Privacy Wrongs in Search of Remedies

by
JOEL R. REIDENBERG*

Introduction

The American legal system has generally rejected legal rights for data privacy and relies instead on market self-regulation and the litigation process to establish norms of appropriate behavior in society. Information privacy is protected only through an amalgam of narrowly targeted rules.[1] The aggregation of these specific rights leaves many significant gaps and fewer clear remedies for violations of fair information practices.[2] With an absence of well-established legal rights, privacy wrongs are currently in search of remedies.

The American public is beginning to demand that data privacy violators be held accountable. In a recent survey, Internet users overwhelmingly called for sanctions ranging from jail time to blacklisting of organizations that failed to respect privacy policies. [3]

* Joel R. Reidenberg. Professor of Law, Fordham University School of Law. This paper was originally prepared for the Nov. 15–16, 2002, symposium, "Enforcing Privacy Rights," jointly sponsored by the Institute for Law and Economic Policy, the Samuelson Law, Technology and Public Policy Clinic at Berkeley and the *Hastings Law Journal*. The author thanks the symposium participants for their thoughtful comments on the draft and thanks Tyler Malin for his research assistance. A Fordham Law School faculty research grant supported work on this article.

1. *See, e.g.,* Fair Credit Reporting Act, 15 U.S.C. §§ 16811681u (2000); Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (2000); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2000); Electronic Communications Privacy Act, 18 U.S.C. § 2510 (2000); Video Privacy Protection Act, 18 U.S.C. § 2710 (2000); Telecommunications Act of 1996, 47 U.S.C. § 222 (2000); Cable Communications Policy Act, 47 U.S.C. § 551 (2000).

2. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 379–96 (1996).

3. Opinion Surveys: What Consumers Have To Say About Information Privacy: Hearing Before Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce, 107th Cong. (2001) (testimony of Harrison "Lee" Rainie, Director, Pew Internet & American Life Project) (reporting on a major national survey of Internet users: "94% of Internet users want privacy violators to be disciplined. If an Internet company violated its stated privacy policy and used personal information in ways that it said it would not, 11% of Internet users say the company's owners should be sent to prison; 27% say the owners should be fined; 26% say the site should be shut down;

Public enforcement actions and private law suits in the United States are just emerging as an important force in the creation of adequate protection for citizens' personal information in American society.

This Article first describes privacy rights and wrongs that frame the search for remedies in the United States. In particular, this section focuses on two different types of harm created by the misuse of personal information and the desire to find protective rights: personal or private wrongs and public or societal wrongs. Next this piece explores public enforcement of these privacy wrongs. The Federal Trade Commission and state Attorneys General have become important "enforcers" against personal wrongs, but their efforts fall short of accomplishing systemic change and fail to provide individual victims with any real remedy. The third part of this Article examines private claims for privacy wrongs. This section explores some tortured efforts to obtain redress for privacy violations and offers a few theories for unexploited and unexplored claims. Finally, this Article concludes with an instrumentalist view of the search for remedies. The current mismatch between privacy wrongs and remedies creates a destabilizing force that will ultimately push in favor of enhanced legal rights for data privacy.

I. Privacy Rights and Wrongs

Data privacy presents a confused array of rhetoric and principle. The rhetoric often conflates a wide range of interests and values. Privacy does not neatly fit a single conceptual model.[4] Americans have asserted that privacy rights protect extremely disparate interests such as nude sunbathing,[5] safe sex,[6] electronic communications,[7] and spam-free electronic mailboxes.[8] Jerry Kang usefully identifies three groups of asserted privacy rights: spatial, decisional and informational.[9] Spatial rights delineate the individual's physical sphere of control. Decisional rights relate to an individual's control

30% say the site should be placed on a list of fraudulent Web sites."), available at http://energycommerce.house.gov/107/05082001Hearing209/Rainie308.htm.

4. *See, e.g.,* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1090 (2002).

5. United States v. Biocic, 928 F.2d 112 (4th Cir. 1991) (rejecting a privacy right to sunbathe in the nude).

6. Griswold v. Connecticut, 381 U.S. 479 (1965).

7. Konop v. Hawaiian Airlines, 302 F.3d 868 (7th Cir. 2002).

8. Timothy J. Muris, FTC Chairman, Remarks at the Privacy 2001 Conference, Protecting Consumers' Privacy: 2002 and Beyond (Oct. 4, 2001) ("Consumers' third concern is with practices that are unwanted intrusions in our daily lives. Unwanted phone calls disrupt our dinner, and our computers are littered with spam."), *at* http://www.ftc.gov/speeches/muris/privisp1002.htm.

9. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202–05 (1998).

over personal choices. Informational rights define a citizen's role in the treatment of personal information. Across different types of articulated privacy interests and values, principles protecting those interests are enshrined only with great difficulty into American law.[10] At the same time, a wide range of data privacy wrongs emerge and underlie the profound sense of unease that Americans report for the state of privacy in the United States.[11] This sense of unease has also led to changing public expectations. These shifting expectations add significant uncertainty to claims for corporate liability.

A. Basic Data Privacy Rights

The "right to data privacy" is a fractured and incomplete right in American law.[12] While the federal constitution provides some structure to the data practices of the state, the Constitution obviously never contemplated modern data processing. The Fourth Amendment and Fifth Amendments impose basic prohibitions on government data collections by banning illegal searches and seizures as well as compelled self-incrimination, while the First Amendment assures significant communications freedoms.[13] However, these rights do not offer a legal framework for private sector data practices.

The emergence of the concept of standards for fair information practice originated in the early days of computerization when the U.S.

10. *See generally* PAUL SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW (1996).

11. *See, e.g.,* Ben Charny*, Protect your Internet Privacy . . . By Lying*, ZDNET NEWS, Aug. 21, 2000, *available at* http://zdnet.com.com/2100-11-523232.html?legacy=zdnn (reporting that up to 25% of Internet users provide false identifying information as a way to protect their privacy online); Robert O'Harrow Jr., *Opinion Split on Web Privacy Seemingly Contradictory Results Show Lawmakers' Problem*, WASH. POST, Apr. 3, 2001, at E12, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A28560-2001Apr2?language=printer (reporting that a majority of Americans want law enforcement to have access to suspects' email, but also want stronger privacy laws); Laura Rohde*, Study: U.S. Surfers Want Guaranteed Privacy*, THE INDUSTRY STANDARD, Aug. 21, 2001, *available at* http://www.thestandard.com/article/0,1902,17854,00.html (reporting that the majority of Internet users want guarantees of privacy online); Press Release, Harris Interactive, First Major Post-9/11 Privacy Survey Finds Consumers Demanding Companies Do More To Protect Privacy; Public Wants Company Privacy Policies To Be Independently Verified (Feb. 20, 2002), *available at* http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429 (reporting that "most consumers still do not trust companies to handle their personal information properly."); Business Week/Harris Poll, *A Growing Threat*, BUS. WEEK, Mar. 20, 2000, *available at* http://businessweek.com/2000/00_12/b3673010.htm (reporting that 82% of Americans are not at all comfortable with the typical data profiling practice of merging data from different sources).

