A Recipe for Cookies: State Regulation of Consumer Marketing Information

Bruce H. Kobayashi & Larry E. Ribstein*

George Mason University School of Law

February 15, 2001

* Prepared for delivery at the American Enterprise Institute, Federalism Project Roundtable on Internet Privacy, January 30, 2001. We thank Michael Greve, Eugene Volokh, two anonymous referees and Roundtable participants for valuable comments.

EXECUTIVE SUMMARY

The debate over the regulation of consumer marketing information so far has focused on what form any such regulation should take. Despite the lack of consensus on the basic framework for allocating rights to use consumer marketing information, there seems to be broad consensus that any regulation should be promulgated at the federal level. Privacy advocates have stressed uniform federal law as a solution to the potential for under-regulation by the states. Firms have advocated uniform federal law as a solution to the problems of over-regulation by some states and having to comply with multiple and inconsistent state laws.

This paper argues that the focus on a uniform federal solution is misguided. Given the lack of consensus on a basic framework for allocating rights in this area, it would be counterproductive to straightjacket emerging technologies and business practices with a federal law. Rather, consumer marketing information is best regulated at the state rather than the federal level. A process of state experimentation, competition and evolution would allow discovery of appropriate and comprehensive responses to problems concerning consumer marketing information, in contrast to the growing patchwork of federal laws that inhibit the development of such responses.

A state law approach will not lead to over- or under-regulation as some have predicted as long as merchants and consumers can contract for the applicable law and forum. Contractual choice of a jurisdiction that under-regulates privacy is constrained by market forces and by the political forces within that state. Enforcement of contractual choice of law and forum would allow firms and consumers to agree to the application of a particular state's law, thereby eliminating the costs of having to comply with inconsistent or excessively burdensome state laws.

TABLE OF CONTENTS

Polls suggest a high level of consumer concern about privacy on the Internet. Privacy rights already are subject to government regulation in most industrialized nations other than the U.S. Privacy advocates criticize the lack of a comprehensive privacy law in the U.S.[1] and change may be coming. The Federal Trade Commission has issued a report on on-line privacy calling for legislation and instituted proceedings under its general power to discipline deceptive trade practices. The political pressure seems to be building in Congress for action on Internet privacy. Internet privacy has been placed "[a]t the top of the list of New Economy issues likely to be the subject of legislation in the coming year" and the issue has "bipartisan support.'[2] Senator John McCain's committee heard testimony on October 3, 2000 from representatives of AOL and Hewlett Packard and consumers on several pending bills.[3]

The U.S. government's regulation of privacy rights could determine important aspects of the Internet's structure and reduce the flexibility and openness that has made the Internet a major economic force. Before this happens, it is crucial to consider the nature of the consumer Internet privacy problem and whether there are regulatory alternatives that can preserve flexibility and adaptability while still providing adequate protection. Most importantly, this article questions whether federal law is the appropriate answer to consumers' privacy concerns.

Public debate on consumer Internet privacy has been hindered by the failure clearly to separate distinct privacy issues. First, government intrusions qualitatively differ from those of firms. While government can compel people and firms to turn over information, private firms that abuse consumer information lose customers. Thus, equating governments' and firms' privacy incursions, as some commentators have done,[4] questionably assumes that markets do not work. Although citizen exit from government regulation is feasible, particularly when regulation is at the state level, this requires letting parties choose the applicable regime ex ante. One who is subject to government regulation solely by virtue of residing there must choose the entire bundle of state rules, such as those mandating disclosure of personal information when citizens engage in a

---

[1] For writings advocating mandatory privacy laws in the U.S., *see* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373 (2000); Jessica Litman, *Information Privacy/Information Property,* 52 STAN. L. REV. 1283 (2000); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules In Cyberspace,* 52 STAN. L. REV. 1315 (2000) (hereafter Reidenberg *Resolving Conflicting Rules*); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector,* 80 IOWA L. REV. 497, 516-18 (1995); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce,* 14 BERKELEY TECH. L. J. 771, 771 (1999); Pamela Samuelson, *Privacy as Intellectual Property?* 52 STAN. L. REV. 1125 (2000); Paul M. Schwartz, *Privacy & Democracy in Cyberspace,* 52 VAND. L. REV. 1609 (1999).

[2] See Tatiana Boncompagni, *Expect Talk but Little Action on Tech Issues*, Legal Times, November 16, 2000, available on http://www.law.com (accessed November 16, 2000). *See also* Ariana Eunjung Cha, *Key Firms Back Bill On Web Privacy*, Wash. Post, October 4, 2000, Page E1 (noting that "[t]he consensus that some legislation is needed--even if the two sides differ on the remedy--makes it likely Congress will take some action in the coming year").

[3] *See Hearing on Privacy Legislation Before the Senate Commerce Committee* 2000 WL 23833311 (October 3, 2000) ("Privacy Hearing").

[4] See Cohen, supra note 1; Schwartz, supra note 1, and Reidenberg, *Resolving Conflicting Rules, supra* note 1.

state-regulated or state-monitored activity, including birth, driving, working or dying.

Second, it is helpful to further distinguish between information that consumers clearly expect to be kept private, such as medical records, and consumer marketing information -- that is, relatively mundane identifying information and click-trails, or "cookies," that merchants use to focus their marketing efforts -- where such expectations are much less clear. People turn over the former type of information expecting that it will not be disclosed to others without their consent. The main issues here concern whether firms and governments should be able to use the information notwithstanding this expectation, and how and under what circumstances violators should be punished. Given greater uniformity of preferences and expectations, state law's advantage of offering diverse approaches does not come as strongly into play.[5]

The questions as to whether to protect consumer marketing information and at what price suggest that alternative rules and contracts may be important. It is unclear whether any government regulation is appropriate given firms' incentives to post and adhere to privacy policies in order to encourage customers to deal with them on the Internet and to reveal information. The form of regulation might range from disclosure rules and guidelines for private regulatory groups, through requiring specific consumer consent to use of information, to mandating specific protection irrespective of contract.

This paper focuses more precisely on the question whether regulation should be at the state or federal level. A federal solution would address potential over- and under-reaching of state regulation. States might try to regulate all Internet transactions that connect locally, thereby tying up the Internet with multiple regulations. To the extent that states can reach only transactions that originate locally, harms to consumers may go unregulated. Federal law can preempt multiple state laws and regulate across state borders. Indeed, a leading industry trade group has called for federal regulation "to create uniform U.S. privacy standards and work for international harmonization. Otherwise, online business could face 50 conflicting sets of privacy rules.'[6]

We present an alternative view of the tradeoffs between state and federal law. In brief, we believe that state rather than federal law is the appropriate mechanism for regulating consumer privacy on the Internet. Federal law would perversely lock in a single regulatory framework while Internet technology is still rapidly evolving. State law, by contrast, emerges from 51 laboratories and therefore presents a more decentralized model that fits the evolving nature of the Internet. Moreover, competition among state laws can mute the inefficient tendencies of interest group legislation. At the same time, state law adequately protects consumers because the vibrant Internet marketplace would punish vendors who choose lax regulatory regimes. Diverse state laws would not present a problem as long as courts enforce choice of law and choice of forum clauses. State law is likely to evolve toward such enforcement because web operators can block

---

[5] To be sure, there are overlaps between categories, as where medical information is used for commercial purposes without revealing intimate secrets. For a discussion of privileges and duties in this setting *see infra* text accompanying notes 34 and 35.

[6] *See AeA Unveils Federal Privacy Principles*, January 18, 2001, available at www.aeanet.org/public/public_policy/index.html. Industry was concerned about increased enforcement efforts by state attorneys general. *See* Keith Perine, *States to Weigh In on Privacy*, The Industry Standard January 25, 2001, available at www.law.com. State enforcement actions are discussed *infra* text accompanying note 161.

transmission to states that do not enforce contractual choice and legislators who pass oppressive laws that cause firms to shun their states may face political pressure from their constituents. Thus, federal regulation, including federal choice of law statutes, is unnecessary, and may perversely impose rigid solutions that prevent the efficient evolution of state law.

To be sure, the threat of multiple state regulators make it hard for firms to be sanguine about the prospects of state law. But this article shows that there are real, even if not obvious, constraints on state regulation. At the same time, the salvation firms seek in federal law may be illusory. Congress may ignore the interests of small and potential firms that are hurt most by burdensome regulation, or bend more to consumers than to business. Even worse from business' standpoint, states or consumer lobbies may persuade Congress simply to add a layer of regulation to state law rather than to replace state with federal law. In short, careful policy analysts should avoid the Nirvana fallacy of comparing a realistic or pessimistic view of state law with an idealized view of federal law.

This article proceeds as follows. Part I examines questions concerning the extent to which the law should give consumers rights in consumer marketing information. In general, the question is what rules can best facilitate bargaining over this information. Part II discusses general regulatory alternatives in this area. Part III, the heart of the article, shows why a state law approach is preferable. Part IV discusses what role, if any, should be preserved for federal statutory law. Part V concludes.

I. THE COSTS AND BENEFITS OF REGULATING CONSUMER MARKETING INFORMATION

It is important to identify precisely the benefits of consumer marketing information, and therefore the costs of regulating it, and any defects in the market that may justify regulation. Because these costs and benefits vary from one context or transaction to another, a multiplicity of state approaches rather than a one-size-fits-all federal approach is appropriate.

We begin by describing the regulatory context. The technology of Internet shopping has generated new types of and markets for information. Consumers who move through the Web leave behind two types of data trails they would not generate in a shopping mall: the more conventional track from email addresses or other information needed to enter a website, which can be linked with other information through databases and search tools; and "clickstream data,"[7] which is more significant for present purposes because it is generated silently and therefore raises more significant issues about informed consent. Websites place unique identifying numbers called "cookies" on the hard drives of surfing consumers who use the popular Netscape and Internet Explorer browsers. Web operators can use cookies to combine all information generated by visits to the site by a particular computer. Thus, the web operator knows which pages the computer visited and how long it spent on each page. The web operator may be able to link this information with identifying information the consumer has supplied, including email addresses, passwords, and credit card numbers (although this does not necessarily mean that the web operator can grab such information from a consumer who has merely viewed the web page). This is how Amazon.com knows that you are "Larry" or "Bruce" when you visit it, what your addresses are, and what books you have bought in the past.

---

[7] See Reidenberg, *Resolving Conflicting Rules*, supra note 1 at 1321-3.

Buyers of web space such as DoubleClick and other advertising networks can also buy the web sites' cookies and aggregate information from many websites, thereby creating huge databases of individuals' visits to websites, identities and demographics.[8] Privacy advocates became particularly concerned about the size of these databases in June, 1999, when DoubleClick announced a merger with a direct marketer, Abacus Direct, that held such information as individuals' credit card numbers, mailing addresses, phone numbers, and household income.

In general, consumer marketing information benefits both merchants and consumers by reducing information and transaction costs, and in turn inefficient transactions and fraud.[9] Such disclosures can be part of a mutually beneficial exchange of money and information for goods and services on terms that reflect the disclosed information. They tell web merchants how many and what types of consumers they are reaching, and help them target particular advertisements to particular consumers. The data creates new companies such as DoubleClick and a new product for web merchants to sell, which may be critical to firms' survival given the thin margins of web retailing.[10] Cookies help consumers because more precise targeting of web advertising increases its information value to consumers, thereby helping consumers satisfy their preferences.[11] Consumers also get reduced prices or free benefits for using websites that collect data, and from an expanded choice of products and services.

It is, therefore, important to determine how to regulate this market without killing it. This requires a focus on the precise problems that require regulation. Even if merchants collect and use information for purposes other than completing the transaction, as when they sell transactional and "clickstream" data to third parties, there is no problem if the consumer is informed and voluntarily agrees to use of the information. Informed consumers will give up personal information when its privacy value is less than what someone else is willing to pay for it, which in turn depends on the value of subsequent use of the information. Problems may arise when such data is collected and used without the consumer's knowledge or agreement. There is a potential conflict between the social benefits of disclosure, including from creating new databases, and an individual's desire to control the further dissemination of consumer information because of the threat of reputational harms, a general taste for privacy or autonomy, or the possibility of identity

---

[8] This has been referred to as the related problems of "data warehousing" and "data creep," where sellers use cheap storage to keep increasing the amount of information they compile with a view to possible future uses. See *id* at 1323-24.

[9] *See, e.g.,* Richard A. Posner, OVERCOMING LAW, Chapter 25 (1995); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEG. STUD. 623 (1980).

[10] This became evident in the recent efforts by Toysmart to sell consumer data in bankruptcy, and Amazon's response to the Toysmart controversy of quietly changing its privacy policy to classify customer information as a business asset that is transferable if Amazon or one of its business units is sold. *See* Keith Perine, *Privacy Centers Have Their Eyes on Amazon*, The Industry Standard, December 6, 2000 (available at http://www.law.com).

[11] See Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of* Privacy, 84 GEO. L. J. 2381 (1996). (citing Equifax Survey showing that 78% agreed that "because computers can make use of more personal details about people, companies can provide more individualized services than before")

theft.[12]

Attempts to resolve this conflict focus on whether an individual should have a privacy right and, if so, what form this right should take.[13] Because such a right would protect information, much of the debate has concerned the desirability of intellectual property right protection.[14] However, factual consumer marketing information would not be protected under current federal statutory regimes. Since such information would be produced without property right protection, the benefits of legal protection are unlikely to outweigh the increased costs of monopoly and expression.[15] Where consumer marketing information is used to produce valuable databases and other works, federal statutory intellectual property rights can cover subsequent uses of these facts under some circumstances, but not the facts themselves or obvious compilations.[16] Analogously, although novel and non-obvious discoveries based on personal genetic information can be patented,[17] intellectual property laws do not protect the genetic information itself.[18] Nor would consumer marketing information appropriately be covered by state laws that seek to encourage the production of facts,[19] trade secret law,[20] or right of publicity statutes that protect celebrities' interests in their original and distinctive identities.[21]

---

[12] See Richard A. Posner, *Privacy*, in THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW, Vol. 3 at 103-8 (P. Newman, ed. 1998).

[13] *See* Murphy, supra note 11. *See generally,* Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. PAPERS AND PROCEEDINGS 347 (1967) (showing that technological changes that alter the relative value of certain resources have resulted in the creation of new property rights).

[14] See Samuelson, *supra* note 1, Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution,* 52 STAN. L. REV.1545 (2000).

[15] *See, e.g.,* William M. Landes and Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEG. STUD. 325, 347-9 (1989) (noting that strengthening intellectual property protection can reduce welfare by increasing the cost of producing subsequent works); Litman, *supra* note 1 at 1295, and Samuelson, supra note 1 at 1138, reject the creation of intellectual property rights in part because such systems would make it difficult to prevent the alienability of personal information. However, this critique may be overstated given the ubiquitous use of licensing as a means to contractually impose inalienability.

