently proactive in confronting the threats posed by spyware,²²⁵ the FTC's deliberative and cautious approach ensures that the broad

²²¹ See Federal Trade Commission, *Monitoring Software on your PC: Spyware, Adware, and Other Software* at p. 20 n. 204 (Staff Report) (Mar. 2005) <<http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf>>; 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/>>

²²² 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>

²²³ 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/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>>

²²⁴ See Federal Trade Commission, *Monitoring Software on your PC: Spyware, Adware, and Other Software* (Apr. 19, 2004) <http://www.ftc.gov/bcp/workshops/spyware/>

²²⁵ See Declan McCullagh, *Few Solutions Pop Up at FTC Adware Workshop*, C/Net News.com (Apr. 19, 2004)

range of considerations will be fully considered and provides an opportunity for non-regulatory solutions to emerge.²²⁶

B. Legislative Proposals

Spyware concerns captured the attention of federal legislators early 2004.²²⁷ Several bills have since been floated,²²⁸ with Representative Mary Bono's Securely Protect Yourself Against Cyber Trespass Act (SPY Act) garnering the most attention and support.²²⁹ The House of Representatives passed the SPY Act on May 23, 2005.²³⁰

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.²³¹ The Act prohibits collection of personal information without notice and consent, subject to various exceptions and limitations on liability for telecommunication entities.²³² The Act also delegates rulemaking authority to the Federal Trade Commission²³³ and vests the agency with enforcement powers.²³⁴

http://news.com.com/Few+solutions+pop+up+at+FTC+adware+workshop/2100-1028_3-5195222.html

²²⁶ See Declan McCullagh, FTC officials blast spyware measures, CNet News.com (Apr. 29, 2004) (noting FTC concerns that proposed laws could harm legitimate software products and innovation) <http://news.com.com/FTC+officials+blast+spyware+measures/2100-1023_3-5202016.html>; Declan McCullagh, Making the wrong move against spyware, CNET News.com (May 2, 2005) (advocating a cautious approach to spyware regulation and allowing enforcement under existing regulatory authority to proceed) <http://news.com.com/Making+the+wrong+move+against+spyware/2010-1071_3-5690270.html>

²²⁷ 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>

²²⁸ See Benjamin Edelman, "Spyware": Research, Testing, Legislation, and Suits <<http://www.benedelman.org/spyware/#legislation>>

²²⁹ See H.R. 29 (formerly H.R.2929)

²³⁰ Roy Mark, House Approves Anti-Spyware Bills, Internet News (May 23, 2005) <<http://www.internetnews.com/bus-news/article.php/3507211>>. An 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>>

²³¹ See SPY Act, §2.

²³² See SPY Act, §3.

²³³ See SPY Act, §§__,__.

Of most importance for 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

(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 in two respects. First, state regulators may well have resources and information that could compliment federal enforcement. Second, such a restrictive enforcement regime raises the concern that federal authorities could be prone to capture by interest groups opposing regulation. Third, centralized standard setting and enforcement ensures the most cohesive regulatory environment.

²³⁴ See SPY Act, §4.

Concluding Remarks

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 paper 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 argues 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 – common law or statutory – has this effect. Internet businesses can be haled into court in any state and therefore must consider legal risks in every state. The problem is compounded by the amorphous quality 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.²³⁵ 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 paper 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 advocating global regulatory solutions to Internet-related

²³⁵ 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 (N.D. Cal. 2000); Steven Kam, <BTLJ annual review note on trespass to chattels>. Thus, 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*, 3 J. Small & Emerging Bus. 1 (1998), but unlike with spyware, companies can limit their exposure to the rules of any state by computer code that they write.

activities,²³⁶ regulation of Internet activities in any one country can have effects beyond the borders of that particular nation.²³⁷ 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.²³⁸ 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.²³⁹

In some respects, however, nation-based regulation may provide some of the advantages of policy experimentation that Justice Brandeis endorsed. International jurisdiction 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 database protection,²⁴⁰ spyware,²⁴¹ and keyword advertising.²⁴² On the other hand, there is some risk that such experiments will have undesirable spillover effects and that nations may use differential constraints to serve protectionist goals.

²³⁶ See William J. Clinton & Albert Gore, Jr., A Framework for Global Electronic Commerce (1997), available at <http://www.ecommerce.gov/framework.htm> (discussing the need for a set of globally recognized commercial law rules); The Legal and Policy Framework for Global Electronic Commerce: A Progress Report, 14 Berkeley Tech. L.J. 503-886 (1999).

²³⁷ Cf. Joel R. Reidenberg, Yahoo and Democracy on the Internet, 42 Jurimetrics 261 (2002).

²³⁸ 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.J. 601 (1999); cf. A. Michael Froomkin, Of Governments and Governance, 14 Berkeley Tech. L.J. 617 (1999).

²³⁹ See Irwin Arieff, UN panel fails to agree on how to govern Internet, Reuters (Jul. 14, 2005) <http://today.reuters.com/news/NewsArticle.aspx?storyID=2005-07-14T221616Z_01_N14734082_RTRIDST_0_NET-TECH-INTERNET-UN-DC.XML>.

²⁴⁰ See Stephen M. Maurer, P. Bernt Hugenholtz & Harlan J. Onsrud, 'Europe's Database Experiment', Science, vol. 294 (26 October 2001), p. 789-790; James Boyle, A natural experiment, Financial Times (Nov. 22, 2004) <<http://news.ft.com/cms/s/4cd4941e-3cab-11d9-bb7b-00000e2511c8.html>>

²⁴¹ 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 Pushes \$10,000 Fine, AustralianIT (May 12, 2005) <<http://australianit.news.com.au/articles/0,7204,15262588%5E15331%5E%5Enbv%5E15306-15318,00.html>>

²⁴² See Nanterre Court (TGI), emergency order, Hotels Méridien v. Google France, December 16, 2004 <<http://www.juriscom.net/jpt/visu.php?ID=631>>

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) 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.