12. *See* SCHWARTZ & REIDENBERG, *supra* note 2.

13. *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). *But see* Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000).

Department of Health and Human Services elaborated a code of practice in 1973 for the fair treatment of citizens' personal information.[14] In 1980, the Organisation for Economic Cooperation and Development ("OECD") Guidelines succinctly expressed a set of basic principles as benchmark standards consisting of:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle[15]

These common standards for the fair treatment of personal information attracted wide acceptance and the principles are universally recognized for their value as an expression of data privacy rights.[16]

More recently, the US government distilled the basic principles into a more abbreviated list of standards for:

- Notice
- Choice
- Security
- Data Integrity
- Access
- Enforcement[17]

14. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), *reprinted in* U.S. PRIVACY PROTECTIONS STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 15 n.7 (1977).

15. OECD, RECOMMENDATIONS TO THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND THE TRANSBORDER FLOWS OF PERSONAL DATA (Sept. 23, 1980), available at http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-nodirect-orate-no-no-10255-13,00.html#title1.

16. The US Department of Commerce has even stated that the OECD Guidelines form the basis for most privacy codes and US statutes. *See* U.S. DEPT. OF COMMERCE, PRIVACY AND ELECTRONIC COMMERCE § 2 (June 1998) *available at* http://web.archive.org/web/20001205195900/http://www.doc.gov/ecommerce/privacy.htm *See also* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1325–30 (2000) (showing universal recognition of these First Principles).

17. *See* U.S. DEPT. OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (July 21, 2000) *available at* http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.

In the United States, the basic principles are only partially enshrined in legal rights.[18] Statutes such as the Fair Credit Reporting Act[19] or the Telecommunications Act[20] address specific elements of fair information practices, but do not address the full set of concerns enunciated by the complete set of principles. Tort protections have not expanded to fill the statutory voids and face significant conceptual obstacles.[21] Gaps in statutory rights will only be filled, if at all, through the marketplace and alternative policing.

B. Privacy Harms and Wrongs

The public debate in the United States tends to confuse distinct types of privacy harms or "wrongs." Breaches of the fair information practice standards create private wrongs to the individuals about whom the data relates. In effect, the failure to respect basic standards forms a *per se* harm to the individual as an unfair treatment of personal information. This first category of privacy wrongs might be termed "personal or private" wrongs.

For data gathering, individuals will perceive intrusive information practices as wrongful.[22] This harm maps to Kang's concern over spatial privacy. Noxiously intrusive gathering of personal information or clandestine gathering of data attacks an individual's physical sphere. Similarly, surveillance of individuals often evokes the sense of invaded space.

The misuse of personal information is likewise a significant privacy wrong. When data is collected for one purpose and then treated differently, the failure to respect the original expectation constitutes a cognizable harm. Often, however, this privacy harm is obscured by the polemic that surrounds annoyance and nuisance. To illustrate, the receipt of junk mail or junk telemarketing calls are

18. *See* SCHWARTZ & REIDENBERG, *supra* note 2.

19. 15 U.S.C. §§ 1681–1681u (2000).

20. 47 U.S.C. § 222 (2000).

21. See, e.g., Jay Kesan, *Cyber-Working or Cyber-Shirking? A First Principles Examination of Privacy in the Workplace*, 54 FLA. L. REV. 289 (2002); Jeffrey Sovern, *Protecting Privacy with Deceptive Trade Practice Legislation*, 69 FORDHAM L. REV. 1305 (2001); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); Joel R. Reidenberg, *Privacy in the Information Economy*, 44 FED. COMM. L. J. 195 (1992).

22. Professor Solove suggests that the typical paradigm for privacy invasions is based on the Big Brother metaphor and violations from surveillance or intrusiveness and that the harm caused by surveillance or intrusiveness consists of inhibition, self-censorship, embarrassment, and damage to one's reputation. He argues that this restrictive view misses the problems inherent in database treatment of personal information. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

nuisances for most people.[23] These are intrusive, though infrequently at the level of noxiousness. The annoyance is a derivative consequence of an underlying privacy wrong. The underlying privacy wrong is the misuse of personal information that gives rise to the unwanted solicitation. This misuse results from the individual's non-participatory role in the treatment of personal information. Such a situation occurs when an individual has no opportunity to object to the processing of personal information or when participation is obtained under false pretenses. Additionally, a misuse arises when data is manipulated in violation of the individual's reasonable expectations.

Another important type of private wrong arises from outrageous and noxious data disclosures. Metromail's processing of sensitive consumer information by incarcerated Texas convicts is a prime illustration of this point.[24] Similarly, Qwest's plan to sell the personal information of the company's telecommunications customers caused a public outcry.[25]

Beyond the personal harms, a second type of privacy wrong involves "public" or "societal" harm. Scholars argue that data privacy is a societal value and a requisite element of democracy.[26] Society as a whole has an important stake in the contours of the

23. *See, e.g.,* John Schwartz, *Consumers Finding Ways to Zap Telemarketer Calls*, N.Y. TIMES, Dec. 18, 2002, at C1 ("consumers have already signed up by the millions for the growing number of statewide do-not-call lists").

24. Dennis v. Metromail, No. 96-04451 (Tex. D. Ct. Travis County July 7, 1999) (notice of pendency hearing on proposed settlement), *available at* http://www.entwistle-law.com/news/cases/settled/pdf/newmetronot.pdf.

25. In 2002, Qwest informed customers that the company would sell customers' information. The plan raised a public outcry that forced the company to abandon the program. *See* Press Release, Qwest, Qwest Communication Withdraws Plan to Share Private Customer Account Information Within Company (Jan. 28, 2002), *available at* http://www.epic.org/privacy/cpni/qwest_press_release.html. The plan was probably legal following the Tenth Circuit's absurd decision in *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied sub. nom* Competition Policy Inst. v. U.S. West, 120 S. Ct. 2215 (2000). In that case, the FCC adopted an opt-in standard following an extensive fact-finding proceeding on the difference between opt-in and opt-out. The federal circuit court, however, utterly disregarded the administrative record and disingenuously stated that the FCC had failed to consider various alternatives. *Compare U.S. West*, 182 F.3d 1224 (holding that the FCC had not considered opt-out alternatives) *with In re Implementation of the Telecommunications Act of 1996*, CC Docket Nos. 96-115, 96-149, Second Report and Order and Further Notice of Proposed Rule-Making, FCC 98-27, at §§ 86107 (rel. Feb. 26, 1998) (extensively discussing and rejecting evidence supporting opt-out).