[16] *See* Feist Publications v. Rural Telephone Service, 499 U.S. 340 (1991). *See also* Lemley, *supra* note 14 at 1546-7 (noting the lack of protection for database compilations of information individuals would seek to cover under privacy rights).

[17] *See* Diamond v. Chakrabarty, 447 U.S. 303 (1980).

[18] *See* Moore v. Regents of the University of California, 793 P.2d 479 (Cal. 1990), *cert denied* 499 U.S. 936 (1991); Litman, *supra* note 1 at 1303-4.

[19] Factual information can be protected under the tort of misappropriation, but protection is limited to "hot news" and protection against "free-riding" by direct competitors. See International News Service v. Associated Press, 248 U.S. 215 (1918); National Basketball Association v. Sports Team Analysis and Tracking Systems, 105 F.3d 841 (2nd Cir. 1997).

[20] However, Samuelson, supra note 1, suggests adopting default contract terms based on trade secret law.

[21] A property right to a public figure's identity can serve as an incentive to produce and as a

Although state and federal intellectual property rights laws do not appropriately address privacy concerns, some privacy protection for consumer data may be efficient. One alternative would be to protect privacy concerns directly by prohibiting the sale or further dissemination of consumer marketing information.[22] Such a rule can increase consumers' willingness to transact business and disclose information, either explicitly or through visiting a website,[23] while preventing the production of valuable databases and increasing transaction costs.[24] Because circumstances vary across transactions, a contract default rule may be more efficient than a mandatory rule.[25]

The fundamental issue is whether a default rule of privacy is more efficient than a default rule that allows collection and dissemination of consumer data. Given transaction costs, an efficient rule would maximize social surplus net of the costs of contracting around the rule.[26] This depends on what the parties would have agreed to ex ante, in the absence of transactions and information costs.[27] As noted above, parties presumably

---

disincentive to dissipate a valuable asset. *See* Mark F. Grady, *A Positive Economic Theory of the Right of Publicity*, 1 UCLA ENT. L. REV. 97 (1994). *But see* Vanna White v. Samsung Electronics America, Inc. 989 F.2d 1512 (9th Cir. 1993) (dissent from order rejecting the suggestion for a hearing en banc).

[22] *See* Litman, *supra* note 1 at 1302-3.

[23] *See, e.g.,* Murphy, *supra* note 11; Frank H. Easterbrook, *Insider Trading, Secret Agents, Evidentiary Privilege, and the Production of Information*, 1981 SUP. CT. REV. 309 (1982) (discussing contractual prohibition against disclosure of information); Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. LEG. STUD. 683 (1980) (same).

[24] See Solveig Singleton, *Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector*, CATO Institute Policy Analysis No. 295 (1998). A privacy-induced increase in the use a web site or consumer service is not always desirable. *See* the Posner and Stigler articles, *supra* note 9. For example, A&M Records, et al. v. Napster, 114 F. Supp. 2d. 896 (2000), found that the majority of files transferred by persons using the Napster service have been unauthorized copies of copyrighted music, and ordered Napster to cease operations for contributing to copyright infringement. The 9th Circuit affirmed the district court's grant of the plaintiff's motion for a preliminary injunction. However, the 9th Circuit found that the scope of the injunction was overbroad, and remanded the case to the district court. See A&M Records, et al. v. Napster, _ F3d _ (2001). The 9th Circuit noted that the "mere existence of the Napster system, absent actual notice and Napster's demonstrated failure to remove the material, is insufficient to impose contributory liability." See id at _ (citing Sony Corp. v. Universal City Studios, 464 US 417, 442-43 (1984)). The question for the district court on remand, then, is whether Napster can differentiate infringing and non-infringing uses so that a remedy would not unduly interfere with legitimate activities. Napster or the recording companies could use cookies or Globally Unique Identifier (GUID) technology to allow copyright holders to detect licensing or copyright violations without deterring non-infringing uses. For a discussion of the use of GUID technologies, see Jonathan Weinberg, *Hardware-Based Id, Rights Management, and Trusted Systems*, 52 STAN. L. REV. 1251, 1261-3 (2000).

[25] *See e.g.,* Murphy, supra note 11, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998).

[26] See Ronald Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1 (1960); Harold Demsetz, *When Does the Rule of Liability Matter?* 1 J. LEG. STUD. 13 (1972). *See also* Lemley, *supra* note 14, at 1554 (noting that allocating strong rights to consumers is inefficient because high transactions costs will prevent the value increasing transfer of such rights).

[27] Frank H. Easterbrook & Daniel R. Fischel, *Contractual Freedom in Corporate Law*, 89 COLUM. L. REV. 1416, 1433 (1989); Charles J. Goetz & Robert E. Scott, *The Mitigation Principle: Toward a*

would agree to allow collection and dissemination of consumer data if and only if the expected value of future uses of the information at the time of contracting exceeds the value of privacy. The rule could be embodied in statutes or tort law.[28] While protection against dissemination of accurate and factual personal information based on the tort of invasion of privacy is limited,[29] courts have, under limited circumstances, protected privacy concerns based on the tort doctrine of breach of trust.[30] It has been suggested that the breach of trust tort should be expanded,[31] which would involve creating new implied duties of non-disclosure analogous to those in attorney-client and doctor-patient relationships.[32] Since any discernable principle underlying such duties is one of implied contract,[33] the appropriate rule would depend on the same default rules analysis as above, and liability for dissemination of consumer data would be subject to explicit or implied consent.

To illustrate these issues, consider *Moore v. University of California*.[34] After Moore's spleen was removed for medical reasons in connection with his treatment for hairy cell leukemia, inspection of tissue samples from the spleen revealed that its cells had unique properties. On the doctor's instructions, Moore returned to give additional blood and tissue samples, some for research but not medical purposes. A valuable and patented cell line was eventually established from Moore's tissues. Moore sued for conversion of his spleen cells. He lost on his property claim but won on his tort claim of breach of fiduciary duty based on the doctor's failure fully to disclose the reasons for the subsequent visits. The decision correctly denies Moore an intellectual property right to his cells since the medical research use of Moore's cells does not require attribution to or identification of Moore and Moore had signed a standard form prior to surgery consenting to having blood and tissue samples taken after surgery, with the usual boilerplate about medical research.

Should Moore's doctor have a fiduciary duty to his patient to disclose more based

---

General Theory of Contractual Obligation, 69 VA. L. REV. 967, 971 (1983). *But see* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L. J. 87 (1989) (arguing that penalty defaults can be efficient).

[28] *See* RESTATEMENT (2D) OF TORTS §652A-C (1976) (providing that the right of privacy is invaded by unreasonable intrusion upon the seclusion of another, appropriation of the other's name or likeness, the unreasonable publicity given to the other's private life, or the publicity that unreasonably places the other in a false light before the public).

[29] See Murphy, supra note 11, Schwartz, *supra* note 1; Robert Gellman, *Does Privacy Law Work?* in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Phillip E Agre & Marc Rotenberg, eds., 1997).

[30] See Murphy, supra note 11.

[31] See Litman, supra note 1.

[32] The attorney-client and other privileges are qualified. *See, e.g.*, Ronald Allen, et al., *A Positive Theory of Attorney-Client Privilege and the Work Product Doctrine*, 19 J. LEG. STUD. 359 (1990) (arguing that privilege protects only communications that contain negative information). *See also* Easterbrook, *supra* note 23.

[33] *See* Murphy, supra note 11, at 2410. *See also* Richard A. Posner, ECONOMIC ANALYSIS OF LAW, at 271-2 (5th ed. 1998) (noting identity of economic analyses of tort and contract law).

[34] 793 P.2d 479 (Cal. 1990), *cert denied*, 499 U.S. 936 (1991).

on Moore's general expectation of privacy in the doctor-patient relationship with respect to medical records or genetic information? Although Moore's cells were anonymous and his spleen had no value to him in the absence of medical research, if he had known the medical value of his cells Moore might have demanded a high payment for his continued cooperation. On the other hand, an informed Moore might be able to appropriate much of the value of the cell line despite the fact that any payment in excess of the opportunity costs of Moore's time would be a pure rent to Moore. Requiring disclosure might be welfare-reducing because doctors would discard valuable spleens. Thus, a focus on fiduciary duties may yield the wrong disclosure rule. Contracts are enforced despite one party's failure to disclose material information about which it knows the other side is mistaken in order to encourage production of information.[35] This supports a default rule in the *Moore* situation permitting use of the information even without explicit patient consent.

Moore is useful more for contrast with the consumer marketing information context than as a direct guide. Unlike in *Moore*, one consumer could not capture the value of the data compilation by threatening to withhold his future cooperation. Also, because consumer data identifies the individual, privacy concerns may be greater than in *Moore*. Thus, unlike in *Moore*, a rule that requires disclosure of the potential uses or consumer data can be the correct result.

Cases decided based on common law and state consumer protection statutes recognize a disclosure requirement in contexts closer to consumer marketing information, but also suggest that the nature of consumers' expectations may vary from one context to another. In *Dwyer v. American Express*, American Express had collected and analyzed cardholders' spending patterns without obtaining informed consent. Cardholders sued American Express in the Illinois state courts for intrusion, appropriating their personal spending habits, and violating Illinois and other states' consumer fraud statutes. The appellate court affirmed dismissal of the tort intrusion claim for failure to show intrusion, and held that there was no tort misappropriation because the defendant created the value "by categorizing and aggregating [cardholders'] names.'[36] However, Amex's failure to inform cardholders that their spending habits would be analyzed and their names sold to advertisers constituted a deceptive practice under the Illinois Consumer Fraud Statute because some consumers may not have used the card if they knew of the practice, although plaintiffs failed sufficiently to allege damages from defendants' practices.

In *Weld v. CVS Pharmacy*, CVS used information collected from customers who filled prescriptions at their stores to maintain, without customers' informed consent, a database that CVS used to conduct a direct mail campaign funded by several pharmaceutical companies.[37] Customers sued CVS and the pharmaceutical companies

---

[35] Anthony T. Kronman, *Mistake, Disclosure, and the Law of Contracts*, 7 J. LEG. STUD. 1 (1978). *See also* Janet K. Smith and Richard L. Smith, *Contract Law, Mutual Mistake, and Incentive to Produce and Disclose Information*, 19 J. LEG. STUD. 467 (1990). Some have even suggested that the informed party should be able to lie. *See* Robert Heidt, *Maintaining Incentives for Bioprospecting: The Occasional Need for a Right to Lie*, 13 BERK. TECH. L. J. 667 (1998). *See also* Saul Levmore, *Securities and Secrets Insider Trading and the Law of Contracts*, 68 VA. L. REV. 117 (1982).

[36] Dwyer v. American Express, 273 Ill.App.3d 742, 745-46, 749, 652 N.E.2d 1351, 210 Ill. Dec. 375 (1995).

[37] 1999 WL 494114 (Mass. Superior Ct. June 29, 1999). The court subsequently certified a class

for violation of a statutory right to privacy,[38] unfair practices,[39] breach of confidentiality and fiduciary duties, and for tortious misappropriation of private personal information. The trial court denied defendant's motions for summary judgment on all claims, noting individuals' special expectation of privacy concerning medical information, and distinguishing *Dwyer*.[40]

These cases indicate that the extent of protection should depend on, among other things, the consumer's expectations of privacy, and on how regulation will affect incentives to produce valuable information. Also, as discussed in more detail in the next Part, it is not clear what form any protection might take, including whether the rules should be of the opt-in or opt-out variety. Thus, a particular default rule may be wrong for a significant number of transactions.[41] This suggests the desirability of a regime that lets the parties contractually select from among a variety of state rules.

II. REGULATORY ALTERNATIVES

The economics of consumer marketing information raises issues concerning the types of *regulations*, and types of *regulators* that should protect consumers' rights. This Part discusses some of the choices. Approaches can be combined, and there are myriad specific variations concerning such matters as adjudication methods, penalties, defining protected information, disclosure techniques and mechanics of consent. Table 1 summarizes some of the many alternative possible approaches to regulating consumer marketing information. Consistent with the analysis in Part I, different constraints might apply to different types of information. For example, strong consent might be required for sensitive types of information, while only opt out is required for other types of personally identifiable information, and no constraints at all apply to information that is in neither category.[42] Also, the rules might apply only to disclosure of the information to third parties or use for purposes other than those for which the information was collected rather than to mere collection of the information.

The variety of proposals underscores the main lesson from this Part that the many questions concerning the appropriate regulatory approach, combined with doubts raised in Part I about the nature of the rights to be protected, suggest that it may be harmful prematurely to lock in a particular approach through uniform federal regulation.

---

of Massachusetts CVS customers that received a mailing. *See* Weld v. CVS, 1999 WL 1565175 (Nov. 19, 1999).

[38] Mass. G.L. ch. 214, §1B provides that "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy."

[39] *See id.* ch 93A (which the court characterized as based on unfairness, immoral, unethical, oppressive, or unscrupulous conduct, or injury to competitors or other business people, 1999 WL 1565175, slip at 6).

[40] 1999 WL 494114 at 5. However, the court also noted that the misappropriation claim was probably preempted by the privacy statute cited above. *Id.* at 6-7.

[41] See Posner, *supra* note 33 at 112-3.

[42] *See, e.g.,* 2000 AZ H. 2717. For potential Federal approaches, see the text accompanying notes 86-90.

A. TYPES OF CONSTRAINTS

1. Disclosure

Vendors' disclosure to consumers arguably should be a minimum prerequisite to their right to use consumer marketing information. A website operator might be required simply to disclose the types of information it is collecting, how it is using this information and how consumers can learn what specific information the operator is or has collected from them. The disclosure might be made in several ways varying according to the effort necessary to get it, including an information screen flashed to the individual user on logging on,[43] a statement that the information is available at a specified web address or place on the website the consumer is already surfing, or by request by email, telephone or letter.[44] The appropriate approach obviously depends on balancing the costs both to the vendor and the consumer of more affirmative disclosure methods, including forcing web surfers to click through disclosure screens, against the benefits of reducing consumers' search costs.[45]

2. Opt-in v. Opt-out

A website operator might be prohibited from collecting any information *unless* it obtains the consumer's affirmative consent to the particular use, or *if* the consumer opts out of the practice the operator proposes, in either case after disclosure to the consumer.[46] Consumer consent might be as simple as clicking on an "I accept" box or even based simply on the consumer's decision whether to use the website that gathers the information.[47] On the other hand, the law might require an actual written, or at least electronic, signature.[48] Where the use precedes precise disclosure, consent may or may not be predicated on the consumer's general knowledge of the information-gathering activity.[49]

An opt-in procedure draws the consumer's attention to her right to refuse to consent to the collection. By contrast, an opportunity to opt out of a website operator's policies and practices regarding consumer marketing information would give legal significance to consumer inaction, and therefore reduce the directness with which the consumer is presented by an explicit choice.

