The Offensive Internet

Privacy, Speech, and Reputation

Edited by

Saul Levmore and Martha C. Nussbaum

HARVARD UNIVERSITY PRESS

Cambridge, Massachusetts, and London, England 2010

Printed in the United States of America

Library of Congress Cataloging-in-Publication Data

The offensive Internet : speech, privacy, and reputation / edited by Saul Levmore and Martha C. Nussbaum.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-674-05089-1 (alk. paper)
1. Internet—Law and legislation—United States. 2. Libel and slander—United States. 3. Privacy, Right of—United States. 4. Reputation (Law)—United States. 5. Privacy, Right of—United States. I. Levmore, Saul X. II. Nussbaum, Martha Craven, 1947–
KF390.5.C6O344 2010
343.7309'944—dc22

2010022409

CHAPTER 6

Reputation Regulation: *Disclosure and the Challenge of Clandestinely Commensurating Computing*

FRANK PASQUALE

There are many reasons to worry about the unsubstantiated rumors, opinions, and evaluations now polluting cyberspace. Viral culture online has made literally true the old bromide, "A lie can be halfway 'round the world before the truth has got its boots on." Although the emancipatory potential of digital connectivity is clear, critical Internet studies have illuminated its role in reinforcing old structures of unfair disadvantage and unearned privilege. Regulation may be necessary to check these trends.

For years, search engines have tried to reassure us that diligent "vanity searching"—that is, entering one's own name as a search query, in order to see what comes up—is the key to good "online hygiene." If an objectionable result comes up about a person, she can litigate against its publisher, or try to "drown it out" with rival information designed to drive the unflattering material to less salient positions in search results. Companies like Reputation Defender offer such services, acting as twenty-first century "reverse private detectives" who specialize in concealing or obscuring damaging information.

The self-help approach always had many shortcomings. Defamation lawsuits are expensive and uncertain projects, especially in the United States. Litigation can backfire, increasing the salience of provocative material if the suit garners media attention. Even the best search engine optimizer cannot guarantee the success of an effort to "bury" unflattering results with other material. But these tactics at least offered some means of trying to "clear one's name" online by detecting, deterring, and occasionally obscuring slurs and innuendo viewable to all.

New search technology has now fatally compromised self-help strategies. As personalization advances, there is no single set of "search results" for a person's name. One searcher may see a collection of positive or neutral results about an individual; another might be presented with compromising material. Screeners within human resources or credit-approval departments may order specialized software that scours the Internet for the most troubling material about any applicant. It is unlikely that the applicants they evaluate will have access to similar software.

In the United States, expansive interpretations of the First Amendment undermine even modest proposals for regulating the results of search engines. However, promoting individuals' access to the Internet results obtained by those making important decisions about them would pass constitutional muster. It would also reduce the reputational "unknown unknowns" that can wreak havoc on careers, credit, and educational opportunities. To the extent that key decision makers know more about us, we need to know exactly what data they have and how they are using it. As David Brin predicted in *The Transparent Society*, further disclosure from corporate entities needs to accompany the scrutiny we all increasingly suffer as individuals.[1]

Reputational systems can never be rendered completely just, but legislators can take two steps toward fairness. The first is relatively straightforward: to ensure that key decision makers reveal the full range of online sources they consult as they approve or deny applications for credit, insurance, employment, and college and graduate school admissions. Such disclosure will at least serve to warn applicants of the dynamic digital dossier they are accumulating in cyberspace. Effective disclosure requirements need to cover more than the users of reputational information—they should also apply to some aggregators as well. Just as banks have moved from consideration of a long-form credit report to use of a single commensurating credit score, employers and educators in an age of reputation regulation may turn to intermediaries that combine extant indicators of reputation into a single scoring of a person. Since such scoring can be characterized as a trade secret, it may be even less accountable than the sorts of rumors and innuendo discussed above. Any proposed legislation will need to address the use of such reputation scores, lest black-box evaluations defeat its broader purposes of accountability and transparency.

Internet-Driven Decision Making

In developed countries, having an online presence is a near inevitability for all but the most marginalized. Classes routinely complete projects online, and profiles on social-networking sites are becoming not only a social but a professional necessity. An individual need not try to create a web presence for herself—detractors or admirers can instantly catapult her into micro-celebrity with or without her permission. Blogging also creates both professional opportunities and dangers, as Heather B. Armstrong, the author of the blog "Dooce," learned when she was fired by her employer for her online commentaries. She ultimately had the last laugh: "getting Dooced" became a slang term for being fired for blogging, and she was able to support herself from advertising as the site became more popular. But many others with online presences may never discover the adverse impact of the "digital person" they appear to be online.[2]

Search engines and social networks offer a tempting trove of data for decision makers. In the college admissions context, "a recent study by the University of Massachusetts-Dartmouth found that 25 percent of college admissions offices admit to using search engines such as Google, Yahoo, and MSN to research potential students and that 20 percent look for the same information on social networking sites such as Facebook and MySpace."[3] Employment lawyers routinely offer guidelines to employers who plan to Google job applicants.[4] There is evidence that "as many as 50% of employers and 77% of job recruiters concerned about alcohol/drug abuse, violence, and similar problems check out potential employees on the Web."[5] Sources for online scrutiny range from Google, Facebook, eBay, and Yahoo to PeopleFinders .com, Local.Live.com, Zillow.com (real estate purchase and sale data), Feed ster.com, Technorati.com (to search for blogs), and Opensecrets.org and Fundrace.org (to search for campaign donations).