26. See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707 (1987).

protection of personal information.[27] Individual autonomy needs protected zones that defy a purely proprietary, choice model of data privacy.[28]

The public harm arises from offensive and socially corrosive practices. For example, Acxiom, one of the largest information-selling companies in the United States sought to profit from invidious stereotyping. In its product catalog, the company offered a "comprehensive ethnicity coding system" for clients to "overlay Assimilation codes . . . identifying individuals who may speak their native language, but do not think in that manner."[29] The same company also proposed to clients racial coding that resembled Nazi Germany's Nuremberg laws.[30] The information trafficking abuse of children is another illustration of offensive and corrosive practices. One prominent member of the Direct Marketing Association, the Student Marketing Group, was caught routinely obtaining data from children under false pretenses in order to sell the information.[31] The company even offered the data categorized by intelligence and religion.[32]

Additionally, public harm arises from the externalities of information sharing. Each member of society may have a non-represented stake in another's disclosures of personal information. Genetic data demonstrates this problem. The disclosure of one person's DNA simultaneously reveals information on that person's family members. Unless the family members can compel confidentiality, they lose their informational privacy with the disclosure of the relative's DNA. The effect of data aggregation and profiling presents the same type of risk, but in a subtler manner. As data is aggregated in purportedly anonymous fashion and then used for demographic profiling, the aggregations compromise the ability of any single member of society to participate in decisions about the treatment of personal information. To the extent that profiles

27. *See, e.g.,* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000).

28. Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

29. Acxiom Product Catalog, at 5 (1999).

30. *Id.*, (identifying "Jewish" as a race).

31. *See* Press Release, N.Y. Attorney General, Long Island Firm Sued for Tricking Students into Providing Private Information (Aug. 29, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug29a_02.html.

32. *See* STUDENT MARKETING GROUP INC., DATABASE & SERVICE, COLLEGE BOUND HIGH SCHOOL STUDENTS, *available at* http://www.studentmarketing.net/collbnd.htm (data selects include grade point average, and religious affiliation); STUDENT MARKETING GROUP INC., DATABASE & SERVICES, *available at* http://www.studentmarketing.net/dataserv.htm#ReligiousAffilx (offering to "select . . . children by age, gender, and declared religious affiliation").

become more refined and more predictive, individuals will be stereotyped for particular behavior and "aggregate" data becomes associated with individuals. Information redlining becomes the norm. These inaccurate stereotypes have a socially corrosive power, while accurate profiles without any participation of the affected individual begins to resemble clandestine social surveillance.

C. Changing Expectations

Shifting public expectations for privacy pose an important predicament for organizations that strive to be "good citizens." Privacy expectations are rising and now include a morally-charged environment.[33] Transparency of data practices is more prevalent now than five years ago.[34] Yet, transparency is only one element in the set of basic principles and is insufficient to assure the fair treatment of personal information. There is a growing public recognition that the misuse of personal data is harmful. In a rare public referendum on privacy, North Dakota citizens repealed the legislature's weakening of the state privacy law and restored opt-in privacy for financial information by a vote of 72% to 28%.[35]

For companies trying to do the "right thing," the guideposts are moving. Consensus on accountability for privacy remains elusive in the United States. At the same time, companies trying to respect privacy interests and values find themselves enmeshed in a turbulent legal environment. The structure for the treatment of personal information is increasingly defined through scandals and enforcement actions rather than sensible fair information practices.

33. See Steven Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*, 16 BERKELEY TECH. L.J. 877 (2001).

34. *See, e.g.*, 15 U.S.C. § 6803 (requiring notice by financial institutions of sharing of personal information); U.S. Dep't Health & Hum. Servs. Notice of Privacy Practices for Protected Health Information, 45 C.F.R. § 164.520 (2000) (requiring notice of use of personal information in health care); FTC, A REPORT FROM THE FTC STAFF: PROTECTING CONSUMERS ONLINE THE FTC'S FIRST FIVE YEARS 20 (Dec. 1999), *available at* http://www.ftc.gov/os/1999/9912/fiveyearreport.pdf (reporting that only a small percentage of web sites posted privacy notices in 1998, but that the percentage had risen substantially by 1999). *See also* HARRIS INTERACTIVE, CONSUMER PRIVACY ATTITUDES AND BEHAVIORS SURVEY WAVE II AT 4, July 11, 2001, *available at* http://www.bbbonline.org/UnderstandingPrivacy/library/harris2-execsum.pdf (reporting that 82% of Internet users had seen privacy notices in April 2001); Georgetown Internet Privacy Policy Survey, Report to the FTC (June 8, 1999), *available at* http://www.msb.edu/faculty/culnanm/GIPPS/gipps1.pdf, at 6 (reporting that 34% of web sites posted no privacy notices at all).

35. *See* S. Bill 2191, 2001 Leg. Assem, (N.D. 2001), *available at* http://www.state.nd.us/sec/pdf/referredmeasureno2ballotlang2002.pdf; *Bank Privacy Measure Fails*, Grandforks.com (June 12, 2001) (North Dakota voters "threw out a new state law that . . . made it easier for banks to sell their customers' checkbook secrets.") *available at* http://www.grandforks.com/mld/grandforks/3450535.htm.

II. Public Enforcement of Privacy Wrongs

Media attention to privacy scandals and concern among the public for privacy wrongs motivate state actors to seek remedies. As a normative proposition, public enforcement ought to devote its resources toward systemic corrections in industry practices that would stop or prevent public wrongs. Such an emphasis would promote remedies that are socially constructive and "democracy enhancing." However, in the absence of statutory data privacy rights, public enforcement is adrift. The lack of clear statutory authority for information privacy actions results in strained efforts to find a remedy. Indeed, public enforcement depends on creative and often convoluted theories of liability. These tertiary theories tend to mismatch public enforcement with personal wrongs rather than match them with public wrongs. At the same time, public enforcement relies on actors of expedience rather than enforcement agencies with specific privacy mandates. On the national level, a somewhat unlikely agency, the Federal Trade Commission, reluctantly took the federal lead and pursues enforcement actions through legal mechanisms that were not designed for privacy claims.[36] The states Attorneys General, though, are more disenchanted by the deficit in privacy rights and are more aggressive in their search for privacy remedies.