---

[43] *See, e.g.,* 1999 WI S. 375 (display of notice describing information collected).

[44] *See, e.g.,* 1999 AK H. 273, 1999 AK 410. (notification by mail or e-mail at time of subscription).

[45] Compare 1999 NY A.1909 (requires notice at time of agreement) and 1999 CA AB 1793 (separate affirmative consent required for each disclosure).

[46] Compare 1999 AK H. 273 (written opt-in), and 1999 AK 410 (written opt-out).

[47] *See, e.g.,* 2000 CO H. 1459 (consumer must have option to opt-out).

[48] *See, e.g.,* 1999 CA A.B. 1793; 1999 MI S.B. 1065; 1999 NY S. 8021 (requiring affirmative consent in writing).

[49] *See, e.g.,* 1999 KS H. 2896 (Requires "knowledge of subscriber").

As with disclosure, the appropriate policy depends on balancing the costs to website operators and consumers of offering and making choices against the benefits to consumers of making the choices more obvious.[50] Aggressively presenting choices to consumers might give them more leverage over merchants in dealing with their information. On the other hand, affirmative disclosures slow down consumers' web surfing, increase transaction times and tie up servers. While these costs increase directly with the number of disclosures, repetitively reminding consumers of privacy choices may have diminishing benefits.

3. "Baseline" protection

The above discussion makes the amount of regulation turn on consumer choice. An alternative would be a rule requiring websites to offer certain minimal "baseline" protections to all consumers. This approach could be combined with one of the others by requiring disclosure of additional protections, perhaps coupled with opt-in or opt-out rules. This alternative is generally identified with government regulation, and is discussed as such below. But a baseline approach also might be applied by private regulatory groups, or incorporated into consumer self-help if consumers configure their computers to surf only complying sites. In the latter situation, the baseline applies to all websites but varies from one consumer to the other.[51]

---

[50] See ProCD v. Zeidenberg 86 F.3d 1447, 1451 (7th Cir. 1996) *See also* J. Howard Beals III, *Economic Analysis and the Regulation of Pharmaceutical Advertising,* 24 SETON HALL L. REV. 1370, 1381 (1994) (noting the effect of disclosure on the costs of advertising and other forms of marketing communication); Howard Beals, et al., *The Efficient Regulation of Consumer Information*, 24 J. L. & ECON. 491 (1981).

[51] Baseline regulation has emerged from a focus on so-called "Fair Information Practices." *See, e.g.,* Schwartz, *supra* note 1. An emerging standard of such practices is the 1980 Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*:

1. Collection Limitation Principle: There should be limits on the collection of personal data, and such data should be gathered legally, and with the knowledge or consent of the data subjects.

2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection, and all subsequent uses should be limited to those purposes.

4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for alternative purposes without consent from the data subject or by the authority of law.

5. Security Safeguards Principle: Personal data should be protected from unauthorized access, destruction, use, modification, or disclosure.

6. Openness Principle: There should be a general policy of openness about developments in data collection and use. Means should be readily available to ascertain the existence and nature of personal data, the main purpose of their use, and the identity and location of the data controller.

7. Individual Participation Principle: An individual should be able to contact a data controller

Again, the policy decision requires balancing costs and benefits. Offering choices may consume valuable resources of both consumers and web operators. On the other hand, adopting baseline restrictions on web operators' use of consumer marketing information to some extent precludes bargaining that can place an accurate value on particular information and protections and thereby efficiently allocate resources. The efficiency of this approach depends on, among other things, consumers' ability to obtain and process information relevant to bargaining, regulators' ability to anticipate vendor and consumer preferences in particular situations, and the degree of variation among transactions. Thus, the efficiency of a baseline approach may depend on who imposes the constraints. It might make sense for individual consumers or industries, but not for across-the-board federal regulation.

B. NON-GOVERNMENT CONSTRAINTS

Each of the above approaches might be applied by a variety of government and non-government regulators.[52] First, individual website operators might simply contract with their users for the level of protection regarding consumer marketing information. The standard contract remedies, buttressed by reputational and other market-based penalties, would enforce any contracts firms make with consumers. The law might reduce contracting costs by supplying default rules. As discussed below, consumers also might, in effect, impose their own default rules through self-help mechanisms that block access to sites that do not bargain around the rules.

Second, rather than government's supplying default rules or enforcement mechanisms, firms could subscribe to organizations that supply the rules and police violations through fines or expulsion.[53] Third-party control and monitoring is currently provided by organizations such as Ernst & Young and TRUSTe.[54] Commercial entities might select private providers of legal rules whose judgments are enforced as final in the state court.[55] Johnson and Post also discuss the potential for private regulatory structures

---

about what information the controller has about that person, and be able to correct inaccurate records. If an access request is denied, a reason must be given, and the individual must be able to challenge the denial.

8. Accountability Principle: A data controller should be accountable for complying with the measures which give effect to the principles stated above.

[52] This discussion reserves the main question addressed in this article of whether any government regulation should be at the federal or state level.

[53] These organizations may not accurately be characterized as "self-regulatory," but rather as providing "regulation" based on contract or, like private ordering generally, as operating in the shadow of the law. *See* Lemley, *supra* note 14 at 1554 (describing self-regulation as "illusory").

[54] *See* www.truste.org. TRUSTe licensees must abide by TRUSTe's policies concerning collection and use of consumer information, subject to TRUSTe's monitoring and auditing of licensees and resolution, reporting and possible referral to the FTC of consumer complaints. Other private organizations sponsoring consumer privacy efforts include those established by the Better Business Bureau (bbbonline) and the American Institute of Certified Public Accountants.

[55] *See* Gillian K. Hadfield, *Privatizing Commercial Law: Lessons From the Middle and the Digital Ages*, Stanford Law School, John M. Olin Program in Law and Economics Working Paper No. 195 (March, 2000), available at http://papers.ssrn.com/paper.taf?abstract_id=220252.

on the Internet, possibly including consumer protection doctrines.[56] They suggest that territorial governments will have incentives to grant "comity" to, and not interfere with, these regimes. The industry has been developing the "P3P" protocol, which would permit a kind of automated contracting whereby consumers' computers can block access by firms whose privacy policies do not meet user-configured standards.[57] This would operate in conjunction with consumer self-help, described below, to permit individuals, at low cost, to contract for precisely the level of privacy protection they prefer.[58]

Third, consumers can protect their information by refusing to make personal disclosures or by simply turning off the cookie feature of their browsers. The market also has developed devices that permit consumers to customize the amount of marketing information they make available and to whom they give it.[59] The P3P protocol makes websites work with these devices by standardizing websites' interactions with consumers' computers. These devices force merchants to bargain with consumers. The following section discusses whether consumers are able effectively to deal with merchants over their information without government protection.

C. ARGUMENTS FOR GOVERNMENT REGULATION

Government might provide mandatory rules that impose general fraud liability pr require disclosure of or consent to websites' policies. Government also might monitor private regulatory organizations.[60] The policy question is whether such rules are necessary in light of the availability of the less coercive private alternatives just discussed. The answer depends partly on whether efficient rules are likely to emerge from contracts between vendors and customers, and on whether contracts between vendors and consumers will ignore third party interests. Commentators have argued strongly that individuals have fundamental privacy rights to protection of personal information that mandatory rules should enforce.[61]

---

[56] *See* David R. Johnson and David Post, *Law And Borders--The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1380, 1383, 1390-91 (1996). They analogize this to the private regulatory structures that have developed in other areas, including securities exchanges (*id*. at 1392) and the law merchant (*id*. at 1389-90).

[57] *See* Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE, 160 (1999) (endorsing P3P as giving individuals a kind of automated property right in their information).

[58] *See* Note, *Internet Regulation Through Architectural Modification: The Property Rule Structure of Code Solutions*, 112 HARV. L. REV. 1634 (1999).

[59] *See, e.g.*, www.anonymizer.com (making available free software that allows anonymous surfing); www.adsubstract.com (offering a cookie customizer that allows users to manage cookies); www.junkbuster.com. *See also* David P. Hamilton, *Freedom Software Lets You Get Some Privacy While Surfing the Web*, Wall St. J., August 10, 2000 at B1 (discussing software that lets users hide behind alternate identities).

[60] *See* Federal Trade Commission, *Final Report of the FTC Advisory Committee on Online Access and Security*, May 15, 2000 (available online at www.ftc.gov) (discussing regulatory options including government, third party under guidelines, or third party with disclosure; noting that second option imposes regulatory burden on government but raises concern about lax standards).

[61] See e.g., Christopher D. Hunter. *Recoding the Architecture of Cyberspace Privacy: Why Self-Regulation and Technology Are Not Enough* (February, 2000); Schwartz, *supra* note 1; Reidenberg, *supra*

The appropriate regulatory policy is not necessarily evident from actual consumer and industry practices. For example, the FTC privacy study emphasized evidence that only 10% of websites were implementing "fair information practices" that the FTC had identified.[62] However, rejecting these practices might efficiently balance costs and benefits. Nor is it necessarily enough to point to incidents in which Web retailers apparently have breached their privacy promises or otherwise failed to meet consumers' expectations.[63] The question is whether the costs of partial regulation outweigh the benefits of consumer choice. As shown below, much of the case for central regulation rests on questionable assumptions.

Nor is the need for regulation evident from the "adhesion" nature of contracts between consumers and website operators. Consumers might accept or reject vendors' policies without bargaining over details because individualized bargaining with each of the myriad sites consumers contact is excessively costly.[64] However, even in this situation consumers have the viable choice of using alternative sites or vendors. Accordingly, the "adhesive" nature of a contract does not alone make it inefficient.[65]

1. The Internet as a lemons market

It has been claimed that consumers will resort to brick-and-mortar merchants

---

note 1; Cohen, *supra* note 1. The focal point of the debate is the 1980 Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, quoted above.

[62] *See* FTC Report, *supra* note 60 at 37.

[63] *See* Don Clark, *RealNetworks Will Issue Software Patch To Block Its Program's Spying on Users*, WALL ST. J., Nov. 2, 1999 at B8 (discussing RealNetworks Inc. gathering of information about consumers' listening habits without their consent); Michael Moss, *A Web CEO's Elusive Goal: Privacy*, WALL ST. J., February 7, 2000 at B1 (discussing how ELoan, despite touting the strength of their privacy policy, tracked information about consumers without their consent); Perine, *supra* note 10 (discussing criticism of change in Amazon privacy policy to permit sale of consumer marketing information); Rebecca Quick, *On-Line: GeoCities Broke Privacy Pledge, FTC Declares*, WALL ST. J. August 14, 1998 at B1 (discussing GeoCities settlement of an FTC complaint that it misrepresented that information on application forms would not be disclosed to third parties); Thomas E. Weber, *Network Solutions Sells Marketers Its Web Database*, WALL. ST. J., February 16, 2001 at B1, 2001 WL-WSJ 2854616 (discussing Network Solutions' plan to sell database of customer information); Nick Wingfield, *DoubleClick Moves to Appoint Panel for Privacy Issues*, WALL ST. J., May 17, 2000 at B2, 2000 WL-WSJ 3029717 (discussing DoubleClick Inc.'s plans to combine databases of people's Web-surfing habits and of users' personal information).

[64] *See generally*, David Friedman, *In Defense of Private Orderings: Comments on Julie Cohen's "Copyright and the Jurisprudence of Self-Help"*, 13 BERK. TECH. L. J. 891, 898 (1998). However, automated contracting, as through web agents, or "bots," aided by protocols such as P3P (*see supra* text accompanying note 57), might make a form of individualized bargaining feasible.

[65] *See* Declan McCullagh, *Why Internet Privacy Is Overrated*, Thursday, April 29, 1999, available at privacy http://www.speakout.com/Content/ICArticle/3821 (noting that consumers are not at the mercy of Amazon because they can always go to Barnes & Noble); ProCD v. Zeidenberg, supra note 50 at 1453 (noting that "[c]ompetition among vendors, not judicial revision of a package's contents, is how consumers are protected in a market economy.") *See also infra* note 128 and accompanying text (discussing choice-of-law contracts).

unless online merchants are tightly regulated.[66] This suggests that consumer marketing information involves a "lemons" market: because consumers cannot distinguish between high and low-quality promises of data protection and enforcement levels, they will not be willing to pay for higher levels of protection and low-quality merchants will dominate the market.[67]

A "lemons" problem seems inconsistent with three important features of Internet markets. First, because on-line merchants need to encourage consumer trust in this new market, they have ample incentives to build reputations for trustworthiness. These investments function to bond future performance. Merchants that frustrate consumer expectations devalue their reputations and effectively forfeit their bonds.[68]

Second, various media, including the Internet itself, spurred by highly vocal privacy advocates, rapidly disseminate information about background facts and individual merchants. For example, when DoubleClick acquired a direct-mail company and planned to merge its cookie data with the direct-mail database, "a fierce backlash" forced DoubleClick to postpone the database merger plan and hire prominent consumer advocates as privacy monitors.[69] Because consumers can refuse to deal with offending websites or deny marketing information to these sites, a consumer backlash can reduce web operators' ability to accumulate information and give them an incentive to change their practices.

Third, it is unnecessary for all consumers to be sophisticated or aware of the problems for markets to protect all consumers. Because of vendors' high costs of discriminating between the informed and uninformed in this setting, due partly to their reliance on standard form contracts, competition for the marginally informed consumer protects the uninformed consumer.[70] Marginal Internet consumers, who are likely to be

---

[66] *See, e.g.,* Schwartz, *supra* note 1. The FTC Report notes that consumer "apprehension likely translates into lost online sales due to lack of confidence in how personal data will be handled," citing survey reports. *See* FTC Report, *supra* note 60 at 2. *See also* Murphy, supra note 11 (citing results of Equifax Surveys showing large increases in percentage of those responding who were "concerned" about their privacy).

[67] See George Akerloff, *The Market for `Lemons': Qualitative Uncertainty and the Market Mechanism,* 84 Q. J. ECON. 488 (1970).

[68] *See generally,* Benjamin Klein & Keith B. Leffler, *The Role of Market Forces in Assuring Contractual Performance,* 89 J. POL. ECON. 615 (1981); Benjamin Klein et al., *Vertical Integration, Appropriable Rents, and the Competitive Contracting Process,* 21 J. L. & ECON. 297 (1978). As to the nature and size of reputation penalties, *see* Jonathan M. Karpoff and John R. Lott, Jr., *The Reputational Penalties Firms Bear from Committing Criminal Fraud,* 36 J. L. & ECON. 757 (1993); Mark L. Mitchell, *The Impact of External Parties on Brand-Name Capital: The 1982 Tylenol Poisonings and Subsequent Cases,* 27 ECON. INQ. 601 (1989); Mark L. Mitchell and Michael T. Maloney, *Crisis in the Cockpit? The Role of Market Forces in Promoting Air Travel Safety,* 32 J. L. & ECON. 329 (1989).