Legal efforts to ensure the fairness and accuracy of such reputation-affecting information have not caught up to technological advances in producing it. For example, if a human resources department has "personalized" its results to ensure that the most damaging information available about a person (from its perspective) comes up first, that applicant has no right to learn what information the office considered as it made its negative decision. The applicant would have to avail himself of the same personalizing software to be fully aware of all the negative information such a personalized search was generating. Yet trade secrecy and contracts could

easily prevent him from ever accessing an exact replica of the programs used by the educators, employers, landlords, bankers, and others making vital decisions about his future. Even as health reform legislation makes it harder for insurers to discriminate against individuals on the basis of health status, employers or other entities may start to consult personal health data on sites including "Patients Like Me" if users fail to adequately secure their information.[6] Online openness can lead to permanent records of one's weight, health status, and mental health issues.

In popular books like Ian Ayres's *Super Crunchers* and Stephen Baker's *The Numerati*, legal scholars and journalists have celebrated data-driven decision making as a cornerstone of future advances in productivity.[7] However, the individual who is an *object* of such "super-crunching" may fear that a crucial decision about her is being made on the basis of a misunderstanding—an unfair reduction of a complex person to one trait, fact, or record.

In *The Politics of Recognition*, Charles Taylor explores the claims of individuals who felt that they were treated unfairly—or, worse, degraded and subordinated—on account of their ethnic identity.[8] Taylor advanced discussion of multiculturalism by articulating the harm of *misrecognition*—of being understood by others in an untrue or insultingly unflattering light. For example, women are routinely treated unfairly (and even brutally) solely on the basis of gender-based stereotypes.[9] Those dogged by digital scarlet letters may find whole new modes of discrimination blocking their professional or personal advance.

Of course, employers, colleges, and banks have a right to reject or approve applications as they see fit. But while it is one thing to be judged on an identified fault, it is a different experience altogether to to suffer a negative judgment for an unknown reason. While such a problem might seem unlikely now, personalized search technology makes it increasingly possible in the future. As any individual uses a search engine, he gradually trains it to prioritize certain types of results and de-prioritize others.[10] This translation of behavior into a "database of intentions" helps searchers a great deal—but can create uncertainty and anxiety once one is the object searched.[11] While the investigative consumer reports (ICRs) generated by credit-reporting agencies (CRAs) are subject to several strictures, personalized searches are not regulated in the United States.[12] The regulatory framework surrounding extant background checks may unfairly induce the use of informal, digital methods that increase the chance of mis-recognition and reductionism. It is time to develop a consistent regulatory approach for credit bureaus and

other sources of reputational information. Antidiscrimination norms may well lead us from legislating against aggregate stereotyping to creating opportunities for individuals to correct misinformation.

Background on the Fair Credit Reporting Act

Much like today's Internet, the files of pre-Fair Credit Reporting Act (FCRA) credit bureaus were often contaminated with irrelevant and inaccurate information, or innuendo. Their dossiers included judgments laced with prejudice; for example, "in 1972, a man in San Francisco discovered that a consumer report about him for life insurance policy included the comment that he used 'his hands in an effeminate manner, also talks in an effeminate manner.' "[13] Senator William Proxmire translated public concern about "erroneous and selective credit reporting" into hearings about credit industry practices and eventual passage of the FCRA.[14]

Congress passed the FCRA in 1970 to protect consumers and regulate the consumer credit-reporting industry. The Congressional findings associated with the act describe the sorry state of the industry as it existed before the passage of FCRA.[15] Congress intended the law "to require that consumer-reporting agencies adopt reasonable procedures . . . for [compiling] consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[16]

The act regulates the preparation of consumer credit reports by "credit-reporting agencies," as well as the disclosure of those reports, and procedures associated with the maintenance of consumer credit information.[17] When the act applies, it establishes the permissible uses for which an agency may release a report or disclose information, such as by consent of the consumer or for insurance and credit applications. The FCRA also requires that agencies make reasonable efforts to verify information, including the identities of consumers, to increase accuracy.