A. Tertiary Claims

The lack of fundamental statutory protection forces government actors to find tertiary rights for the assertion of privacy claims. This instrumental constraint limits public enforcement of personal wrongs where specific harms occur and inhibits state actors from addressing the public wrongs where more general harms occur. Most notably, state agencies resort to trade practice legislation as a means of policing voluntary disclosures of information-handling practices by companies. The most aggressive public enforcement focuses on data collection vices rather than the reform of profiling and information redlining practices.[37]

Beginning in 1996, the staff of the Federal Trade Commission recognized that some privacy wrongs might be addressed through existing statutory authority relying on the FTC's "unfair and

36. For an interesting discussion of the FTC's jurisdictional interest, see Steven J. Hetcher, *The FTC as a Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000).

37. *See* Edward C. Baig et al., *Privacy: The Internet Wants Your Personal Info. What's In It For You?*, BUSINESS WEEK ONLINE, April 5, 1999 *available at* http://www.businessweek.com/1999/99_14/b3623028.htm ("Some companies use the gold mine of consumer data to discriminate against customers who don't make the grade.").

deceptive trade practice"[38] jurisdiction. Two years later, the FTC brought its first case under this theory against GeoCities.[39] The theory maintains that companies commit an "unfair" or "deceptive" practice when they inaccurately describe their information handling practices. More recently, state Attorneys General have brought enforcement actions based on the state analogs of the federal statute. This approach targets the data collection process and its transparency. Since few companies have any obligation to disclose their privacy policies, this public enforcement only improves the accuracy of any transparency.[40] In an ironic twist, this public enforcement also provides a disincentive for greater transparency. A company risks liability by making a disclosure, but does not risk accountability by remaining silent. Alternatively, a company's policy may be drafted to avoid any meaningful disclosures and any privacy commitments at all. Indeed, for real transparency, an access right is necessary. Yet, the trade practice theory does not create an affirmative obligation to grant an individual access to personal information held and processed by an organization.

To a very limited extent, the objectives of prosecution for deception, do advance a systemic goal through a societal effect. While the results of any enforcement predicated on "unfair and deceptive practices" relate only to specific companies, the public efforts generally seek to raise corporate awareness and change industry behavior. At best, the trade practice theory advances the accuracy of statements about privacy practices, but does not obtain a remedy for any individual victim. The goal of the public proceeding is the cessation of a specific company's wrongful information practice. The narrowness of this approach is also evident, since its objectives do not include the prevention of information misuse itself. In effect, the theory is a weak proxy for the wrongs associated with misuse of personal data.

The other main effort at public enforcement looks to data security as a proxy for wrongful disclosures of personal information.[41]

38. *See* 15 U.S.C. § 45(a)(1) (2000); *See also* FTC STAFF REPORT, PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE 29 (Dec. 1996), *available at* http://www.ftc.gov/reports/privacy/privacy.pdf.

39. In 1998, the FTC reached a settlement with Geocities after complaining that Geocities obtained personal information through misrepresentations. *See In re* GeoCities, FTC Docket No. 98-23051 (Aug. 13 1998) (agreement containing consent order) *available at* http://www.ftc.gov/os/1998/9808/index.htm#13.

40. Financial service companies are the unusual exception. The Gramm-Leach-Bliley Act requires financial service providers to disclose their information privacy policies. 15 U.S.C. § 6803 (2000).

41. *See, e.g.,* Press Release, N.Y. Attorney General, Spitzer Reaches Internet Privacy Agreement with Alta Vista (Aug. 21, 2001), *available at* http://www.oag.state.ny.us/press/2001/aug/aug21a_01.html; Press Release, N.Y. Attorney General, Major

In the Eli Lily case, for example, the pharmaceutical company sent an email to patients who received information from the company on a drug to treat their psychiatric problem. The message revealed the addresses of all the patients as a result of improper use of the email software. Instead of attacking the wrongful disclosure itself—the real harm—the public enforcement action addressed the violation of the company's promise to treat patients' personal information with adequate security measures.[42]

In effect, the necessity for state actors to rely on creative, tertiary theories for privacy claims means that state enforcement does not address the public wrongs. The tertiary claims miss the underlying public issues of potentially corrosive practices such as profiling and stereotyping individuals. For example, the New York Attorney General's case against Student Market Group attacks the company's data gathering practices as wrongful methods in obtaining data from children.[43] The real privacy issue and public wrong, however, is the offensive trafficking in children's data. But, this wrong could not be the core of the public enforcement action when the basis for state enforcement was a tertiary theory of unfair trade practice.

B. Expedient Actors

Public enforcement of data privacy relies on an expedient set of actors who are generally mismatched to remedy public wrongs. The public actors do not have specific statutory privacy rights authority. Instead, they exploit derivative powers to play a role in privacy claims. At the federal level, the current enforcement agency is the Federal Trade Commission.[44] In many ways, this agency is an illogical

Pharmaceutical Company Agrees to New Safeguards for Consumer Data (July 25, 2002), *available at* http://www.oag.state.ny.us/press/2002/jul/jul25c_02.html; N.Y. Press Release, Attorney General, Major Tech Publisher Reaches Agreement with Attorney General on E-commerce Security Standards (Aug. 28, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug28a_02.html.

42. Press Release, N.Y. Attorney General, Major Pharmaceutical Company Agrees to New Safeguards for Consumer Data (July 25, 2002), *available at* http://www.oag.state.ny.us/press/2002/jul/jul25c_02.html.

43. *See* Press Release, N.Y. Attorney General, Long Island Firm Sued for Tricking Students into Providing Private Information (Aug. 29, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug29a_02.html.

44. The FCC never really thought about information privacy (other than wiretapping) until the Telecommunications Act of 1996 added a provision protecting the privacy of "customer proprietary network information." Under the Telecommunications Act, the FCC engaged in a rulemaking to determine the requisite degree of subscriber participation in service providers' decisions to market call information. *See* U.S. West Inc. v. FCC, 182 F.3d 1224, 1229 (10th Cir. 1999) *cert. denied sub nom.,* Competition Policy Institute v. U.S. West Inc., 120 S. Ct. 2215 (2000).

choice for the protection of citizens' privacy. The FTC's mission is to enforce antitrust and certain consumer protection laws:

> The Commission seeks to ensure that the nation's markets function competitively, and are vigorous, efficient, and free of undue restrictions. The Commission also works to enhance the smooth operation of the marketplace by eliminating acts or practices that are unfair or deceptive.[45]

Reliance on the FTC as a primary enforcer of citizen privacy is misplaced. The prevention of privacy wrongs, and particularly the public wrongs, as such, is simply not part of the core mission of the FTC. The FTC is not charged with the enforcement of civil rights, nor is the agency equipped or permitted to handle employment or telecommunications privacy matters. In fact, the FTC only grudgingly accepted involvement with privacy issues. During the mid-1990s, Commissioner Christine Varney persistently raised privacy as an important issue. For many years, the FTC hoped that the market would self-regulate and did not want to intervene aggressively. The FTC even opposed new federal legislation to protect information privacy.[46]

The FTC has historically admitted that its unfairness jurisdiction is "evolutionary."[47] Indeed, in the past, the FTC has stated to Congress that consumer unfairness requires substantial injury and that "emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair."[48] Since all of the FTC's deceptive practices cases have settled prior to any court decision, the legal standards remain uncertain. The scope of the FTC's "unfairness" jurisdiction remains ripe for a court decision.[49] More importantly, changes in the composition of the FTC can result in significant policy changes with respect to enforcement. Whether the FTC will even retain a serious interest in privacy enforcement remains to be seen.