[69] *See* Wingfield, *supra* note 63.

[70] *See* Alan Schwartz & Louis L. Wilde, *Intervening In Markets on the Basis of Imperfect Information: A Legal and Economic Analysis,* 127 U. PA. L. REV. 630 (1979). *See also* Jeffrey R. Brown & Austan Goolsbee, *Does the Internet Make Markets More Competitive?* NBER Working Paper No. W7996, http://papers.ssrn.com/paper.taf?abstract_id=248602 (November 2000) (showing evidence that Internet comparison shopping for life insurance has caused general price decreases across demographic

highly educated and technically adept, and not the uninformed inframarginal consumers, will determine contract terms in this setting.

2. The Internet as a lambs market

Advocates of regulation argue that consumers may be unable accurately to value their information in monetary terms.[71] Consumers will not even know the value of what they are giving up, and therefore, like lambs, will be shorn unwittingly of their information. Merchants will be able to obtain consumer marketing information at less than its value to consumers and will have little incentive to offer high levels of consumer protection in order to lure consumers to the Web. Merchants who have this information will be better able to price discriminate among consumers, thereby reducing customers' surplus.[72]

For the reasons discussed in subsection 1, consumers probably are not ignorant of use of merchants' use of consumer marketing information.[73] The question is whether consumers systematically undervalue their information, or value it correctly but nevertheless derive enough benefit from web transactions that they are willing to give up the information for less than its value to merchants. Assuming that consumers know that their marketing information is valuable to merchants, it is not clear why they would systematically undervalue the information, rather than either systematically overvaluing it or, more likely, valuing it accurately on average across consumers and transactions. The fact that merchants such as Internet service providers are willing to buy advertising space on consumers' computers by offering free or heavily discounted services suggests that consumers are aware of the value of their data.[74] If consumers accurately value their information but nevertheless choose to sell it for less than it is worth to website operators, then there is a further question of whether this division of the surplus is somehow inefficient.[75]

---

groups).

[71] *See* Cohen, *supra* note 1; A. Michael Froomkin, *The Death Of Privacy?* 52 STAN. L. REV. 1461, 1504-5 (2000) (arguing that consumers are "myopic").

[72] *See* David G. Post, *What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace,* 52 STAN. L. REV. 1439, 1446-7 (2000); Weinberg, *supra* note 24 at 1275. The net effect of price discrimination is ambiguous. Some consumers will be better off, and total welfare can increase. Id at 1275-6. *See* also ProCD v. Zeidenberg, *supra* note 50 at 1449.

[73] See Murphy, *supra* note 11 (citing Equifax survey reporting that 42% polled had refused to provide information to a business because of privacy concerns).

[74] A recent anecdote tends to confirm this. Wired Magazine offered its readers a free device called :CueCat, a barcode reader for connecting subscribers with advertisers' websites. Wired's publisher wrote that "many [readers] aren't crazy about the idea." All three letters to the editor the magazine reprinted on the subject complained that advertisers could use the device to obtain information about readers. For example, one said: "Are we too dumb to notice that the point of the Cat is to track our shopping behavior? I'm not giving up that info for nothing." Wired, *Rants & Raves,* January, 2001 at 43. Wired readers, though more sophisticated than average, may be the marginal consumers for whom websites are designed.

[75] Because the website operator needs incentives to create additional value through the collection and aggregation of consumers' data, it would be inefficient to let the consumer extract all or most of this additional value. *See* discussion surrounding notes 34 and 36.

Advocates of regulation argue that markets are inadequate because they do not protect non-market values such as dignity and self-expression.[76] Circulating information about individuals constrains their ability to take positions and lead lifestyles that do not conform to social norms, thereby becoming a strong force for conformity. But again, it is not clear why these considerations would not lead people to overvalue their information, and therefore make too little of it available from a social welfare standpoint. Moreover, it is not clear why government would make better choices than individuals. Regulators' guess at a value higher than that reflected in market transactions might be wrong, and therefore might reduce rather than increase individual autonomy, as by preventing people from effectuating their shopping preferences through cookies. This suggests that government should move carefully in second-guessing market decisions. One way it could do so is by maximizing exit through an emphasis on state, rather than federal, regulation.

3. Network externalities[77]

It has been argued that network externalities will prevent the development of an efficient market in consumer marketing information. One argument along these lines is that information "norms" will develop that are unfavorable to consumers.[78] Another is that technical standards will develop that do not efficiently reflect consumer preferences. P3P has been criticized in part on the ground that "[i]f not enough sites support the standard, consumers are not likely to deal with the daunting configuration, yet if not enough consumers demand it, marketers are unlikely to bother implementing it," thereby relegating consumers who prefer privacy to a "data ghetto."[79] This is essentially a claim that P3P will be unable to create a new "network" in which users efficiently can connect with websites.[80]

---

[76] *See* Cohen, *supra* note 1; Reidenberg, *supra* note 1 at 1346.

[77] Privacy advocates claim that there are other externalities, but these are even weaker arguments for regulation than the externalities argument discussed in the text. For example, forcing disclosure of personal information is said to restrict self-expression, and thereby the choices made in a democratic society. *See* Reidenberg, *supra* note 1 at 1346-47. More generally, it is claimed that this information may construct a particular type of social truth that excludes other perspectives. *See* Cohen, *supra* note 1. Consumers do not bear these social costs of selling their information, thereby creating a kind of externality. But these claims are not very plausible. For example, it is not clear why restricting self-expression by Internet tracking also would affect non-tracked decisions like those people make in voting booths. Moreover, opposing externalities arguments are at least equally plausible. For example, as discussed in the text, restricting consumer marketing information may impede individuals' expression of preferences, thereby indirectly affecting social welfare. Moreover, the information such as that involved in *Moore* may have social benefits that do not accrue to the individual who has power over the information.

[78] *See* Schwartz, *supra* note 1.

[79] *See* R.E. Bruner, *P3P: Programming Privacy, Executive Summary,* Vol. 1, No. 7 (June 30, 1998), available at http://www.exec-summary.com/trends/980630.phtml.

[80] For general discussions of network externalities *see e.g.,* Joseph Farrell & Garth Saloner, *Standardization, Compatibility, and Innovation*, 16 RAND J. ECON. 70, 71-72 (1985) (characterizing the problem as one of excess inertia); Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93 (1996). For writings critical of network externalities theory, *see* Larry E. Ribstein & Bruce H. Kobayashi, *Choice of Form and Network Externalities, ms.* (February, 2001); S. J. Liebowitz & Stephen E. Margolis, WINNERS, LOSERS, AND MICROSOFT: COMPETITION AND ANTITRUST IN

In fashioning public policy, it is necessary to distinguish "network benefits" from "network externalities." A network benefit occurs whenever the advantages of a particular product or standard, such as P3P or the telephone, increases with the number of users. Network benefits can be "externalities" because new adopters of the standard or service consider only their own benefits and not those they would confer on other users by adopting the product or standard. People may not buy a new product or adopt a new standard even if it is better than the old one apart from network benefits, and a new product or standard might not emerge even if it might have given rise to a superior network but for externalities.

A problem with identifying network externalities is that others besides individual users, such as the companies that form the high-profile consortium that is developing P3P, might internalize the benefits of creating a new standard.[81] Moreover, apart from network externalities, the market may not adopt a new standard because of its inherent inferiority.[82] If P3P fails despite all of the attention it has been given that may be because few consumers have the privacy preferences it enables.[83] If so, mandating the device through government regulation obviously will introduce inefficiency rather than curing a market failure.

4. Summary

In general, arguments for government regulation of consumer marketing information rest on questionable assumptions concerning consumers' ability to protect themselves and the existence of externalities.[84] All of this is not to say that markets will

---

HIGH TECHNOLOGY (1999) ("*Winners, Losers*"); S. J. Liebowitz & Stephen E. Margolis, *The Fable of the Keys*, 33 J. L. & ECON. 1 (1990) ("*Fable*"); S. J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 J. ECON. PERSP. 133 (1994) ("*Tragedy*").

[81] *See* Liebowitz & Margolis, *Fable*, *supra* note 80.

[82] For example, the QWERTY/Dvorak story on which the network externalities theory originally was based broke down upon a closer examination of the factual background. Liebowitz and Margolis demonstrated that the evidence for Dvorak's superiority was weak, and that QWERTY won only after proving itself against competing standards. *See* Liebowitz & Margolis, *Fable*, *supra* note 80; Liebowitz & Margolis, *Tragedy*, *supra* note 80. Similarly, Liebowitz & Margolis have attributed Microsoft's dominance in the software market to the superiority of their products, which weakens the argument for network externalities in this context as well. *See* Liebowitz & Margolis, *Winners, Losers*, *supra* note 80.

[83] This problem would seem to be exacerbated by proposals to increase the level of P3P protection by enabling functions preferred only by the most privacy-sensitive users, such as the ability to ask detailed questions of the website operator. *See* Hunter, *supra* note 61 (noting critique of P3P by privacy advocates that users cannot ask questions about such matters as the type of business, where it is incorporated, whether it is a subsidiary of another company, and contact persons).

[84] It has also been argued that permitting consumers to sell marketing information lets the rich consumers get richer by reaping merchant discounts while the poor get poorer because merchants do not value their information. *See* Cohen, *supra* note 1. This argument assumes that rich and poor sell their information for what it is worth. One problem with restricting consumers' autonomy on this basis is that it is not clear that the advantage the rich get in this context can be distinguished from other problems associated with the allocation of wealth in a capitalist economy. The rich get better schools, housing, health care, information, and so forth, all of which enables them to get richer still. Thus, it is not clear where regulation imposed on this basis would stop.

operate perfectly. For example, even if most firms have market incentives to respect consumer privacy, a failing firm with no further reputation to protect may make an unauthorized one-shot sale of consumer data before going out of business. But it is unlikely any regulation could solve problems like this.

Even if some regulation is appropriate, it should not necessarily be the sort of all-out regulation that is imposed by federal law. As discussed below, state regulation and enforcement of contractual choice facilitates diversity, experimentation and competition among regulatory approaches. This approach better effectuates consumer choice than relying on contracts alone. State laws also can help build new standards better than contracts alone, and thereby respond to any network externalities problems that may exist.[85] Thus, a reliance on state law can be viewed as a way to find the appropriate level of regulation, and thus as a compromise between privacy zealots who demand strong regulation and libertarians who want none.

III. THE STATE LAW ALTERNATIVE

As discussed at the beginning of the paper, Congress seems poised to enact federal regulation. Pending bills would require web operators to disclose their practices for using personal information collected from consumers, and provide for private remedies and public enforcement.[86] Bills vary, among other ways, according to whether they provide for opting into or out of protection,[87] empower the FTC to regulate use or disclosure of personal information without consent,[88] allow operators to satisfy regulatory requirements by following guidelines set by private groups,[89] or preempt more restrictive state regulation.[90]

The October, 2000 hearing outlined the political debate on privacy regulation.[91] Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, a consumer privacy group, advocated favor strong "baseline" protections, consistent with the above arguments about market failure. Jerry Berman, Executive Director of the Center for Democracy and Technology, said that "a hapless patchwork of policies in this border-less medium will confuse consumers, frustrate businesses, complicate enforcement and in the end fail to provide strong privacy protection." George Vradenburg, III, AOL's Senior Vice President for Global & Strategic Policy, indicated the industry's concern with proliferating state law standards and preference for federal

---

[85] For a discussion and evidence of how state laws can overcome network externalities, *see* Ribstein & Kobayashi, *supra* note 80.

[86] *See, e.g.,* Consumer Onliine Privacy and Disclosure Act, 2001 U.S. H. 347.

[87] *See, e.g.,* 1999 U.S. S 2606 (opt-in for personally identifiable information, opt-out for other non-personally identifiable information. Special rules for book and video (opt-in) and cable and satellite (opt-out); 1999 U.S. H 5430 (opt-out); 1999 U.S. S. 3180 (opt-in).

[88] *See, e.g.,* 1999 U.S. H. 2882.

[89] *See, e.g.,* 1999 U.S. H. 3560, 1999 U.S. S. 809, 1999 U.S. S. 2928.

[90] *See infra* discussion accompanying note 178.

[91] *See Privacy Hearing*, *supra* note 3.

preemption of inconsistent state law. However, Rotenberg opposed preempting the state regulatory tool. Berman, an advocate of promoting the Internet as an open medium, was concerned about rules that would restrict entry by new and small businesses. Witnesses further disagreed about such specifics as whether the rules should require affirmative consumer opt-in (with Rotenberg favoring opt-in and Vradenburg opposing it).[92]

As indicated above, the tradeoffs involved in regulating privacy are still unclear enough to make definitive regulation risky even by the best-motivated legislators. This Part shows that it is better to rely on state regulation. State law allows for a variety of approaches and facilitates legal experimentation and evolution as well as competition among diverse regimes. It also promotes individual over collective choice by permitting consumers, by shopping among websites, to vote with their mice for the regulatory regime they want to apply.

A. POTENTIAL ADVANTAGES OF STATE OVER FEDERAL LAW

1. Exit and political discipline

Legislation may favor the interest groups that can organize most cheaply and effectively to raise and spend money, or to mobilize votes and other political resources.[93] Since a successful interest group's gains reflect its organization costs, these gains may not outweigh losses to the rest of society. Interest group dynamics at the federal level may lead to stringent regulation of consumer marketing information. Larger and more established website operators may favor disclosure and monitoring burdens that would restrict entry into the industry. This meshes with the interests of privacy advocates who place a high value on consumer control over marketing information. Consumer and privacy advocates would favor legislation that heightens public awareness of the privacy issue and thereby increases the demand for these groups' lobbying activities. And established players such as AOL may want federal regulatory standards suitable to a closed architecture or at least prefer federal preemption of burdensome state regulation to an open Internet. Mostly lost in this mix are those who would tend to oppose strict regulation, including low-margin operators and potential new entrants who are hurt most by regulatory burdens, and consumers who prefer convenience to disclosure screens and "I accept" boxes.

Although interest groups operate at the state level as well, here the social costs of legislation are constrained by individuals' opportunities to exit undesirable regimes.[94] Charles Tiebout recognized that people decide on their preferred levels of taxes and expenditures by voting with their feet.[95] Any interest group compromise at the state level

---

[92] Industry also opposes strong access rights by consumers, arguing that such rights would invite corruption of the data by hackers and others. *See* Cha, *supra* note 2.