CRAs must remove information from a report after a certain period of time to reduce the likelihood of reporting obsolete information. If incorrect or inaccurate information is reported, a consumer has the right to dispute the record, at which point the agency must reasonably investigate at no cost to the consumer, and must delete inaccurate data. In addition, consumers are supposed to benefit from mandatory disclosure after an adverse action is taken against them based on a credit report, which gives them the opportunity to

dispute inaccuracies under the FCRA. When an agency fails to comply, the FCRA provides a cause of action for civil liability.[18]

Scholars have addressed the policy behind the "second chances" that FCRA mandates are meant to ensure. While "practical obscurity" used to occlude transgressions over time, the CRAs' data storage technology necessitated a legal requirement to restore the old balance between obscurity and publicity. Updating its mandates for the digital age, Jonathan Zittrain has proposed a form of "reputational bankruptcy," giving individuals the ability to block out some features of their online identity.[19] Viktor Mayer-Schonberger's book *Delete: The Virtues of Forgetting in the Digital Age* takes up the difficult task of specifying technical standards for this type of monitoring.[20] Each of these proposals fits into the framework of Danielle Citron's model of "technological due process"—ensuring that the de facto adjudications and rule makings made by software programs live up to some standards of reviewability and revisability.[21]

To complement proposals for "editing by deletion," I have proposed an "annotation remedy" designed to give a more complete picture of persons who object to certain hyperlinks in search results.[22] Such a remedy would permit individuals to add an asterisk to the offending hyperlink, directing web users to their own comment on the objectionable result. Google has recently adopted an "online profiles" program that is one small step toward such annotation rights.[23] My proposal is inspired by Helen Nissenbaum's characterization of privacy as "contextual integrity"—a social condition affording the individual more chances to give a full and complete picture of oneself in a world increasingly driven by scores, snapshots, and sound bites.[24]

Can such ideas be incorporated into a regime like the FCRA? At first glance, the FCRA's focus on the mundane transactional details of credit and debt management has little to offer in the way of solutions to online reputation problems generally. But the very regulatory infrastructure that imposes some minimum standards on credit reports may unfairly elevate the salience of online reputation generators, which can report more provocative (and less vetted) information and rumors. As search engines and other online ratings and rankings entities grow in prominence, some level playing field needs to develop to take into account their roles as data collectors and arrangers. Finland has prevented employers from using Google results (among other unauthorized information sources) in evaluating potential applicants.[25] In this essay, I propose a less draconian solution: requiring

important decision makers to reveal the online sources they use in order to evaluate applicants, and revealing the particular information found out about an applicant to that applicant after any decision is made.

A Fair Reputation Reporting Act?

The FCRA is targeted at credit bureaus and the reports they generate. Now that search engines permit anyone to compile a digital dossier on anyone else, can such distributed activity be effectively regulated? Probably not—but at least some elementary steps toward the disclosure of such materials by critical decision makers can curb the most Kafkaesque features of the new reputation systems.

The types of unfairness created by undisclosed reputation dossiers are traditional concerns of three bodies of law: antidiscrimination law, employment law, and fair information practices.[26] None of these laws aspires to cover all human endeavors, and a Fair Reputation Reporting Act would need to be focused, too.[27] Critical decision makers—those with the power to grant or deny applications for employment, credit, insurance, housing, and education—are a logical starting point for such a law. As these decision makers take into account new sources of aggregated information, it would be deeply unfair for applicants not to have a chance to review the digital dossier compiled about them.

Business interests are likely to object to the obligations generated by such a review requirement. However, the same technology that makes so much information available presently can ease the transition to dedicated documentation. As storage costs decline and cloud computing becomes ubiquitous, a decision maker can use software to default to recording the online "leads" pursued as she investigates an applicant. Anyone who has seen a search engine's "web history" knows how revealing and meticulous that documentation can be.

The exact scope of the requirements will need to be worked out by an administrative agency—perhaps the Federal Trade Commission, or perhaps a true privacy regulator to be created pursuant to the proposed act. Regulators will not need to reinvent the wheel. Administrative law has long addressed the record-keeping requirements of government agencies, carefully separating the types of searches for information that constitute forbidden "ex parte contacts" from the run-of-the-mill research no one expects to be recorded.

Though this essay is too brief to flesh out the administrative details of disclosure provisions in a Fair Reputation Reporting Act, it should address three key objections to it. First, while administrative law principles of disclosing the basis of a decision are accepted for government actors, why should the private actors targeted by such legislation also be required to be open about what they are reviewing? Second, should word of mouth or personal recommendations be subject to the same level of review? Third, would the new transparency render reputation reporting as overly positive because individuals will contest negative information, but have no incentive to correct inaccurate positive information?

The first objection merits a layered response. Issuers of credit and insurers are pervasively regulated. As the financial crisis has demonstrated, these entities rely on government as their "ultimate risk manager."[28] After the failure of financial industry deregulation, an ever-closer intertwining of state and the FIRE (finance, insurance, and real estate) industries is a hallmark of the Obama administration.[29] "Coming clean" on the bases of their decisions is a small price to pay for the degree of government subvention they are now receiving.