While the FTC seems to be the federal regulator of choice for a light touch in enforcement against privacy wrongs, the states' Attorneys General have taken a more aggressive stance. The National Association of Attorneys General has an Internet Law task force that studies and coordinates the enforcement of privacy.[50] In

45. FTC, VISION, MISSION, & GOALS, *at* http://www.ftc.gov/ftc/mission.htm.

46. FTC, SELF-REGULATION AND PRIVACY ONLINE: REPORT TO CONGRESS (1999), *available at* http://www.ftc.gov/os/1999/9907/privacy99.pdf (urging Congress not to legislate privacy rights for online activities, but to wait for self-regulation).

47. *See* Letter from FTC to Senate Consumer Subcomm. of the Comm. on Commerce, Science and Transp., (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

48. *See id.*

49. *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239-45 (1972).

50. *See* Nat'l Ass'n. of Attys. Gen., *at* http://www.naag.org (last visited Jan. 16, 2003).

effect, the states are unwilling to wait for federal results. This more aggressive stance of public enforcement at the state level is illustrated well by an enforcement action brought against DoubleClick. In February 2000, the Electronic Privacy Information Center ("EPIC"), a prominent privacy advocacy group, filed a complaint against DoubleClick with the Federal Trade Commission based on the company's practice of profiling web users without adequate disclosure.[51] EPIC's complaint focused on the lack of disclosure and on profiling as an "unfair and deceptive practice." The FTC eventually closed its investigation with no action.[52] However, a coalition of ten states pursued DoubleClick's practices and compelled DoubleClick to accept a binding agreement regarding privacy policies and disclosure; DoubleClick also accepted a fine of $450,000 to reimburse the states' investigative costs.[53]

Like the federal actions, the state cases that rely on "unfair and deceptive practices" statutory authority do not address the public wrongs directly. When states pursue claims, the results are only able to achieve company specific cessations of particular data processing practices.[54] These remedies address specific harms to individuals rather than the broader harms caused by wide-spread practices. The absence of claims against companies that engaged in egregious profiling and stereotyping, like Acxiom, illustrates that addressing directly the public wrongs falls generally outside the scope of a state Attorney General's statutory authority.

51. *See* EPIC Files FTC Complaint Against DoubleClick Alleging "Deceptive and Unfair Trade Practices" in Online Data Collection (Feb. 10, 2002) copy of the complaint available at http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

52. *See* Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, Federal Trade Commission, to Christine Varney, counsel for DoubleClick (Jan. 22, 2001), *available at* http://www.ftc.gov/os/closings/staff/doubleclick.pdf.

53. *See* In the Matter of DoubleClick: Agreement between the Attorneys General of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick (Aug. 26, 2002) *available at* http://www.oag.state.ny.us/press/2002/aug/aug26a_02_attach.pdf; Press Release, N.Y. State Att'y Gen., Major Online Advertiser Agrees to Privacy Standards for Online Tracking (Aug. 26, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug26a_02.html.

54. *See, e.g.,* Press Release, N.Y. State Att'y Gen., Spitzer Reaches Internet Privacy Agreement with Alta Vista (Aug. 21, 2001), *available at* http://www.oag.state.ny.us/press/2001/aug/aug21a_01.html; Press Release, N.Y. State Att'y Gen., Major Pharmaceutical Company Agrees to New Safeguards for Consumer Data (July 25, 2002), *available at* http://www.oag.state.ny.us/press/2002/july/july25c_02.html; Press Release, N.Y. State Att'y Gen., Major Tech Publisher Reaches Agreement with Attorney General on E-commerce Security Standards (Aug. 28, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug28a_02.html; Press Release, Minn. Att'y Gen., Minnesota Attorney General and U.S. Bancorp Settle Customer Privacy Suit, (July 1999) *available at* http://www.ag.state.mn.us/consumer/Privacy/PR/pr_usbank_07011999.html.

III. Private Claims for Privacy Wrongs

The main goal of private claims for privacy wrongs should be the vindication of a personal harm. The key objective for citizens, when faced with abusive information practices, is redress. In this context, the use of private claims as a policy mechanism to achieve systemic change would not be congruent with the goal of individual redress. Redressing personal wrongs, however, presents troubling obstacles. As a threshold matter, the identification of an enforceable legal right to privacy poses an important challenge. Recent attempts to fit data privacy within existing rights have met strong court resistance. Other unexploited claims and creative new theories offer attractive instruments for redress. However, these possibilities also face significant practical challenges.

A. The Threshold Obstacle: Finding a Right

Victims of the abuse of personal information have a difficult time identifying a legal right that would afford a remedy for data privacy violations. In general, American law does not require the disclosure of data practices.[55] However, the creative use of consumer protection statutes serves to police the accuracy of any privacy policy disclosures made by organizations. However, the federal statute lacks any private right of action.[56] State statutes may offer private rights of action though these are likely to impose particular injury requirements that are hard to meet[57] or other restrictions on the use of the statutory right.[58]

Privacy wrongs related to offensive data collection practices similarly face a void in remedial options. Without a direct statutory right to the fair treatment of personal information, Internet privacy victims unsuccessfully argued recently that the surreptitious gathering by DoubleClick of information about web users' surfing was an illegal interception of communications between the user and the web site.[59] The federal district court, in an opinion worthy of Charles Dickens'

55. Several laws in particular circumstances do require some disclosures. *See, e.g.,* 12 U.S.C. § 6903 (financial institutions must provide notice of data practices), 12 U.S.C. § 1681 (b)(C)(1)(B) (consumer reporting agencies must provide notice of an opt-out right for certain types of unsolicited marketing offers).

56. *See, e.g.,* 15 U.S.C. § 45(a)(2) (2000) (creating public enforcement without any private remedies).

57. *See, e.g.,* Smith v. Chase Manhattan Bank, USA, 741 N.Y.S.2d 100 (N.Y. App. Div. 2d. Dept. 2002).