[93] *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1971); ROBERT E. MCCORMICK & ROBERT D. TOLLISON, POLITICIANS, LEGISLATION AND THE ECONOMY (1981); Robert D. Tollison, *Public Choice and Legislation*, 74 VA. L. REV. 339, 361-62 (1988).

[94] *See* Richard A. Epstein, *Exit Rights under Federalism*, L. & CONTEMP. PROBS., Winter 1992, at 147.

[95] Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416 (1956). *See*

faces competition with the laws of fifty other jurisdictions operating on the level playing field set by the Constitution. By contrast, competition between U.S. federal law and that of other countries is constrained by the costs of dealing with different legal systems, languages and infrastructures. The significant potential for exit in the U.S. federal system can force state lawmakers to consider the public interest in order to avoid losing clientele.[96] Exit is a potentially more effective disciplinary mechanism than the political process because it operates through individual choice rather than the need to coordinate through interest groups. As exit costs fall, as by letting people contract for the applicable law rather than having to physically move from one jurisdiction to another, so does the effect of inefficient laws. For example, because firms easily can choose their states of incorporation, state corporation law has been described as "trivial.'[97]

2. Variation and individual preferences

Whether or not state competition effectively disciplines interest groups, relying on state law would enable individuals to select the regulatory regime that best fits their needs. By contrast, federal law would foreclose many of their options. For example, all of the proposed bills discussed above assume that consumers should have strong rights to consent to use of consumer marketing information, that firms should be required to make detailed disclosures about use of the information, and that any rules should be backed by legal liability. Passing any of these bills would take off the table issues concerning the costs and benefits of disclosure and consent for individual consumers and different types of information. One-size-fits-all disclosure and consent methods would preclude the development of technologies that permit customization of disclosure and use practices according to individual preferences.

3. Experimentation and evolution

Even if a single uniform law ultimately proves to be desirable, that law should not be imposed at the federal level until state experimentation identifies the best approach.[98] Once federal law is imposed, Web architecture and industry practices necessarily would follow, thereby making change costly. Evolutionary theories suggest that efficient laws may emerge even if state legislators are not knowingly competing.[99] Individuals and

---

also Bruno S. Frey & Reiner Eichenberger, *Competition among Jurisdictions: The Idea of FOCJ, in* COMPETITION AMONG INSTITUTIONS, 209 (L. Gerken, ed.) (1995); Luder Gerken, *Institutional Competition: An Orientative Framework, in* Gerken, *supra,* at 1; Wolfgang Kerber & Viktor Vanberg, *Competition among Institutions: Evolution within Constraints, in* Gerken, *supra* at 33.

[96] *See* Frank H. Easterbrook, *Antitrust and the Economics of Federalism*, 26 J. L. & ECON. 23 (1983); Daniel R. Fischel, *From MITE to CTS: State Anti-Takeover Statutes, the Williams Act, the Commerce Clause, and Insider Trading*, 1987 SUP. CT. REV. 47; Tiebout, *supra* note 95.

[97] *See* Bernard S. Black, *Is Corporate Law Trivial?: A Political and Economic Analysis*, 84 NW. U. L. REV. 542 (1990).

[98] *See* Jack Goldsmith & Alan Sykes, *The Internet and the Dormant Commerce Clause*, Chicago Olin Working Paper (2d) no. 105 at 29-30 (http://papers.ssrn.com/paper.taf?abstract_id=246100) (discussing benefits of state experimentation).

[99] *See* Armen Alchian, *Uncertainty, Evolution, and Economic Theory*, 58 J. POL. ECON. 211 (1950) (observing that a study of the "adaptive mechanism" of the market may be more fruitful than that of "individual motivation and foresight").

firms who have an incentive to minimize their transaction and information costs and an ability to choose legal regimes that accomplish this goal over time may cause the law to move toward efficiency, if only because inefficient regimes end up governing fewer and fewer people and transactions.[100]

4. Interaction between federal and state law

Although federal law may rationalize diverse state laws, it also may introduce confusion within individual states. The state law of contract governs consumers' interactions with web vendors. Every state has law that may cover consumer marketing information, including, as discussed above in subpart I(A), the common law of tort, privacy regulation, and regulation of deceptive transactions. Adding a federal regulatory structure to the mix raises potentially difficult issues concerning the extent to which the state law is preempted and, if not, how the regulatory schemes interrelate. By contrast, any new state regulation of consumer marketing information can be tailored for each state's existing regulatory system.

B. THE PROBLEM OF DETERMINING THE APPLICABLE LAW

A website's simultaneous accessibility in all states raises questions about the viability of state law in addressing Internet privacy. Some believe that conventional territorial-based methods of regulating are inappropriate for the Internet. Most prominently, Johnson and Post claim that territorial-based restrictions will lead to each jurisdiction's attempting to regulate the entire web, so that cyberspace itself should be considered a distinct regulatory jurisdiction.[101] But state regulation of the web is not so hopeless. As discussed below, under U.S. jurisdiction rules a state cannot regulate web transactions based solely on the local accessibility of the website. Moreover, in determining the applicable state law, a court needs to sort through only a limited number of options, and must evaluate only the sufficiency of the local basis for regulating rather than the claims of all states that can exercise jurisdiction.[102]

The main problem with state regulation of the Internet is not that states have potentially unlimited reach, but that any limits only make the choice of law problem tractable for courts *ex post*, after a dispute arises. Default conflict-of-law rules, coupled with vague rules on state jurisdiction, do not enable individuals to choose among competing jurisdictions at the time of the transaction. This impedes parties' ability to choose the law that is most efficient or that best fits their situation, thereby undercutting the benefits of state law just discussed. These problems will be discussed below in this subpart. As shown below in this Part, the argument for state law depends partly on the

---

[100] There is also evidence of such evolution with respect to the demand for statutory forms. *See* Bruce H. Kobayashi & Larry E. Ribstein, *Evolution and Spontaneous Uniformity: Evidence from the Evolution of the Limited Liability Company*, 34 ECON. INQ. 464 (1996).

[101] *See* Johnson & Post, *supra* note 56 at 1379. This problem attained a global dimension with a French court's recent order that U.S.-based Yahoo must install a system blocking French users from accessing Nazi memorabilia on Yahoo or face stiff daily fines. *See* Mylene Mangalindan and Kevin Delaney, *Yahoo! Ordered To Bar the French From Nazi Items*, WALL ST. J., November 21, 2000, at B1, 2000 WL-WSJ 26617563.

[102] *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1235, 1237 (1999).

enforcement of contractual choice of law.[103]

1. Conflict-of-laws

In the absence of agreement on the applicable law, the Second Restatement of Conflicts applies an indeterminate approach that depends on weighing a variety of facts in the particular case. If use of consumer marketing information is considered a breach of contract, the applicable law would depend on place of contracting, negotiation of the contract, performance, subject matter, and domicile, residence, nationality, place of incorporation and place of business of the parties,[104] weighed in light of such general considerations as the parties' expectations and the policies of the forum and other interested states.[105] If merchants' use of consumer marketing information is considered a tort invasion of privacy, the applicable law may be that of the state where the defendant communicated the information and thereby appropriated the plaintiff's name or likeness, or the plaintiff's domicile if the invasion is deemed to occur in multiple states.[106]

These rules obviously could support application of the buyer's local law in many cases involving consumer marketing information. For example, if the court deems use of the information a breach of contract it might reason that placing a cookie on a consumer's computer locates the performance, subject matter, one of the parties, and perhaps contracting and negotiation in the consumer's state. If sale of a consumer marketing information database is considered a tort breach of privacy, the applicable law may be that of the plaintiff's domicile, the purchaser's location, or some other place.

The Constitution only loosely checks state courts' selection of the applicable law. *Allstate Insurance Co v. Hague* held as a matter of due process and full faith and credit that Minnesota, where the decedent worked, widow resided and insurer did business, could apply its rule "stacking" uninsured motorist coverage on the insureds' vehicles rather than the different Wisconsin rule where the policy was issued and the insured resided, reasoning that Allstate would not be unfairly surprised by the application of Minnesota law.[107] An expectations-based test provides little predictability as long as the parties' expectations can be shaped by the choice-of-law rules the courts happen to apply.

---

[103] For general discussions, *see* Committee on Cyberspace Law, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet,* 55 BUS. LAW. 1801 (2000) ("*Order in Cyberspace*"); Jermyu Gilman, *Personal Jurisdiction and the Internet: Traditional Jurisprudence for a New Medium*, 56 BUS. LAW. 395 (2000).

[104] RESTATEMENT (SECOND) OF CONFLICT OF LAWS §188(2) (1971).

[105] *Id.* §6.

[106] *See id.* §152 and comment c (stating that law of place of invasion applies unless some other state has more significant relationship under §6); §145(f), 153 (noting importance of plaintiff's domicile in multistate cases).

[107] 449 U.S. 302. 318, n. 24 (1981). Justice Stevens, concurring, said that the parties' expectations are significant under the Full Faith and Credit Clause, *id* at 324 n.11, and suggested that the Due Process Clause would raise fairness concerns if the parties had made their expectations explicit by providing for application of a particular law, *id.* at 328-29.

The dormant Commerce Clause might play some role in choice of law.[108] Applying inconsistent state regulations to website operators based on minimal jurisdictional contacts can significantly burden multi-state Internet operations. Courts have cited such problems in invalidating on commerce clause grounds state statutes regulating conduct on the Internet.[109] However, state regulation does not violate the dormant commerce clause merely because it might have out-of-state effects. Rather, courts should, and in effect do, balance any costs imposed on out-of-state parties against the local harms the statute is intended to redress.[110] Courts must analyze costs and benefits of consumer marketing information regulation in light of the available and potential technology, including website operators' ability to block access to their website by users in particular states, and users' ability to configure their browers to avoid intrusive websites.[111] Thus, the application of the dormant commerce clause to consumer marketing transactions may depend on how easily website operators can restrict access to their sites in states where their websites are illegal, whether application of the law takes such efforts into account, and on whether customers can cheaply avoid dealing with companies whose privacy policies they do not like. In other words, Constitutional constraints may not be justified under a balancing test for the same reasons that state law is ultimately likely to produce efficient results, as discussed below in this Part.

2. Jurisdiction

The applicable state law is determined not only by conflict-of-laws rules but also by where the plaintiff can obtain personal jurisdiction over the defendant. The due process clause permits the state to assert jurisdiction over only those parties who have had minimum contacts with the state.[112] In general, the defendant must direct its action toward the forum rather than merely being aware that action might result there.[113] Once a

---

[108] *See* Larry E. Ribstein, *Choosing Law By Contract*, 18 J. CORP. L. 245, 287-94 (1993).

[109] For cases invalidating statutes prohibiting distribution of obscene material to minors on the Internet, *see* ACLU v. Johnson, 194 F.3d 1149 (10th Cir. 1999); American Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997) (reasoning that the Internet "must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether"). *But see* Hatch v. Superior Ct., 79 Cal.App.4th 663, 94 Cal.Rptr.2d 453 (2000) (California statute did not violate Commerce Clause because statute did not punish conduct outside of California).

[110] *See* Goldsmith & Sykes, *supra* note 98.

[111] This technology is discussed *supra* note 59 and *infra* note 163 and accompanying text.

[112] *See generally* World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980); International Shoe Co. v. Washington, 326 U.S. 310 (1945).

[113] Asahi Metal Industry Co v Superior Court, 480 US 102 (1987). A court may assert general jurisdiction over a defendant that has extensive local contacts such as maintaining a principal place of business even if the contacts did not arise out of or relate to the particular transaction at issue. See Helicopteros Nacionales De Columbia, S.A. V. Hall, 466 US 408 (1984). Merely selling through a website into a forum is clearly insufficient for this purpose. See DEC v. Altavista Technology, Inc., 960 F. Supp. 456 (D. Mass. 1997). *See also* Coastal Video Communications, Corp. v. Staywell Corp., 59 F. Supp. 2d 562 (E.D. Va. 1999) (holding no specific jurisdiction in Virginia for declaratory judgment action by out of state plaintiff based on accessibility of defendant's interactive website in Virginia, although general

state with jurisdiction enters judgment, the judgment may be enforced in any state where the defendant has assets.[114]

Internet jurisdiction has gone through three phases. A few courts initially held that a state could exercise jurisdiction merely on the basis that a website was broadcast into the state.[115] However, courts now generally deny personal jurisdiction based merely on a receiver's downloading.[116] In the second phase of Internet jurisdiction cases, the courts focused on the degree of interactivity of the website in the relevant jurisdiction.[117] Several cases have based jurisdiction primarily or exclusively on the maintenance of an interactive website that can take orders.[118]

In the third phase, a defendant may be able to escape jurisdiction in a state if it has not "targeted" that jurisdiction or has targeted its conduct elsewhere. The leading case suggesting this approach, *GTE New Media Services, Inc. v. Bellsouth Corp.*, reasoned that due process requires predictability, analogizing web access to an out-of-state telephone call which had been held not to trigger long-arm jurisdiction, and distinguishing cases involving activities directed toward the forum that had held in favor of minimum contacts.[119] In one of these cases, *CompuServe, Inc. v. Patterson*,[120] the

---

jurisdiction might be supported by proof the website was accessed by many residents in the forum, indicating continuous and systematic contacts).

[114] *See* Full Faith and Credit clause, US Const, Art IV, § 1.

[115] *See* Inset Systems, Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996); Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996) (basing jurisdiction on defendant's decision to transmit advertising information to all Internet users). The Virginia Internet Privacy Act pushes this approach to its outermost reach providing for jurisdiction in Virginia based merely on routing of email or other Internet transmissions through Virginia. *See* VA. CODE ANN. § 8.01-328.1. While this may be a boon for local Internet service providers, particularly including AOL, who want to sue remote users of their service, it is probably unconstitutional under the more restrictive approaches to jurisdiction discussed in the text below. ISP's probably are better off relying on contractual consent-to-jurisdiction clauses. *See infra* note 141 and accompanying text.

[116] *See* Bensusan Restaurant Corp. v. King 937 F. Supp. 295 (S.D.N.Y. 1996), aff'd 126 F.3d 25 (2d Cir. 1997) ("[t]he mere fact that a person can gain information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product in New York."); Goldsmith, *supra* note 102 at 1216-21.

[117] *See* Cybersell, Inc. v. Cybersell, Inc 130 F 3d 414 (9th Cir. 1997) (holding that the court should look to the level of interactivity and analyze contacts in the jurisdiction; in the present case site invited visitors to submit name to get more info; passive web operation not enough); Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997) (for interactive website, the court must determine the degree and nature of the information exchange through the site).