The case of employers and educators is slightly more complicated. These decision makers are subject to many antidiscrimination laws, and the fair data practices discussed above might better be incorporated into extant regulation on those grounds rather than being a free-standing privacy law. Given the extraordinary targeting of women documented by Danielle Citron and Martha Nussbaum in this volume, there is already a serious civil rights case to be made against indiscriminate reliance on Internet sources.

Citron's documentation of the negative effects of Internet abuse on women is also part of a suite of responses to the second objection. Unlike a recommendation letter written for one or a few readers, or a phone call that is almost never heard by anyone other than the callers, Internet-based rumors and lies are frequently persistent, searchable, replicable, and accessible to any decision maker with access to the right software or database. A negative reference hurts only for as long as a job seeker keeps it on her résumé; a negative comment online is almost always beyond her control. Anyone affected by such expression deserves at least some chance at discovering whether it has been considered by key decision makers.

The third objection above attempts to shift our attention from the rights of the individual to the information environment as a whole. While individuals will likely contest or try to obscure negative data about them, they

have no incentive to eliminate incorrect positive information about them. The problem of incorrect positive information has plagued employment references for some time. If decision makers must disclose the reports and research they use to make decisions, the information environment overall could become biased.

To help sort out these problems, it is helpful to examine J. H. Verkerke's work on the law of employment reference practices.[30] Verkerke provides a typology of three problems facing employers and regulators: "falsely negative references, an inadequate supply of reference information, and falsely positive references."[31] At this level of generality, Verkerke's typology also fits the problem of matching customers to insurers and banks, tenants to landlords, and students to schools. Verkerke argues that any effort to improve the quality of references risks reducing the quantity of information available. He concludes that proposed "regulatory measures that would . . . deter [employers] from providing falsely positive references . . . [present an] inescapable trade-off between quantity and quality substantially weakens the case for these reforms." Could the same be said of the fair information practices promoted in this essay? I believe there are many reasons to believe that the information environment and our understanding of reputation have changed sufficiently since Verkerke's piece was published to justify taking special aim at false and negative information.

First, we might want to consider the implications of environmental law for information privacy. Dennis D. Hirsch argues that just as new forms of pollution have caused extraordinary damage to the natural environment, "the digital age is causing unprecedented damage to privacy . . . [as a] 'faceless infrastructure' employs . . . data to deny us jobs, credit, insurance, and other social goods, often without our knowledge."[32] He observes that environmental law has long grappled with the problem of balancing the costs and benefits of regulation. If a given effort to purify the natural environment becomes too costly, state and federal agencies provide many opportunities for feedback designed to subsequently reduce the costs of compliance. Any agency enforcing a Fair Reputation Reporting Act should be open to concerns that its actions have "biased" the information environment, and respond accordingly.

We can already envision some concrete methods of doing so. For example, just as the agency enforcing FCRA could be seen as a guardian of consumers' reputations, a counter-agency dedicated to dispelling false, positive information could arise to assist businesses. Such an agency would investigate

suspicious "sock-puppet" behavior designed to create a misleading impression of the authority, talent, or other positive attributes of an individual. Tal Zarsky has noted the problem of manipulative gaming of reputational systems and has recommended deterrence of "gamers" and "sock-puppeteers."[33] The rise of fusion centers and other public-private surveillance initiatives suggests that state actors will assist businesses in such endeavors in exchange for businesses' supplying antiterrorism and other crime-fighting leads.[34]

Even if the state does not become involved on behalf of businesses in this way, information intermediaries can also sniff out false, positive information on their behalf. Verkerke already predicted their rise in his 1998 article, and Lior Strahilevitz has written about their emergence in areas ranging from real estate to insurance.[35] Just as credit bureaus emerged to vet applicants for customers and banks, they and other information intermediaries may start to scrutinize sources of information online. Using algorithms like those employed by Google, they could begin to weight sources of information by reliability in order to give decision makers a clearer sense of exactly how reliable a given positive or negative piece of information is.

Frontiers of Reputation Regulation

Credit bureaus have already gone beyond merely vetting *sources* of information about individuals. They routinely commensurate information into a single score purporting to assess the creditworthiness of applicants for loans. The FCRA may have helped spur the development of this reputation mechanism. After the content of their reports had to be accessible to consumers, credit bureaus became increasingly reliant on opaque credit scoring. Though a credit score is computed via proprietary algorithms protected as trade secrets, it is widely treated as a fair and objective evaluation of an individual's creditworthiness.[36] Disclosure of such secrets can easily amount to a "taking," requiring government compensation for all the business based on it.