58. *See* Goshen v. Mutual Life Insurance Co. of N.Y., 744 N.E.2d 1190 (N.Y. 2002) (private parties limited in ability to bring suit); Oswego Laborer's Local 214 Pension Fund v. Marine Midland Bank, 647 N.E.2d 741 (N.Y. 1995) (for a private action, deception is measured against the reasonable person.).

59. *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y., 2001).

"circumlocution office,"[60] rejected a consolidated class action claim.[61] The court held that the participating web sites could, under the Electronic Communications Privacy Act,[62] consent to the gathering of personal information from their users without their users knowledge or consent.[63] Courts have also rejected the argument that DoubleClick acted tortiously, thereby invalidating the consent.[64]

Similarly, attempts to treat data collection wrongs as a form of trespass in the online environment do not work. Secret gathering of personal information might be an offense under the provisions of the Electronic Communications Privacy Act that address stored wire and electronic communications records.[65] These sections were designed to sanction computer hackers. However, according to at least one court, these protections do not extend to personal computers, but rather are reserved for the protection of Internet access services through ISPs or other servers.[66] Victims are grappling to fit wrongful data collections into the existing legal protections against wiretapping.[67] Victims are also trying to fit offensive, secret data collection practices into the prescriptions of the Computer Fraud and Abuse Act.[68] The law creates protection against any person who intentionally accesses computers without authorization and against any computer user who exceeds authorization.[69] The statute requires "losses aggregating at least $5000" and the courts seem to be split on whether to require a showing of economic loss from a single act over the course of a one-year time period.[70]

In at least one other prominent case, the search to find a remedy against a wrongful disclosure of personal information fell flat. An educational institution illegally released a college student's disciplinary record. Despite the illegality of the release of the record

60. CHARLES DICKENS, LITTLE DORRIT, 104 (Alfred A. Knopf, Inc. 1992), *available at* http://www.freebooks.biz/Classics/Dickens/Little/Little10_1.htm.

61. *DoubleClick Inc*., 154 F. Supp. 2d at 526–27.

62. 18 U.S.C. § 2510–11 (2000).

63. *DoubleClick Inc*., 154 F. Supp. 2d at 510–11.

64. *Id.* at 514–19. In a separate case, another federal district court came to the same conclusion. Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001). *See also In re* Pharmatrack Inc. Privacy Litig., 220 F. Supp. 2d 4, 12 (MA, 2002) [hereinafter *In re Pharmatrack Litigation*]

65. 18 U.S.C. § 2510–11 (2000).

66. *In re Pharmatrack Litigation*, *supra* note 64, at 13.

67. *See, e.g., In re* Toys-R-Us Privacy Litigation, No. 00-1381 2001 U.S. Dist. LEXIS 16947 * 3–6 (N.D. Cal. 2001).

68. 18 U.S.C. § 1030(a)(2) (2000).

69. *Id.* § 1030(a)(2).

70. *See* EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577, 584–85 (1st Cir. 2001); *In re Pharmatrak Litigation,* supra note 64 at 15. *But see In re* Toys R Us, Inc., 2001 U.S. Dist. LEXIS 16947 at *32; *In re* America Online Inc. Version 5.0 Software Litigation, 168 F. Supp. 2d 1359, 1382 (S.D. Fl. 2001).

under the Federal Education Right to Privacy Act ("FERPA"), the statute provided no direct remedy and the victim sought unsuccessfully to graft a remedy on FERPA through the civil rights law.[71]

In all, these claims show that privacy remedies for personal wrongs are not easily accommodated within the existing set of legal rights. Even worse, these possibilities do not provide a basis for many basic elements of fair information practice such as a data subject access right, the right to have obsolete data purged, and the right to fairness in the collection of personal information.

B. Under-Exploited Options and Theories

Although the efforts to find remedies for personal wrongs under existing statutory rights leave many gaps, a number of under-exploited options and theories may nevertheless emerge. The Fair Credit Reporting Act ("FCRA"),[72] for example, may serve as a stronger protection against profiling and general data misuse. The FCRA seeks primarily to assure the integrity of consumer information used to evaluate an individual's creditworthiness, fitness for employment, and eligibility for insurance.[73] Credit report information is now a very attractive source of data for marketing efforts since credit reporting agencies maintain some of the most current, reliable information available on individuals' financial status.

Increasingly, credit report information is sought for general marketing purposes rather than the original purpose of credit decision-making. The FCRA prohibits obtaining and using credit report information without a permissible purpose.[74] The statute only allows the release of credit report information for marketing purposes "if the transaction consists of a firm offer of credit or insurance."[75] Companies such as Worldcom and AT&T Wireless have tried to skirt the FCRA's prohibition on the disclosure of credit report information for unsolicited advertising. Both of these companies have been rummaging through consumer credit reports to drum up business for wireless phone service and for the sale of wireless telephones.[76] At

71. Gonzaga University v. Doe, 122 S. Ct. 2268, 2276 (2002) (denying a remedy under 42 U.S.C. § 1983).

72. 15 U.S.C. § 1681–1681v (2000).

73. 15 U.S.C. § 1681a (2000).

74. 15 U.S.C. § 1681b(f) (2000)

75. 15 U.S.C. § 1681b(c)(1)(B)(i) (2000).

76. *See* Solicitation from Worldcom, May 2002 ("You have been pre-approved for WorldCom Wireless service"); Free Phone Voucher from Worldcom, May 2002 ("This Pre-approved Voucher entitles you to a FREE Motorola digital wireless phone"); Solicitation from AT&T Wireless, Feb. 2002 ("You are Pre-Approved for a FREE wireless phone when you activate new service with AT&T Wireless").

least one credit reporting agency, Equifax, is a willing accomplice.[77] Other companies, like USSearch.com or ChoicePoint, engage in precisely the type of profiling that the FCRA targets.[78] Yet, these companies reject the obligations of the FCRA.[79] The potential claims against credit reporting agencies for illegally disclosing credit information and failing to comply with the FCRA, as well as the claims against their clients—the companies that illegally obtained the data—are significant.

A promising, though largely untested, theory for private remedies is the common law tort of misappropriation of name or likeness.[80] This tort essentially protects the commercial value of an individual's identity from conversion. The classic cases involve the use of a celebrity's name without permission to endorse a product. The value of the celebrity's name is used to market the product. This is very similar to the collection of data for profiling and sale. When individuals are profiled, the characteristics of the profile take on a commercial value. The value of any particular profile or name in a database may be small, but in the aggregate the profiles have a

77. The FCRA requires companies sending unsolicited offers of credit or insurance to disclose how and where the consumer's name was acquired. Ironically, AT&T Wireless and Worldcom respected this provision. *See* Solicitation from Worldcom, May 2002 ("information contained in your credit report maintained by Equifax . . . was used in connection with this offer"); Solicitation from AT&T Wireless, Feb. 2002 ("we used information we obtained from a consumer-reporting agency . . . Equifax").