[118] *See* Park Inns Intern., Inc. v. Pacific Plaza Hotels, Inc., 5 F. Supp. 2d 762 (D. Ariz. 1998), (website could take hotel reservations); Stomp, Inc. v. NeatO, LLC, 61 F. Supp. 2d 1074 (C.D. Cal. 1999) (website permitted a small number of on-line sales); Online Partners.Com, Inc. v. Atlanticnet Media Corp., 2000 WL 101242 (N.D. Cal. 2000) (website permits online subscriptions); Citigroup Inc. v. City Holding Co., 97 F. Supp. 2d 549 (S.D.N.Y. 2000), (website permitted customers to apply for loans on-line, print out applications for fax submission, click on a "hyper link" to "chat" on-line with a representative of defendants and e-mail defendants with home loan questions with a quick response from an online representative).

[119] 199 F. 3d 1343, 1349-50 (D.C. Cir. 2000).

defendant had contracted with a locally-based computer network to market his software, which he electronically sent to the state. In the other, *Panavision International, L.P. v. Toeppen,*[121] a "cybersquatter" who allegedly stole defendant's trademarks engaged in conduct that had effects in the relevant state, California, which was the trademark owner's principal place of business and the heart of the motion picture and television industry. It has been said that *GTE* endorses a "strict purposeful availment standard," and that "[b]ecause defendants can control whether they engage in activities targeted toward a specific forum, it is easier for them to predict whether a court will find that they have done so than to predict whether a court will label their websites as sufficiently interactive to warrant jurisdiction."[122] Some other cases include hints of a targeting standard.[123]

The ABA Committee on Cyberspace Law has recommended a targeting limitation based on devices sponsors use to purposefully avail themselves of states' commercial benefits, or that they use to avoid jurisdictions, such as blocking and screening, disclaimers, identification of their home state, listing targeted or non-targeted destinations and, more generally, controlling how goods are advertised, sold, and shipped.[124] Restrictions on jurisdiction also may take into account the availability of bots, or intelligent agents, that consumers can program to prevent access to particular sites, aided by sellers' electronic agents and global protocol standards.[125]

In general, although the law is still developing, the trend in jurisdiction law is toward viable limits on state law's reach. Technology and flow-control will determine the meaning of minimum contacts in cyberspace, and ultimately may erect electronic borders that make personal jurisdiction in cyberspace comparable to that in real-space.[126] As discussed below, they also may bolster the effectiveness of contractual choice of law and forum.

---

[120] CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996).

[121] 141 F.3d 1316 (9th Cir.1998).

[122] See Note, *Civil Procedure--D.C. Circuit Rejects Sliding Scale Approach To Finding Personal Jurisdiction Based on Internet Contacts,* 113 HARV. L. REV. 2128, 2133 (2000).

[123] *See* Roche v. Worldwide Media, Inc., 90 F. Supp. 2d 714 (E.D. Va. 2000) (though website solicited customer e-mail addresses and credit card numbers, no evidence that products were sold in Virginia or that any advertising or other promotional activity was directed specifically to Virginia); Rannoch, Inc. v. Rannoch Corp., 52 F. Supp. 2d 681 (E.D. Va. 1999) (denying jurisdiction in infringement case, where website included section for ads that could be placed on line, though no sales on line, stating that "[t]here was no evidence that the defendant had any dealings with any Virginia resident, placed any classified ads on its Website for products or persons in Virginia, did any business in Virginia, or conducted any advertising or other promotional activity specifically directed to Virginia."). *Cf.* Uncle Sam's Safari Outfitters, Inc. v. Uncle Sam's Army Navy Outfitters-Manhattan, Inc., 96 F. Supp. 2d 919 (E.D. Mo. 2000) (holding that disclaimer re sale of merchandise in Missouri is unavailing because it was posted after the commencement of the suit).

[124] *See Order in Cyberspace, supra* note 103 at 1821, 1881. For example, a website might announce exclusion operator might post a notice excluding residents of certain countries. *Id* at 1892.

[125] *Id*. at 1879, 1893-94. *See also* the discussion of P3P, *supra* text accompanying notes 57-58.

[126] *See* Goldsmith, *supra* note 102 at 1218-19. *See also id.* at 1226-7.

C. A CONTRACTUAL SOLUTION TO CONFLICT OF LAWS

The above rules do not necessarily let merchants and consumers jointly determine the applicable rules at the time of their transaction, when the winners and losers from a particular rule have not yet been determined and when knowledge of the law could shape the parties' conduct. Rather, they let consumers choose the law unilaterally at the time of injury by picking a forum, which in turn has substantial latitude in picking local law. Under this approach, states have incentives to respond to consumers' or trial lawyers' interests rather than to maximize the contracting parties' joint wealth.[127] This subpart discusses an important additional tool that can work to further the efficient evolution of state law: website operators' ability contractually to select the applicable forum, adjudicator and law. Enforcing these clauses maximizes the welfare of all affected parties rather than just of the one who happens to sue.

More specifically, under our proposal, merchants might condition use of their websites on the consumers' acceptance of the designated law and forum.[128] Such a clause was enforced in the consumer marketing information context:

> This License Agreement shall be governed by the laws of the State of Washington, without regard to conflicts of law provisions, and you hereby consent to the exclusive jurisdiction of the state and federal courts sitting in the State of Washington. Any and all unresolved disputes arising under this License Agreement shall be submitted to arbitration in the State of Washington.[129]

The contract might be entered into by placing the clause in a general "terms of use" section of the website, or by making acceptance of the clause a condition of entering the website.[130] Alternatively, states might offer firms the opportunity to select their laws through a procedure analogous to incorporation or formation of other types of business

---

[127] Thus, the problem is not simply that the rules are unclear. Rather, even clear rules that always apply the forum rule and that the consumer can obtain jurisdiction anywhere over the merchant would present the same problems. *See* Erin A. O'Hara & Larry E. Ribstein, *From Politics to Efficiency in Choice of Law*, 67 U. CHI. L. REV. 1151, 1187-90 (2000).

[128] Merchants' designation of the applicable law does not necessarily make the contract one-sided or unenforceable, consistent with the general analysis of so-called "adhesion" contracts. *See supra* note 65 and accompanying text. Consumers, in effect, vote with their mice for the applicable law and forum by contracting with the seller or website operator. Consumers also could try to contract for an alternative regime or for no contractual choice (i.e., for the default conflict-of-law rule), perhaps by using an automatic contracting mechanism such as P3P. Merchants could charge more to contract under regimes that favor consumers or to cover the extra transaction costs of customized contracting. However, given these extra costs, consumers probably will either accept or reject the forms merchants offer, as with other adhesion contracts. Note that state enforcement of *contractual* choice justifies emphasizing the buyer's state under *default* conflict-of-laws rules because sellers would be in the best position to contract around the default. *See* O'Hara & Ribstein, *supra* note 127 at 1201.

[129] *See* Lieschke v. RealNetworks, Inc., 2000 WL 198424 (Feb. 11, 2000, N.D.Ill.), additional opinion, 2000 WL 631341 (May 8, 2000, N.D.Ill.), discussed *infra* text accompanying note 151.

[130] As discussed below, the forum in which the plaintiff sues initially will determine the enforceability of the contract, including the law applicable to determining enforcement, as well as how to deal with any information the website has gathered before visitors reasonably could contract with the operator. However, a choice-of-forum clause may influence these determinations.

associations. Thus, a Virginia bill proposed permitting firms to "domesticate" their websites in Virginia by making a local public filing, and thereby effectively to disclaim certain types of liabilities.[131]

Contractual jurisdictional choice addresses the most significant problems inherent in diverse state laws. These contracts are particularly useful in dealing with state regulations that, for example, restrict use of consumer information even with disclosure, require onerous disclosures or consent procedures, significantly limit changes in policy, impose costly consumer access requirements, or provide for draconian liability.[132]

It is important to emphasize the importance of contracting not only for the applicable law, but also to require disputes to be tried in the state whose law is selected and that the parties consent to the jurisdiction of this court. The forum ultimately will decide which law will be applied.[133] Although a court in which plaintiff sues theoretically can decide not to enforce a choice-of-forum clause, it may be willing to defer to the contractual selection of a different forum even if it would not be willing to apply another state's law.[134] While a judge may face difficulty without much reward from making new law when applying another state's law, enforcing a choice of forum clause lets a court both enforce the contract and avoid directly contravening legislative policy or establishing a potentially troublesome precedent on contractual choice of law. Thus, contractual choice of forum helps courts resolve conflicting incentives regarding enforcement of contractual choice of law.

The contract also might adopt a private regulatory regime or provide for arbitration.[135] Again, a court may be willing to permit arbitration even if it would not enforce contractual choice of law. Although state judges have incentives to enforce local law because their tenure, salary and perks are controlled by state legislatures,[136]

---

[131] *See* 2000 VA S. 767.

[132] On the other hand, merchants may be able to design a single web page that complies with diverse but reasonable state disclosure requirements. Note that contractual choice of law and forum does not effectively permit the choice of no regulation -- that is, where states hold that consumers have no rights in the information would permit merchant use of the information without consent or disclosure. In this situation, contracting for law or forum would require consent and disclosure requirements where none otherwise would be required. However, if allocating no rights to consumers is efficient, states may evolve toward that result, thereby making contractual choice unnecessary.

[133] Thus, the contractually selected law and forum generally will be the same, although theoretically they can differ. In other words, a forum may be selected because of its law or vice versa. *See* Bruce H. Kobayashi & Larry E. Ribstein, *Contract and Jurisdictional Freedom,* in THE FALL AND RISE OF FREEDOM OF CONTRACT (F.H. Buckley, ed. Duke, 1999).

[134] Courts have the alternative of dismissing on forum non conveniens grounds or, in federal court, transferring the case to the jurisdiction whose law is chosen. *See* Note, *Forum Non Conveniens as a Substitute for the Internal Affairs Rule,* 58 COLUM. L. REV. 234 (1958).

[135] *See* Goldsmith, *supra* note 102 at 1246-9 (arguing for solving many problems through international arbitration operating through contract, national arbitration law, international enforcement treaty).

[136] *See* Gary M. Anderson, et al. *On the Incentives of Judges to Enforce Legislative Wealth*

arbitrators have less incentive to resist evasion of state regulation because they are paid by the parties rather than by the state.

There is an important relationship between contracting over the forum and contracting for private remedies. States may regulate Internet transactions whether or not the parties want to deal with the problem only in cyberspace. A consumer or regulator therefore may circumvent attempted contractual privatization by suing in a state that is likely to apply its strong regulatory policy. Thus, firms effectively can contract for private rather than government rules and adjudication only by contractually designating a state forum that respects private remedies. Accordingly, our proposal for enforcing contractual choice of state law and forum does not mean that we prefer government to private ordering, but rather provides a way to make private remedies viable. We do not necessarily disagree with Johnson & Post's arguments for private regimes operating and competing in cyberspace.[137]

Current law appears to give courts significant leeway not to enforce jurisdictional choice. As summarized in *Restatement (Second) of Contracts,* §187(2), courts may not enforce contractual choice of law clauses as to the validity of the contract where:

> (a) the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice, or
>
> (b) application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which, under the rule of §188, would be the state of the applicable law in the absence of an effective choice of law by the parties.[138]

The first exception may restrict shopping for the applicable law in some cases by requiring a connection with the chosen jurisdiction. The second limitation can operate to prevent evasion of state regulation.

However, there is significant support for enforcement of jurisdictional choice. First, courts applying the *Restatement* rule have quite generally enforced contractual choice of law, at least in commercial contracts.[139] Moreover, several states, including California, Illinois, Delaware, New York and Texas, have promulgated statutes that, to

---

Transfers, 32 J. L. & ECON. 215 (1989); W. Mark Crain & Robert D. Tollison, *Constitutional Change in an Interest Group Perspective,* 8 J. LEGAL STUD. 165 (1979) and *The Executive Branch in the Interest-Group Theory of Government,* 8 J. LEGAL STUD. 555 (1979); William M. Landes & Richard A. Posner, *The Independent Judiciary in an Interest Group Perspective,* 18 J. L. & ECON. 875 (1975).

[137] *See* Johnson & Post, *supra* note 56, at 1399, n. 102.

[138] *See* RESTATEMENT (SECOND) OF CONFLICTS, §187(2) (1971).

[139] *See* Ribstein, *supra* note 108; Symeon C. Symeonides, *Choice of Law in the American Courts in 1997,* 46 AM. J. COMP. L. 233, 273 (1998). Cases involving the consumer context involved in consumer marketing information cases are noted in *infra* note 174 and accompanying text. Thus, the U.S. rule in practice resembles the apparently more liberal rule in the leading U.K. case of Vita Food Products Inc. v. Unus Shipping Co. 1939 A.C. 277(enforcing a provision applying English law to a transaction whose only connection with England was the choice-of-law clause).

varying degrees, clarify the enforcement of contractual choice-of-law clauses.[140]

Second, courts have enforced choice-of-forum clauses. U.S. Supreme Court cases have recognized the enforceability of consent to jurisdiction,[141] and forum-selection[142] clauses even in "adhesion" contracts between merchants and consumers[143] despite commentary claiming that no "real" contract is involved in these cases.[144] Although the Supreme Court was deciding constitutional issues or admiralty cases rather than applying state law, the cases are important general authority for enforceability. The Reporter's Note to the Uniform Computer Information Transaction Act adopts the Supreme Court's permissive approach to enforcing choice of forum clauses, noting that the choice "is not invalid simply because it has an adverse effect on a party, even if bargaining power is unequal" and that "[i]n an Internet transaction, choice of forum will often be justified on the basis of the international risk that would otherwise exist. Choice of a forum at a party's location is reasonable."[145]

Third, with respect to arbitration clauses, Section 2 of the U.S. Federal Arbitration Act[146] mandates enforcement of arbitration agreements involving transactions in interstate commerce. Consistent with its approach to choice of forum, the Supreme Court has been very receptive to enforcement of arbitration clauses even in cases involving important federal rights.[147] In a frequently cited case Judge Easterbrook held in favor of enforcement of an arbitration clause in a contract included with a Gateway computer.[148] The ABA's Committee on Cyberspace Law has recommended enforcement of non-

---

[140] Larry E. Ribstein, *Delaware, Lawyers and Choice of Law*, 19 DEL. J. CORP. L. 999, 1003-06 (1994).

[141] *See* National Equipment Rental, LTD. v. Szukhent, 375 U.S. 311 (1964); Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985).

[142] *See* Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585 (1991); M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1 (1972).

[143] *See* Carnival Cruise Lines, *supra* note 142 (enforcing choice of forum clause on passenger ticket).

[144] *See generally* Paul D. Carrington & Paul H. Haagen, *Contract and Jurisdiction,* 1996 SUP. CT. REV. 331. The efficiency of adhesion contracts is discussed *supra* note 65 and accompanying text.