After the subprime debacle, the social importance of credit scoring (and its use by predatory lenders) has become more obvious than ever. Nevertheless, the industry remains highly opaque, with scored individuals unable to determine the consequences of late payments, changes in location, or other decisions. Several disturbing reports have alleged racial, geographic,

and other inappropriate influences on credit scores. Because of concerns about their unreliability and unfairness, use of credit scores has been regulated by forty-eight states.[37]

Credit scores have also come under attack for having a disparate impact on poor and minority populations.[38] The National Fair Housing Alliance has criticized them as embedding sexist and racist assumptions into an ostensibly neutral process:

> Studies as well as lawsuits continue to demonstrate that African Americans, Hispanics, and elderly women are not treated the same as similarly qualified white males when attempting to purchase products such as cars, or secure mortgage loans or homeowners insurance. The terms and conditions for purchase of these products can be driven by the race, national origin or gender of the consumer rather than by their ability to pay or condition of the home.[39]

The scores themselves may be self-fulfilling prophecies, creating the financial distress they claim merely to indicate.[40] If a scorer determines that one missed $10 payment for a woman with two children earning $30,000 per year lowers her credit score by 200 points, she will be more likely to default because her low score means that she is going to be paying much more in interest for any financing she can find. Since the scores are black boxes, we have no assurance that scorers try to eliminate such endogeneity or whether they profit from such self-fulfilling prophecies.

Could the black-box proprietary models now common in credit scoring spread to reputation scoring? Several Silicon Valley entrepreneurs have already made the connection. For example, Auren Hoffman's company, Rapleaf, offers individuals a bargain—in exchange for plugging in all the details of extant online profiles about them into its system, Rapleaf will give them one-stop access to the information, and will generate a "reputation score" for its members. The Korean site Cyworld has long rated users' "friendliness," "karma," and "sexiness," among other qualities.[41] A company called Gorb "allows, even insists on, anonymous comments and ratings about rated individual's" professional and personal lives.[42] Some of these sites aim not merely to rate the willing, but also to rate everyone within a particular sphere.

So far, the only reported legal case pertaining to such sites has concerned the rating of attorneys by a site called Avvo. As reputation regulation develops, policy makers should examine closely professionals' campaign for

accountable rating sites. Though the attorneys ultimately lost their case, physicians have succeeded in forcing insurers that rate them to engage in fair information practices. Both professions' struggles foreshadow future efforts to hold reputation raters more accountable than credit scorers currently are.

In the legal industry, Avvo aims to rate all licensed attorneys within the states it covers.[43] It claims its service gives lawyers the opportunity to increase their exposure and find potential clients. Toward that end, each licensed attorney has a profile on the site. Using public records, Avvo also provides a history of any sanctions or disciplinary measures taken against the attorney. Clients can post reviews of attorneys whose services they have used. Avvo uses this and other information to generate a rating for lawyers, which is a numerical score from 1.0 (the worst—"Extreme Caution") to 10.0 (the best—"Superb"). A rated attorney can add certain information to her profile after "claiming" it by using an identification verification system.

The right to claim the profile is a classic example of Web 2.0 business models. Attorneys listed on the site ignore the profile at their peril, and those critical of Avvo's project are put in a double bind by the profile's very existence. If they ignore the profile, they effectively allow Avvo and others the ability to control this aspect of their online identity. To the extent they tell "their side of the story" on the site, they are feeding data to Avvo and building its reliability. The aggregator acts like Tom Sawyer, inviting others to "paint the fence" by adding to the store of data that increases its authority and comprehensiveness.

Avvo's rating is difficult to assess because the company does not disclose how it is calculated, ostensibly because such disclosure would allow lawyers to manipulate and "game" the rankings in their favor. Avvo does not permit lawyers to pay or purchase ads to help their ratings—however, given the secrecy of its rating algorithm, it is difficult to verify this anti-payola pledge. Partly in order to avoid liability for defamation, Avvo insists that its rankings are merely its opinion, and are not factual.

In 2007, two Washington attorneys filed a complaint against Avvo for violation of the state's Consumer Protection Act (CPA), and sought class certification to include all lawyers rated by Avvo.com. The complaint alleged that "by reporting arbitrary and capricious scores and promoting them to consumers as mathematical calculations and a reliable assessment of a lawyer's competence to handle legal matters, Avvo has engaged in . . . unfair and deceptive acts and practices in violation of" the CPA. The plain-

tiffs alleged that the rating system treated lawyers unfairly and deceived the consumers who relied on it.

Avvo filed a pretrial motion to dismiss the case, arguing that the complaint was insufficient for several reasons. The court granted the motion, ruling that the "opinions expressed through the rating system . . . are absolutely protected by the First Amendment." The court posited that the site did not deceive consumers because it "contains numerous reminders that the Avvo rating system is subjective," an opinion rather than fact. Since the ratings on the site could not be proven true or false, the court ruled that Avvo was immune from liability for defamation. Avvo did not disclose its algorithm at any time in the suit.