78. *See, e.g.,* http://www.ussearch.com (offering "comprehensive" searches including bankruptcies, civil judgments, real estate values and other data that may be included in credit scoring algorithms); Choicepoint Marketview, *at* http://www.choicepoint.com/industry/financial/direct_2.html (the Marketview direct marketing "database includes data on demographics, lifestyle, credit bureau information, and proprietary insurance and financial attributes").

79. ChoicePoint, for example, advertises its database as a general marketing database, but nevertheless offers profiles based on credit factors such as home loans and car loans. *Compare* http://www.choicepointprecisionmarketing.com/data_marketview.html with ChoicePoint Marketing Prospect Lists Personal Lines P & C, http://www.choicepointprecisionmarketing.com/download/cppm_dds_plines.pdf .

USSearch.com disingenuously tries to avoid the application of the FCRA with a disclaimer contained in the Terms and Conditions of the Consumer Services User Agreement. The disclaimer is hard to find and purchasers of services from USSearch.com are not required to make any affirmation that would negate illegitimate uses of personal information prior to acquiring data from USSearch.com. *See* http://www.ussearch.com (follow link to purchase "background searches" to a page where "Enhanced Exhaustive Background with Criminal" searches can be purchased. On the side of this page, there is a fine print link to the "Consumer Services User Agreement."). For the text of the service agreement, *see* US SEARCH.com Inc., Consumer Services User Agreement Terms and Conditions (Oct. 2002), *at* http://www.1800ussearch.com/user_agreement.html.

80. *See* William Prosser, *The Right to Privacy*, 48 CAL. L. REV. 383, 401 (1960). Some states, like New York, have codified the common law tort of misappropriation of a name or likeness. *See, e.g.,* N.Y. CIV. RIGHTS LAW §§ 50–51 (McKinney 1992).

commercial worth.[81] The sale of the profile captures the value of those characteristics of the individual just as a product endorsement captures the value of a celebrity's name. Whether the value is large or small, the tort does not distinguish between the conversions of the name's value.

In the context of data privacy, only four states have faced this claim: Ohio,[82] Illinois,[83] New Hampshire[84] and Virginia.[85] Three of these cases (Ohio, Illinois and Virginia) involved challenges to the sale of mailing lists containing the names and addresses of clients, while the fourth (New Hampshire) addressed the sale of personal information by an information service. In Ohio, the state appellate court confused the claim of misappropriation with the annoyance of receiving junk mail.[86] In Illinois, the state appellate court found that the name on a list did not have intrinsic economic value.[87] The value was only in the associations and profiling created by the gatherer of the personal information.[88] This reasoning does not make any sense. The characteristics associated with the name are precisely the types of value for which the tort assigns control to the individual. Indeed, at least one court has recognized the misappropriation of an individual's information profile to meet the damages threshold in the context of the Computer Fraud and Abuse Act.[89] In Virginia, the state county court found that a deliberately misspelled name does not give rise to a claim for misappropriation.[90] No state supreme court has issued a ruling on the merits of any of these three mailing list cases.

81. For example, a list of names with particular demographic characteristics may be sold for less than $0.15 per name. In March 2003, American List Counsel charged $0.08 per name for new movers profiled by ethnicity and $0.12 per name for "the new generation of moneyed Moms and Dads." *See* American List Counsel, Data Card: New Mover Profiler—New Homeowners ALC, *available at* http://search.alcdata.com/market?page=research/datacard&id=56967 (listing a base fee of $71/thousand names and a supplemental charge of $10/thousand names for an ethnicity selection); American List Counsel, Data Card: Forbes-Successful Young Families with Children, *available at* http://search.alcdata.com/market?page=research/datacard&id=56572 (listing a base fee of $125/thousand names). Other data, such as a credit report, may be more expensive and cost as much as $25 per name. *See* Accurate Business Credit, ABC Resources , *available at* http://www.abccreditreports.com/pricing.html (listing the fee to purchase a single consumer credit report as $25).

82. Shibley v. Time, Inc., 341 N.E.2d 337, 337–38 (Ohio App. Ct. 1975).

83. Dwyer v. American Express Co., 652 N.E. 2d 1351, 1356 (Ill. App. Ct. 1995).

84. Estate of Boyer v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

85. Avrahami v. U.S. News & World Report Inc., No. 95-1318, 1996 Va. Cir. LEXIS 518, at *1 (1996).

86. *Shibley*, 341 N.E.2d at 339.

87. *Dwyer*, 652 N.E.2d at 1356.

88. *Id.*

89. *In re* Toys R US, Inc. Privacy Litigation, No. 00-1381, 2001 U.S. Dist. LEXIS 16947, at *36 (N.D. Cal. 2001).

90. *Avrahami*, 1996 Va. Cir. LEXIS 518 **1718.

The misappropriation tort did, however, reach the New Hampshire Supreme Court in the context of data privacy. There, in *Estate of Amy Lynn Boyer v. Docusearch, Inc.,*[91] an online information service provided a young woman's birth date, home address, social security number, and employment address to her stalker. Using the information, the stalker killed the woman at her place of employment.[92] The victim's estate brought several claims for invasion of privacy against the online information service, including misappropriation of the victim's name for commercial benefit. New Hampshire had never before considered the tort of misappropriation of a name or likeness.[93] The state supreme court recognized the tort, but refused to consider the sale by the investigator as a misappropriation. The court said:

> An investigator who sells personal information sells the information for the value of the information itself, not to take advantage of the person's reputation or prestige . . . . [T]he benefit derived from the sale in no way relates to the social or commercial standing of the person whose information is sold.[94]

Although the Court's factual assertion about the value to the investigator of the information is suspect,[95] the reasoning opens the door widely for claims against information brokers who sell consumer profiles. The benefit from the sale of profile information explicitly appropriates value from the social and commercial standing of the individuals who are profiled.

The misappropriation claim, thus, appears ripe for state courts around the country. In particular, the California courts would be a promising venue to establish this remedy, since the protection against misappropriation exists in California[96] and more significantly, the legal climate is hospitable. California is one of the few states to have a constitutional provision on privacy and is unique in the application of that provision to the private sector.[97] When California added the privacy clause to the state constitution, the trafficking in personal information and the establishment of rights against private conduct were specifically contemplated and part of the successful ballot initiative.[98] Indeed, the scope and remedies of the Constitutional

91. Estate of Boyer v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

92. *Id.* at 1006.