[145] *See* UNIF. COMPUTER INFORMATION TRANSACTIONS ACT (Draft for Approval at NCCUSL Meeting, July 23-30, 1999), §110, Reporter's Notes 2-4 *available at* <http://www.2bguide.com/drafts.html>.

[146] 9 U.S.C. §2.

[147] *See, e.g.,* Gilmer v. Interstate/Johnson Lane Corp., 111 S.Ct. 1647 (1991) (employment discrimination); Rodriguez de Quijas v. Shearson/American Express Inc., 490 U.S. 477 (1989) (securities law claim).

[148] *See* Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir.), *cert. denied,* 522 U.S. 808 (1997). For applications of *Hill* in the same context, *see* Westendorf v. Gateway 2000, Inc., 2000 WL 307369 (Del. Ch., March 16, 2000); Brower v. Gateway 2000, Inc., 246 A.D.2d 246, 676 N.Y.S.2d 569 (1998). Cases specifically involving clickware contracts are discussed below in this subpart.

binding arbitration clauses that call for enforcement of awards pursuant to adequately disclosed choice of forum and law and jurisdictional choices where the consumer has "demonstrably bargained with the seller" or if the contract was made through a bot programmed to reflect the consumer's choices.[149] The Committee notes that the Internet market makes such contracting desirable and viable because, among other things, it gives web buyers more options and often involves contracts between consumers and relatively small firms, and concludes that US courts are likely to defer to choice of law and forum contracts that are not unconscionable.[150]

Judicial recognition of jurisdictional choice has been extended to clickware-type Internet contracts. An important recent case involving consumer marketing information is *Lieschke v. RealNetworks, Inc.*,[151] in which the court enforced contractual arbitration in defendant's home state of customers' claims of trespass to property and privacy based on RealNetworks' use of its products to access users' electronic communications and stored information without their knowledge or consent. Before installing the software users were required to accept RealNetworks' license agreement providing that Washington law governed and that users consented to exclusive jurisdiction and arbitration in state and federal courts in Washington. The court interpreted this as applying the law of the Seventh Circuit (the forum) as to arbitrability, which is notably favorable to enforcement of computer and software agreements,[152] rather than the less pro-enforcement law of the Ninth Circuit, where the contractually selected forum was located.[153] It also rejected an intervenor's unconscionability arguments based on the location of the agreement, the size of the font, difficulty of use, distance of the designated forum from some users' homes, and the failure to provide for class-wide arbitration.[154]

Contractual choice of law and forum has been enforced in other types of Internet transactions. New Jersey residents injured in defendant's Nevada hotel had to go to Nevada for trial under a clause entered into on defendant's website providing for trial in Nevada state and federal courts.[155] The forum selection clause helped justify holding against jurisdiction in New Jersey, the court reasoning in part that "[t]he forum selection clause in defendant's Website demonstrates that it could not reasonably anticipate being haled into court in New Jersey." Contractual choice of Ohio law was enforced in a

---

[149] *See Order in Cyberspace*, *supra* note 103 at 1822, 1893.

[150] *Id.* at 1829, 1832 (noting internet sellers' ability to confine market and wider buyer options on the web), 1894.

[151] 2000 WL 198424 (Feb. 11, 2000, N.D.Ill.), additional opinion, 2000 WL 631341 (May 8, 2000, N.D.Ill.).

[152] *See supra* note 148.

[153] 2000 WL 631341 at 5 (May 8, 2000, N.D.Ill.). Citing the presumption of arbitrability under the Federal Arbitration Act, the court held that plaintiffs' non-contract arguments were those "arising under" the agreement pursuant to the arbitration clause, and rejected their arguments that they should not be required to arbitrate because of the high cost of arbitrating individual claims. 2000 WL 198424 (Feb. 11, 2000, N.D.Ill.).

[154] 2000 WL 631341 at 5-7.

[155] Decker v. Circus Circus Hotel, 49 F. Supp. 2d 743, 750 (D.N.J. 1999).

declaratory judgment action on an Internet transaction based on repeated interactions between an Ohio computer network and a customer who agreed to market his product over defendant's system.[156]

Enforcement of contractual choice of law in the consumer marketing information context is generally consistent with the approach of UCITA §109(d) to computer information sales, which would enforce a choice of law clause in electronic consumer sales unless it would vary a mandatory rule in the *licensor's* state.[157] Significantly, UCITA drops the "reasonable relationship" requirement under the general Restatement rule for enforcing contractual choice of law. The UCITA Reporter's Notes state that in a "global information economy, limitations of that type are inappropriate and arbitrary" and cite the costs of complying with the inconsistent laws of many jurisdictions as the reason for mandating application of the law of the licensor's state in electronic transactions.[158] Although the rule holds licensors to regulation in their own states, they can escape stringent rules by locating in permissive states.

Thus, contractual choice of law, forum and arbitration is generally enforced, including in computer transaction cases. Although enforcement is not assured,[159] choice of law and forum contracts mitigate problems with default conflict-of-laws rules that otherwise would reduce state law's usefulness in regulating consumer marketing transactions.[160]

---

[156] CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996).

[157] More specifically, the provision enforces the contract except where it varies a mandatory rule, in which event it applies the default rule under §109(b), which in turn applies the law of the licensor's state in electronic transactions. *See* Bruce H. Kobayashi & Larry E. Ribstein, *Uniformity, Choice of Law and Software Sales*, 8 GEO. MASON L. REV. 261 (1999). Note that a trade secret licensing approach to consumer marketing information (*see* Samuelson, *supra* note 1) would bring this information under UCITA.

[158] *See* UCITA, *supra* note 145, §109, Reporter's Note 2.

[159] *See* Klocek v. Gateway 2000, Inc., 104 F.Supp.2d 1332 (D. Kans. 2000) (holding against enforcement because plaintiff did not accept the relevant terms); Thompson v. Handa-Lopez, Inc., 998 F. Supp. 738 (W.D. Tex. 1998) (refusing to enforce contractual choice of California law in a case involving a Texas plaintiff's participation in Internet computer games run by a defendant whose principal place of business and server were located in California). In *Thompson*, the court held that the choice of law clause was not a forum selection clause because, although the contract provided for final and binding arbitration in California, it did not require filing a suit in California. *Id.* at 745. The court added that Texas had a strong interest in protecting its citizens from breach of contract, fraud, and violations of the Texas Deceptive Trade Practices Act that outweighed the defendant's burden created of defending in Texas. *Id.*

[160] Note that enforcement of contractual choice of law may be necessary to preserve privacy regulation from invalidity under the First Amendment. Some cases have recognized First Amendment limitations on regulating Internet privacy. *See* U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (FCC regulation restricting telephone companies' use of customers' personally-identified data unless the customers opted into such use violated the First Amendment because more restrictive than necessary); United Reporting Publ'g Corp. v. California Highway Patrol, 146 F.3d 1133 (9th Cir. 1998), *rev'd sub nom.* Los Angeles Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32 (1999) (invalidating statute authorizing release of arrestees' addresses for "scholarly, journalistic, political, or governmental" but not commercial purposes because it was "directed at preventing solicitation practices"). These limitations have

Given this authority for enforcement of contracts, perhaps the biggest gap in protection for merchants involves actions by state attorneys general, primarily under state consumer fraud statutes.[161] Although these actions would not appear to be constrained by clauses in particular contracts selecting states with less restrictive laws, they do not undercut the case for state rather than federal law. First, unlike private plaintiffs, state attorneys general are subject to political pressure, including those that may arise from merchants' avoiding strict-regulation as discussed below in this Part. Second, and perhaps most important, as discussed in more detail below, federal law not only is unlikely fully to address the problem of state enforcement actions, but may even exacerbate it.

D. AVOIDING NON-ENFORCING STATES

Even if contracting parties cannot be sure that courts will enforce their contractual choice of law or forum, they can avoid giving a non-enforcing or excessively regulating state a jurisdictional predicate for imposing its law, or can reward states with reasonable regulation by investing or paying fees in those jurisdictions. Thus, contractual jurisdictional choice can be made more effective by combining it with physical jurisdictional selection and avoidance. We envision a multistage process involving regulation, contracting and moving in reaction to inefficient regulation and failure to enforce contracts that ultimately can discipline inefficient state attempts to regulate. This process has worked before to constrain inefficient laws, most notably relating to corporations and other business associations and franchise contracts.[162] It is particularly likely to work in the Internet context given the availability of cheap information and the ease and potential mechanization of the contracting process.

First, sellers may be able to block access of their websites at some addresses, including in states that do not enforce choice of law or choice of forum clauses.[163] To the extent that this is fully successful, states would have no basis for exercising jurisdiction under any jurisdiction rule. Even if sellers cannot block their websites from non-enforcing jurisdictions, the targeting tests discussed above may let them avoid jurisdiction in a state if they show that they have taken all available precautions to block

---

been strongly defended. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049 (2000). However, as Professor Volokh recognizes, *contractual* restrictions on consumer marketing information should survive the First Amendment, including statutory restrictions that the parties can contract around. State mandatory rules can be viewed as default rules to the extent that the parties can avoid them by choice-of-law clauses. By this reasoning, enforcement of such clauses may be essential if facially mandatory restrictions on use of consumer marketing information are to withstand First Amendment attack.

[161] *See* Perine, *supra* note 6 (discussing actions by state attorneys general and their opposition to federal regulation).

[162] *See* Kobayashi & Ribstein, *supra* note 133.

[163] Goldsmith & Sykes, *supra* note 98 at 21-22 discuss technology that allows website operators to identify the geographical origin of a user's Internet Protocol address so that they can tailor content to and comply with different jurisdictions' regulations. They note that this technology is more accurate for national origin (99%) than for state origin (80-90%), and that buyers who reside in a regulating state can access a computer with an address in a non-regulating state. *See id.* at 22 (noting that users can frustrate geographical origin technology through America Online's proxy server, Internet anonymizers, and remote telnet and dial up connections). However, this technology is developing and likely to improve, thereby making jurisdictional choice more effective.

access and disclaim the making of an offer there.[164] Sellers who successfully avoid non-enforcing states will, of course, have to forego the benefits of transactions in those states. On the other hand, consumers also incur costs if their state's onerous law cuts them off from numerous websites or forces them to go through extra steps in order to access the sites. Consumers may respond either by lobbying against the regulation or by refusing to support consumer groups' efforts in favor of the regulation.[165]

Second, firms may minimize the possibility that a state's law will apply by avoiding placing significant assets or headquarters there. Even if states can exercise long-arm jurisdiction over remote sellers, the seller's location is relevant for purposes of general jurisdiction[166] and the enforcement of choice of law and choice of forum clauses. As discussed above, the *Restatement* provides for non-enforcement of contractual choice where "the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice" or where the chosen law contravenes a "fundamental policy" of a state that not only "has a materially greater interest than the chosen state" in determining the issue, but that "under the rule of §188, would be the state of the applicable law in the absence of an effective choice of law by the parties." The latter section looks to, among other things, "the domicile, residence, nationality, place of incorporation and place of business of the parties." A seller therefore is better able to secure enforcement of choice-of-law or choice-of-forum clauses over the range of its Internet dealings if it has its home office in the selected state.

These rules may marginally influence some seller location decisions, thereby disciplining states that attempt to impose excessive regulation and encouraging states to regulate moderately. Because Internet firms can connect their servers to the Internet from any location and their assets consist mostly of highly mobile human capital and intellectual property, states easily can attract Internet companies with favorable regulation, and just as easily lose such companies by increasing regulatory burdens.[167] States may respond to these incentives by not stringently regulating consumer marketing information, enforcing contractual choice of law or forum, or applying their regulations only to local consumers rather than to nationwide customers of firms with local contacts. For example, Virginia, which has aggressively sought to become a hub of high-tech or Internet activity, was the first state to enact the generally pro-seller Uniform Computer Information Transactions Act.[168]

---

[164] However, a website operator may be able to avoid jurisdiction in a state with regard to consumer marketing information only by not planting cookies on and taking information from computers in that state.

[165] *See* Kobayashi & Ribstein, *supra* note 133.

[166] *See supra* note 113.

[167] Lawyers, an important interest group, may be influential in persuading states to attract Internet-related business because these firms provide an attractive source of legal business. For a general analysis of lawyers' role in encouraging state competition, *see* Ribstein, *supra* note 140.

[168] *See* Va. Code Ann., tit. 59.1-501.1, et. seq. However, Maryland's subsequent version of UCITA became effective first. Virginia has offered other inducements to Internet firms, including through a long-arm jurisdiction law designed to benefit local Internet service providers such as AOL (*see supra* note 115). *See also supra* text accompanying note 131 (discussing Virginia proposal to permit website domestication).

Analogously, firms have generally avoided locating in the states with the most stringent franchise regulation that fail to restrict application of their laws to residents.[169] Also, insurers have shown that they will pull out of states where regulation constrains profits.[170] The threat of exit in the long run can discipline states' attempts to inefficiently regulate cyberspace beyond their territorial borders, thereby reducing the number of states imposing excessively harsh regulation or the number of firms subject to it.

The same dynamic may cause efficient standardization or uniformity. Forcing web-surfing consumers to confront varying state regulations may be excessively costly. State laws may spontaneously converge on an efficient standard,[171] or a single state law may emerge as a standard as Delaware has in the corporate area. Firms may find that they can comply at relatively low cost with certain types of disclosure and consent rules, while consumers may find that notice and the ability to consent to such rules is advantageous. Firms that select states that impose harsher rules or that do not enact minimal protections will be penalized.

In general, therefore, contractual and physical jurisdictional selection and avoidance can significantly reduce the need for federally-imposed uniformity. Contracts alone may not be enough because of non-selected jurisdictions' incentives to enforce local law. At the same time, physical avoidance and selection may not be enough because these tactics might leave large, multi-state firms exposed to suit in several jurisdictions. But the two strategies together can be a potent constraint on state law. To be sure, neither the governing rules nor state competition is likely to be perfect. For example, firms may be willing to bear significant regulation before they avoid major markets like California and New York. But while state competition may not be fully effective, the question is whether it is likely to produce better laws over time than a federal regime that cuts off any possibility of evolution or competition. Moreover, as discussed below, federal laws are more likely to add a layer of burdensome regulation than to preempt state laws.

E. RACE-TO-THE BOTTOM ARGUMENTS

If firms can effectively shop for state law, will there be a "race to the bottom" that hurts consumers? Similarly, in the corporate context it has been said that states attract incorporation business by exploiting principal-agent problems resulting from the separation of ownership and control.[172] The contrary argument, that corporate law is a

---

[169] *See* Kobayashi & Ribstein, *supra* note 133.