The blanket protection the *Avvo* court would provide for opinions is open to challenge. Internet law expert James Grimmelmann unpacks the leading case on the issue:

> Milkovich v. Lorain Journal Co., while stating the rule that the Constitution shields opinions, leaves in place two significant exceptions. A statement of opinion may imply an underlying fact (the Court's example: "In my opinion John Jones is a liar."), and even a statement of opinion may be false if not honestly held (the Court's example: "I think Jones lied," where the speaker thought nothing of the sort). . . . The relationship of subjective opinion to objective fact . . . is not simple.[44]

Here, the opinion "John Jones is a terrible lawyer" implies certain facts about what Jones did to make him such a rotten attorney. Avvo's disclaimers about its "subjectivity" notwithstanding, no one would take the site seriously if it did not claim to be based on objective and relevant information.

There are examples of challenges to ratings that survived a motion to dismiss,[45] settled out of court,[46] or lost on the merits.[47] These cases demonstrate that there is no absolute First Amendment privilege for opinions or ratings. Therefore, the threat of costly litigation can be used as leverage to persuade raters to accept regulation. This dynamic may have driven resolution of several lawsuits against physician-rating websites.

In the medical field, insurance companies have begun to create "black-box" evaluation, ranking, and rating systems for doctors. Fearing an unfair tiering of its members, the Washington State Medical Association (WSMA) filed suit against Regence BlueShield, an insurance company that evaluated doctors using allegedly inaccurate and outdated information.[48] The doctors claimed that Regence used four-year-old data, small sample sizes, and focused

on cost of claims rather than quality of care.[49] The complaint alleged defamation and violation of the CPA, among other causes of action.[50] After ten months of litigation, Regence agreed to settle with the WSMA "in an effort to better understand physician concerns,"[51] voluntarily withdrawing the Select Network program. The settlement agreement, effective for at least two years, promises transparency in evaluations, as well as fair methodology.[52]

In New York, the state attorney general, Andrew Cuomo, launched an investigation of insurers' physician ratings that culminated in settlement agreements in 2007. Cuomo claimed that the evaluation programs were confusing and unfair to both physicians and consumers.[53] After negotiating with his office, insurance companies eventually agreed to follow the ranking guidelines in a national model provided by the Office of the Attorney General (OAG) (in cooperation and consultation with the American Medical Association and other provider trade organizations). The model agreements require "insurers to fully disclose to consumers and physicians all aspects of their ranking system."[54] Since there is mandatory disclosure of all data and methodologies, the problem of the "black-box" evaluation system is reduced under the model agreements. Attorney General Cuomo has advocated the codification of the model based on his written agreements with insurance companies, and several prominent members of the New York legislature have agreed to support the bill.[55] The proposed bill suggests a trend toward transparent, quality-based rankings. CIGNA has agreed to make its rating methodologies public.[56] A "Patient Charter for Physician Performance Measurement" has also emerged as a project of the Consumer-Purchaser Disclosure Project (CPDP). The specific terms of the charter call for evaluations that are "meaningful to consumers" and bar decontextualized ratings based solely on cost.

Comparing Lawyers' Failures and Doctors' Successes in Regulating Reputation Scoring

Professional ranking programs are here to stay, and may play a vital role in pay-for-performance programs designed to rationalize compensation for physicians and lawyers. The CPDP's approach suggests some principles that could govern reputation regulation more generally. However, the failure of the Avvo lawsuit shows that First Amendment defenses can pose a formidable challenge to accountability here. Why have lawyers so far failed where doctors have succeeded?

Some nonlegal differences in the two cases spring to mind. Avvo.com is far smaller than the settling health insurance companies. There is an obvious conflict of interest in the latter situation: insurance companies have a financial incentive to "rank" doctors based on their cost to the insurance company, not the quality of care they offer. An insurance company might profitably purport to evaluate and rank doctors by quality, but then put the physicians who cost the company the least money at the top of its rankings. On the other hand, more subtle and dispersed conflicts of interest permeate Avvo's business model. It has no direct financial interest in the costs of lawyers' work, but it does have an interest in spurring attorneys to "claim" their profiles and supply the site with more information.

Frequently blamed for making heartless coverage decisions, insurance companies are eager to avoid additional bad press. Avvo.com is a new company without the image problems of the private health insurance industry. Moreover, Avvo's prime business model is to rate attorneys, while the insurers' core profit centers lie elsewhere. Though both attorneys and physicians have successfully protected their economic interests, more compressed income distribution among the bulk of physicians may make the "logic of collective action" more compelling to them. Finally, while attorneys ignore their Avvo profile at their peril, and cannot directly deny Avvo business, physicians can pull out of offending insurers' networks.