93. *Id.* at 1009.

94. *Id.* at 1010.

95. If the personal information has a commercial value, then the value may in fact derive from attributes of the individual's identity such as where the person lives or works.

96. CAL. CIV. CODE § 3344 (West 1997) (codification of the misappropriation tort).

97. CAL. CONST. art. I, § 1. *See also* Hill v. NCAA, 865 P.2d 633, 641 (Cal. 1994) (applying the constitutional protections to private conduct).

98. *See* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 418 (1992).

provision are largely unexplored for private enforcement against private conduct.

While various new theories and unexploited claims may be asserted in private enforcement actions, an important incongruence will exist for these claims. The FCRA, misappropriation and California constitutional claims are collective action claims. Generally, tens of thousands of individuals will be identically situated, if not millions, in the case of many typical data processing activities. The underlying harm becomes a public wrong against society as a whole for the profiling and large-scale manipulative practices and not just a personal wrong for the misuse of an individual's data. Private enforcement actions would then be seeking to correct public wrongs rather than focusing on individual redress of personal wrongs.

C. Defining the Damage

Beyond the search for an appropriate right, another significant threshold issue is the definition of damage. The *misuse* of personal information is both a personal wrong to individuals and a public wrong to society. Harm comes through the transgression of fair information practices and does not depend on additional consequences from the wrong. Some argue, however, that privacy redress should only occur if there is a monetary harm.[99] In a startling decision under the Cable Communications Policy Act, a federal court ruled that a clear violation of the statutory protection for data privacy caused no harm and refused to grant relief to a private party.[100] Under this "monetary" harm approach, wrongful disclosure is not considered "actual" harm. This approach either misses the point of data privacy or is a disingenuous answer to the privacy wrongs. The very breach of a recognized fair information practice standard inherently wrongs the individual. Such "unfair" information practices are autonomous wrongful acts that do not depend on financial consequences for their harm. The wrongful disclosure in and of itself is an "actual harm" to the individual. More broadly, the corrosive effect of information trafficking on society does not depend on the monetary damages potentially caused to particular victims.

99. *See, e.g.,* Hearing on the Need for Internet Privacy Legislation Before the Senate Comm. on Science and Technology, 107th Sess. 1 (July 11, 2001) (statement of Fred H. Cate, Professor, Ind. Univ. Sch. of Law Bloomington) *available at* http://www.senate.gov/~commerce/hearings/071101Cate.PDF; Solveig Singleton, *Privacy as Censorship*, Cato Institute Policy Analysis No. 295 (Jan. 22, 1998) *available at* http://www.cato.org/pubs/pas/pa-295.pdf.

100. *See* Parker v. Time Warner Entertainment Co., 198 F.R.D. 374, 381 (E.D.N.Y. 2001) (finding no actual harm under the Cable Communications Policy Act, 47 U.S.C. § 557(a)(1), for wrongful disclosures absent a showing of monetary harm).

D. Cost Disincentives

Significantly, the cost of suit generally serves as a major disincentive for individuals to bring claims that would vindicate privacy wrongs. Because privacy violations often occur on a large scale, the damages may be construed as disproportionate to the harm, particularly when harm is measured by the monetary consequences that flow from the privacy wrong. One recent case illustrates this difficulty. Trans Union over a period of years, committed significant violations of the Fair Credit Reporting Act and was challenged by the Federal Trade Commission. After almost a decade of appeals by Trans Union, the Federal Trade Commission prevailed when the D.C. Circuit affirmed that Trans Union illegally sold personal information for marketing purposes.[101] The Supreme Court, with an unusual dissent, denied a writ of certiorari.[102] When the actual victims sought to recover damages under the FCRA's mandatory provision granting minimum statutory damages, the federal district court in Illinois denied class certification because of the potentially crushing blow to the privacy violating company.[103] In effect, the court denied the victims a remedy. Although the FCRA does include a provision on attorney's fees, the minimum statutory damages of $100, without a class action is insufficient to justify litigation over a wrongful act having an incremental impact such as an occasional illegal disclosure of credit information rather than a spectacular consequence such as the denial of a mortgage based on inaccurate information.

Conclusion: The Public Effect of Enforcement for Private Wrongs

The prospects for public and private enforcement of privacy wrongs are at present unsatisfying. On the surface, the current efforts show confused and mismatched objectives between public and private enforcement. In essence, normative goals have been reversed: public enforcement seeks to remedy personal wrongs,[104] while private enforcement seeks to prevent wide-scale harms.[105] The absence of clear statutory data privacy rights constrains public enforcement to

101. Trans Union Corp. v. FTC, 245 F.3d 809, 811 (D.C. Cir., 2001). The author served as an expert adviser and witness in this case for the Federal Trade Commission.

102. Trans Union v. FTC, 122 S. Ct. 2386, 2386-87 (2002).

103. *In re* Trans Union Corp. Privacy Litig., 211 F.R.D. 328, 351 (N.D. Ill. 2002) (class certification denied for sale of personal information in violation of FCRA). A similar problem arose under the Truth-in-Lending Act. *See* Ratner v. Chemical Bank N.Y. Trust Co., 54 F.R.D. 412, 416 (S.D.N.Y. 1972) (no class certification when the calculated damages were disproportional to the monetary harm suffered by the victims).

104. *See* Part II.A.

105. *See* Part III.B.

pursue personal wrongs. These public claims for private harms are not an effective means to achieve personal redress for each victim. Indeed, a variety of misuses of personal information such as the failure to provide access or numerous types of surveillance activities fall outside the scope of any statutory authority for public enforcement. Conversely, many of the private claims against data collection practices try to address much broader public wrongs associated with stereotyping and information redlining. Yet, these private claims can only have an indirect effect on public harms. Private claims bring adverse publicity to industry practices that, in turn, may provoke salutary industry-wide changes such as the increased number of privacy policies posted on web sites. Such improvements, however, are only secondary effects of the publicity and still fall short of providing any effective remedy to individuals for violations of fair information practice standards.

The reversal of goals is an unfortunate consequence of the difficulty of finding a legal right to enforce. The real search behind the efforts to remedy privacy violations is a search to create new legal rights. As the movement for privacy enforcement expands in search of remedies, litigation destabilizes the current status quo that protects privacy violators. At present, without clear statutory rights, there is an important lack of legal accountability or liability for the unfair treatment of personal information by the private sector. Scandals and suits bring these practices to public attention and create higher expectations along with instability for the status quo. This in turn provides an incentive for legislative action to establish greater legal certainty for the treatment of personal information. The mismatch of enforcement mechanisms and creative efforts to find privacy remedies just may be the missing catalyst for new legal rights to privacy in the United States.