[170] For evidence of the importance of exit as a potential constraint on state regulation, *see* Epstein, supra note 94 at 162-5 (discussing the use of exit taxes used to deter the withdrawal of automobile insurance companies from New Jersey and Massachusetts). *See also Aetna Takes off Gloves on Car Insurance*, Wall Street Journal, A4, (June 7, 1990) (reporting Aetna's challenge of laws in Pennsylvania and Massachusetts that control its exits from these states). For other examples of regulation-induced exit, *see* Wall Street Journal, NW4 (August 16, 2000) (noting exit of health insurance companies from Washington State due to state policies); Wall Street Journal (November 15, 1988) (discussing exit of 40 insurers from California due to Proposition 103 rate rollback); Wall Street Journal (August 10, 1992) (discussing withdrawal of Ohio Casualty Corporation from California Market because of excess regulation and poor underwriting results).

[171] *See* Kobayashi & Ribstein, *supra* note 100.

[172] *See* William Cary, *Federalism and Corporate Law: Reflections upon Delaware*, 83 YALE L.J.

"race to the top" disciplined by efficient capital markets,[173] arguably does not apply to Internet transactions in the absence of such of a market.

Internet choice-of-law and choice-of-forum clauses arguably are adhesion contracts in which consumers effectively have little say. Commentators have questioned the viability of consumers' "clickware" contracts concerning consumer marketing information because of inadequate disclosure or because the rushed and casual atmosphere of web surfing is not conducive to contracting away supposedly important privacy rights.[174] Conditioning access on consent to a particular legal regime complicates these issues because the relevant terms are embedded in the chosen law rather than disclosed directly.[175] Thus, a consumer may be surprised to learn she has consented to the application of a law that lacks such protection. Firms operating websites undoubtedly will be better informed about the designated law than the typical consumer. States might therefore tailor their laws to attract firms rather than to protect consumers.

These arguments might lead non-selected states either to refuse to refuse to enforce clickware choice of law or forum clauses or to condition application of another state's law on disclosure and consent procedures that address this problem. Mandating such procedures might significantly reduce consumers' ability to choose among varying levels of state law protection. These arguments might also be used to justify federalizing Internet rules.

There are, however, significant arguments against the "race-to-the-bottom" hypothesis in this context. First, as already discussed, since consumers are not as helpless as they might appear to be, it is unlikely that the Internet is a lemons market that drives out honest vendors or a lambs market to which investors flock to be shorn. The same arguments apply in predicting whether web merchants will be able to get away with cheating consumers by contracting for lax regulation. For example, just as merchants cannot easily offer one web design for their less discriminating customers and another for the more informed and sophisticated, so it would be hard for them to aim different law choices at informed and uninformed consumers. Thus, if many customers are likely to know that a particular state's law and courts unduly favor sellers, the web operator will have an incentive not to contract for that law and forum.

Second, contractual choice of law or forum differs fundamentally from other contract clauses because political entities rather than private parties design the relevant choices. A state legislature that fails adequately to regulate consumer marketing information lets merchants harm users who live in the state. Internet users can employ the

---

663 (1974).

[173] *See* Ralph Winter, *State Law, Shareholder Protection, and the Theory of the Corporation*, 6 J. LEGAL STUD. 251 (1977).

[174] For commentary critical of enforcement of analogous "shrinkwrap" contracts formed when consumers use software sold with licenses in plastic wrapping, *see* Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CAL. L. REV. 111, 120 n.20 (1999); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995). For commentary favoring enforcement of the contract and distinguishing contrary cases *see* Kobayashi & Ribstein, *supra note* 157 at 267-70.

[175] *See* Goldsmith, *supra* note 102 at 1215; Johnson & Post, *supra* note 56 at 1395-1400 & nn 102-03.

same information and sophistication that they use in the product market in making political choices, and the pro-regulatory coalition of consumer groups and big firms will have some influence at the state level. These interest groups also influence state attorneys general, elected officials who have ample incentives to bring highly publicized enforcement actions against Internet firms.[176]

Indeed, these political considerations suggest that the real concern about state regulation is not about a "race-to-the-bottom," but rather about a "race-over-the-top" toward *excessive* regulation. This concern is addressed by the jurisdictional choice regime discussed above in this Part. The important point for present purposes is that there is little risk that jurisdictional choice will lead to *inadequate* regulation.

IV. A LIMITED APPROACH TO FEDERAL REGULATION

It may be tempting for policy analysts to stress the flaws in state law in arguing for federal regulation, either because jurisdictional competition inadequately protects consumers or because the jurisdictional choice mechanisms this article discusses do not adequately protect firms from a multiplicity of state regulations. But as noted in the introduction, it is important to beware the Nirvana fallacy. The equilibrium may be no less efficient than a federal regime in which politics replaces exit. In other words, giving legislators more power by increasing exit costs may simply change the identity of losers and winners rather than increasing social welfare.

Firms concerned about excessive state regulation must be particularly wary about seeking refuge in federal law. First, they cannot be sure that they will get the federal law they want. Even a single federal law can impose greater burdens than firms face in complying with the most rigorous state law. Moreover, federal law can have unpredictable effects because of how it applies to new technologies.[177]

Second, federal law may not purport to preempt state law. State attorneys general, acting through the National Association of Attorneys General, and consumer groups, can be expected to lobby against federal preemption. Thus, many of the federal bills introduced in 2000 do not purport to preempt state law.

Third, there is a significant question as to the effect of even the broadest federal preemption. In particular, federal laws may not preempt state actions based on common law fraud or tort or on general consumer fraud statutes.[178] Thus, federal law may succeed

---

[176] *See supra* note 161 and accompanying text.

[177] Two older federal laws that have been applied to Internet privacy are 18 U.S.C. §§2510-2522 (applying to interception of electronic communications); *id.* §2701 (unlawful access to stored communications). *See* Supnick v. Amazon.com, Inc., 2000 WL 1603820 (W.D.Wash., May 18, 2000) (certifying class action based on these provisions).

[178] Only two of the 2000 bills even purport to preempt fraud. *See* 1999 U.S. S. 2063 (preempting "State or local law regarding the disclosure by providers of electronic communication service or remote computing service and operators of Internet Web sites of records or other information covered by this subsection"); 1999 U.S. S. 2928 (providing that "[n]o State or local government may impose any liability for commercial activities or actions by a commercial website operator in interstate or foreign commerce in connection with an activity or action described in this Act that is inconsistent with, or more restrictive than, the treatment of that activity or action under this section"). For examples of bills that do not preempt state fraud remedies, *see* 1999 U.S. H. 5430; 2001 U.S. H. 89, 1999 U.S. S. 809; 1999 U.S. H. 3560; 1999 U.S.

only in providing another level of legal complexity and unpredictability as plaintiffs' lawyers and regulators exploit holes in preemption.[179] Indeed, federal law might significantly increase regulatory burdens by imposing stringent disclosure requirements breach of which can trigger state fraud remedies.

Thus, federal substantive regulation is not an appropriate response to any potential problems of excessive or inadequate state regulation. But is there a limited role for federal law in addressing problems that may exist under a state law regime? Federal law might bypass the evolutionary process discussed above and ensure immediate enforcement of contractual choice of law and forum. Federal disclosure requirements might address whatever information asymmetry problems might exist under state law. However, though an idealized version of federal law may be efficient, the actual law may not be. This suggests that it might be better to leave regulation to the competitive state law process.

A. FEDERAL CONTRACTUAL CHOICE STATUTE

Congress might provide a short cut to efficient enforcement of contractual choice of law and forum by enacting a statute mandating the enforcement of such contracts under the commerce or the full faith and credit clauses.[180] The statute might provide for application either generally or in Internet transactions where choice of law is a particular concern.

There would, however, be significant problems with a federal statutory approach.[181] Apart from the basic statute implementing the clause,[182] Congress has exercised its full faith and credit power only once in the last 200 years – to empower states *not* to enforce a state law, including one contractually selected in a contract, to the extent that it authorizes same sex marriage.[183] Enacting neutral procedural rules probably would not earn enough rents for federal legislators to justify the political risks of interfering with the traditionally state-governed area of conflict-of-laws.[184] This suggests that Congress is unlikely to pass a general choice-of-law statute. It may act specifically regarding Internet transactions, but then probably in response to the pro-regulatory

---

S. 2606; 1999 U.S. H. 4059, 1999 U.S. H. 2882; 1999 U.S. H. 313.

[179] For an example of the confusion and complexity that may arise, the Gramm-Leach-Bliley financial overhaul act allows for state law, but is subject to the Fair Credit Reporting Act, which preempts inconsistent laws. State legislators have been interpreting these acts as allowing for state privacy laws relating to third-party information firms. *See* 5 BNA ECOMMERCE AND LAW REPORT, 334, 336 (April 5, 2000).

[180] U.S. CONST., Art I, § 8; Art. IV, §1. For a leading proposal favoring a federal choice-of-law statute, *see* Michael H. Gottesman, *Draining the Dismal Swamp: The Case for Federal Choice-of-law Statutes,* 80 GEO. L. J. 1 (1991).

[181] *See* O'Hara & Ribstein, *supra* note 127 at 1224-25.

[182] *See* 28 U.S.C. §1738.

[183] 28 U.S.C.A. § 1738c.

[184] *See* Jonathan R. Macey, *Federal Deference to Local Regulators and the Economic Theory of Regulation: Toward A Public-Choice Explanation of Federalism,* 76 VA. L. REV. 265 (1990).

coalition that is likely to influence federal substantive regulation, and therefore subject to significant exceptions. Indeed, the federal statute might serve only to lock into inefficient regulation that state competition ultimately would have eroded in the absence of federal law.

A better approach to federal regulation would be to mandate enforcement of choice-of-forum clauses. This would be consistent with federal cases favoring enforcement of choice-of-forum clauses and with the Federal Arbitration Act, which mandates enforcement of arbitration clauses in some situations. This type of statute would not involve the same problems as a choice-of-law statute, since it would be neutral as to the type of law that is enforced. However, there remains the danger of exceptions to enforceability that inhibit evolution of efficient law.

B. DISCLOSURE REQUIREMENTS

Federal law might support enforcement of contractual choice of law and choice of forum clauses by providing for a uniform disclosure requirement. This would undercut criticism of such clauses based on information asymmetries. Although markets may be able adequately to address most such problems, a federal disclosure requirement could address the current problems facing firms that voluntarily disclose policies concerning protection of consumer marketing information. If the firm fails to conform to its stated policy, it might be sued under state or federal law, including FTC regulations, concerning deceptive claims. Thus, in the absence of mandatory standards, firms may be better off not saying anything. Of course, the alternative solution is to lighten the penalties for non-adherence to voluntary policies.

V. CONCLUDING REMARKS

Regulating consumer marketing information is best done at the state rather than the federal level. It would be counterproductive to straightjacket emerging technologies and business practices with a federal law, at least before a process of state experimentation, competition and evolution has had an opportunity to discover the right approach or mix of approaches. At this point, there is not even a clear basic model for allocating rights in this area. A state law approach will not lead to over- or under-regulation as some have predicted as long as merchants and consumers can contract for the applicable law and forum. Indeed, this approach points the way toward solutions for other aspects of Internet regulation.

Emphasizing state regulation in the U.S. might have global ramifications. Privacy advocates are pushing for globalization of privacy norms, and European countries already mandate fair information practices.[185] U.S. firms can resist foreign regulation in the same way that they can resist state regulation -- through choice-of-law and choice-of-forum clauses, blocking websites from forum screens, and avoiding locating assets in foreign jurisdictions.[186] However, blocking may not be fully effective, international law permits

---

[185] *See generally*, Reidenberg, *Resolving Conflicting Rules*, *supra* note 1.

[186] As to the latter move, *see* David Pringle, *Some Worry French Ruling on Yahoo! Work to Deter Investments in Europe*, Wall St. J., November 22, 2000 at B2, 2000 WL-WSJ 26617732 (quoting website operator as stating that "companies are going to ensure that they have no assets in Europe to reduce the chances of being successfully sued"). This move may be effective given the lack of a "full faith and credit" clause in the foreign context. *See* Michael Whincop and Mary Keyes, *The Recognition Scene: Game*

enforcement of a choice-of-forum clause in a consumer contract only "to the extent only that it allows the consumer to bring proceedings in another court,"[187] and wholly avoiding foreign jurisdictions constrains U.S. firms' global competitiveness. Thus, U.S. firms may be tempted to tailor their policies to foreign laws rather than fight them, and then seek federal regulation that conforms to European standards so that all U.S. firms, including those that do not do business internationally, will have to compete on a level playing field. This would be a global victory for mandatory privacy policies.[188] It would be better to give the state law approach a chance to take root and demonstrate its merits as compared to a one-size-fits-all federal or global standard. U.S. firms can use their considerable market clout to force non-U.S. regulators to abandon or moderate their protectionist approaches. Moreover, a choice of law model, having demonstrated its success in the U.S., could be scaled up to provide a model for global regulation.

Theoretic Issues in the Recognition of Foreign Judgments, 23 MELB. U. L. REV. 416, 422 (1999).

[187] See Hague Conference on Private International Law, *Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters*, art 4, Paragraph 7(3)(b), available online at http://www.hcch.net/e/conventions/draft36e.html (adopted by the Special Commission on Oct. 30, 1999).

[188] See Reidenberg, *Resolving Conflicting Rules*, *supra* note 1.

Table 1 –Regulatory Alternatives

Nature of Regulated Data	• Sensitivity
	  o Sensitive (with clear expectation of privacy) vs. non-sensitive personal data.
	• Substitutability
	  o Idiosyncratic vs. fungible (valuable only when aggregated with data from others).
	• Identity
	  o Personally identifiable vs. anonymous.
	• How Collected
	  o Passive (clickstream/tracking) vs. active collection.

Disclosure Requirements	• Information to be Disclosed
	  o Fact of collection and potential use vs. specific detail, including nature and type of information collected, how information is to be used, identity of any third party that will receive the information.
	• How Disclosed
	  o On welcome screen, available on site, or available by request.

Consent Requirements	• Consent Trigger
	  o Collection vs. use by third-party or use related to collection
	• Type of Consent
	  o Negative (opt-out) vs. Affirmative (opt-in)
	• Manner of Consent
	  o Assent/clicking vs. in writing/electronic signature
	• Frequency of Disclosure/Consent
	  o At time of initial agreement or visit vs. each time disclosure of data occurs.

Exemptions to government regulation	• Industry self-regulation • Consumer self-protection (e.g., P3P)

Preemption of State Law	• Scope
	  o Broad preemption of state law vs. no preemption
	  o Exclusive federal enforcement vs. concurrent state and private enforcement.
	• Preemption with Exceptions
	  o Fraud & Consumer Protection
	  o Tort, common Law, and other state or private civil actions.