Yet there are also significant legal rationales for the divergent results of the two lines of litigation. Insurers are part of a heavily regulated industry where government decisions are crucial to their ongoing profitability. Many Supreme Court decisions have permitted agencies to shape the speech of recipients of governmental largesse. In its 9–0 decision in Rumsfeld v. Forum for Academic and Institutional Rights, Inc., the Court allowed the government to condition certain benefits on beneficiaries' compliance with governmental standards. Had the insurers failed to settle, they would likely have seen the doctors merely shift their case from the courts to state insurance commissioners. Avvo, by contrast, is a mere web start-up, with very little contact with or (apparent) reliance on governmental largesse. But as a closer examination of the complex web of laws that govern cyberspace intermediaries reveals, they may well be as vulnerable as insurers to governmental pressure designed to ensure basic protections for the individuals they rank and rate.

Free Speech and the Regulatory State

Internet service providers and search engines have mapped the web, accelerated e-commerce, and empowered new communities. They also pose new challenges for law. Individuals are rapidly losing the ability to affect their own image on the web—or even to know what data others are presented with regarding them. Technology's impact on privacy and democratic culture needs to be at the center of Internet policy making. Regulators should promote individuals' capacity to understand how their reputations—and the online world generally—are shaped by dominant intermediaries.

Heraclitus wrote that "for the waking there is one world, and it is common; but sleepers turn aside each one into a world of his own." In our age of fragmented lifeworlds, narrowcasting, and personalization, Internet searchers are increasingly like Heraclitus's sleepers, each turning to customized reports on the persons and events they take an interest in. While many authors have lamented the effects of the "Daily Me" on politics, and others have noted the Kafkaesque implications of data-driven decision making, few have considered the intersection of these trends. This essay has attempted to do so, and has proposed norms of transparency to ensure that the "watched" have some idea of what type of dossier and scoring the "watchers" are compiling about them.

Because First Amendment defenses have so far quashed many tort actions against raters and rankers, this essay has focused on tailored regulatory responses. Although there is no blanket exception from First Amendment protections for regulations, they appear to be less limited by this constitutional privilege than tort suits. This may be because regulations that promote "the social interest in order and morality" can outweigh the First Amendment concerns that have stymied tort suits.[57] As both Robert Post and Fred Schauer have observed, there are a number of examples of speech-restricting regulations that have not been rendered unconstitutional by First Amendment challenges.[58]

For example, commercial speech is one category of expression frequently regulated by the government. The law "accords a lesser protection to commercial speech than to other constitutionally guaranteed expression."[59] When commercial speech is misleading it can be restricted. . . . For example, regulatory actions banning false advertisements are not prohibited by the First Amendment.

Moreover, when the government has a "substantial interest in regulating" commercial speech, it is not necessarily limited by the First Amendment,

even if the speech in question is completely lawful and is not misleading.[60] Copyright and trademark law are two instances where the unfettered right to free speech yields to larger "social interest[s] in order and morality."[61] Provisions of the DMCA strictly regulate what an intermediary like YouTube can keep on its site once it receives a notice that certain material infringes on copyrights. It would be deeply troubling if law could simultaneously be so solicitous of copyright owners (who are able to veto many fair uses, at least temporarily, under the terms of the DMCA), and utterly neglect the interests of those whose reputations are harmed by irresponsible intermediaries.

Just as consumers' interests trump a false advertiser's right to "express himself" with lies about products, so too should certain reputational interests take precedence over the bare right to offer scoring of others' reputations. Norms of due process may throw some sand in the wheels of today's lightning-fast generation of information and scores about individuals. However, fair opportunity in the Information Age depends on accountable rating practices and models. More open and accurate systems of evaluation are a legitimate choice for a culture increasingly disillusioned with clandestinely commensurating computing.

6. Reputation Regulation

1. David Brin, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* (Basic Books, 1999).
2. Daniel Solove, *The Digital Person* (N.Y.U. Press, 2004).
3. Darby Dickerson, Background Checks in the University Admissions Process: An Overview of Legal and Policy Considerations, 34 *J. College & Uni. Law* 419, 492, n. 514 (2008).
4. Robert Sprague, Googling Job Applicants: Incorporating Personal Information into Hiring Decisions, 23 *Labor Lawyer* 19 (2007); Thomas F. Holt Jr. & Mark D. Pomfret, Finding the Right Fit: The Latest Tool for Employers, 14 *Metro. Corp. Counsel* 29 (2006); Robert Sprague, Rethinking Information Privacy in an Age of Online Transparency, 25 *Hofstra Lab. & Emp. L. J.* 395 (2008).
5. Richard A. Paul & Lisa H. Chung, Brave New Cyberworld: The Employer's Legal Guide to the Interactive Internet, 24 *Lab. Law.* 109 (2008).
6. Jeana H. Frost & Michael P. Massagli, Social Uses of Personal Health Information within PatientsLikeMe, an Online Patient Community: What Can Happen When Patients Have Access to One Another's Data, 10 *J. of Med. Internet Research No.* 3 (2008), available at http://www.jmir.org/2008/3/e15#ref26.
7. Ian Ayres, *Super Crunchers* (Random House, 2008) (discussing data-driven decision making by "number crunchers" enabled by ever-faster computers); Stephen Baker, *The Numerati* (Houghton-Mifflin Harcourt, 2008) ("[S]ome 40 PhDs, from data miners and statisticians to anthropologists . . . comb through [IBM] workers' data").
8. Taylor, *The Politics of Recognition* (Princeton University Press, 2001) 25 ("The thesis is that our identity is partly shaped by recognition or its absence, often by the *mis*recognition of others . . .").
9. Martha Nussbaum, "Legal Weapon," *The Nation* (2006) (reviewing Catharine MacKinnon, "Are Women Human?") ("Inequality on the basis of sex is a pervasive reality of women's lives all over the world").
10. With personalized search, a search engine can use artificial intelligence and other methods to gradually "learn" what a user is most likely to want given his or her pattern of responses to past results. See James E. Pitkow, Hinrich Schütze, Todd Cass, Rob Cooley, Don Turnbull, Andy Edmonds, Eytan Adar & Thomas Breuel, Personalized Search, 45 *Communications of the ACM* 50 (2002) (discussing methods of personalizing search systems).
11. For a prescient examination of objectification resulting from reductionism here, see Julie Cohen, Examined Lives: Informational Privacy and the Subject as Object, *Stan. L. Rev.* 52 (2000) 1373.
12. ICRs are "dossiers on consumers that include information on character, reputation, personal characteristics, and mode of living. ICRs are compiled from personal interviews with persons who know the consumer." See Electronic Privacy Information Center, Fact Sheet on the Fair Credit Reporting Act, available at http://epic.org/privacy/fcra/.

13. Robert Ellis Smith, Ben Franklin's Website 317 (2000) (discussing routine invasions of privacy by CRA's; "countless reports included the fact that a prospective insured was living 'without benefit of wedlock' "; "unverified rumors of homosexuality" were common; the southern-based Retail Credit Co.'s "young, barely trained 'investigators' prepared reports for insurance companies that reported the drinking habits of consumers . . .").
14. *Id.*, at 316.
15. 15 U.S.C. §1681(a)(1)–(4).
16. 15 U.S.C. §1681(b).
17. 15 USCS 1681a(f).
18. 15 U.S.C. §1681o. This paragraph and the last summarize provisions from 15 U.S.C. §1681.
19. Jonathan Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press, 2008), 227.
20. Viktor Mayer-Schonberger, *Delete: The Virtues of Forgetting in the Digital Age* (Princeton University Press, 2009).
21. Danielle Citron, Technological Due Process, *Washington L. Rev.* (2007).
22. Frank Pasquale, Rankings, Reductionism, and Responsibility, *Clev. St. L. Rev.* 54 (2006) 115; Frank Pasquale, Asterisk Revisited: Debating a Right of Reply on Search Results, 3 *Journal of Business & Technology Law* (2008) 61.
23. Kaimipono D. Wenger, Google Profiles and Online Self-Ownership, available at http://www.concurringopinions.com/archives/2009/04/google_profiles.html.
24. Nissenbaum assists us in understanding the use of the term "privacy" in the general sense as the "power to share information discriminately." Helen Nissenbaum, Privacy as Contextual Integrity, *Wash. L. Rev.* 79 (2004) 119, 121 (citing James Rachels, "Why Privacy is Important," in Ferdinand David Schoeman ed., *Philosophical Dimensions of Privacy: An Anthology* (1984) 290, 294).
25. *Act on the Protection of Privacy in Working Life* (759/2004).
26. For a discussion of the last area of law, see Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, 2000 *Wis. L. Rev.* 743 (2000).
27. For an example of the limits of discrimination law, see Elizabeth Emens, Intimate Discrimination, 122 *Harv. L. Rev.* 1307 (2009) ("legal regulation targeting individual differentiation on these bases [in the intimate domain of sex and love] would be woefully misguided").
28. Ronald Moss, *When All Else Fails: Government as Ultimate Risk Manager* (Harvard University Press, 1999).
29. Richard Posner, *A Failure of Capitalism* (Harvard Univ. Press, 2009); Andrew Ross Sorkin, *Too Big to Fail* (Viking Adult, 2009).
30. J. Hoult Verkerke, Legal Regulation of Employment Reference Practices, 65 *U. Chi. L. Rev.* 115 (1998) ("Prospective employers and regulators confront three analytically distinct problems: falsely negative references, an inadequate supply of reference information, and falsely positive references").

31. *Id.*
32. Dennis D. Hirsch, Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law, 41 *Ga. L. Rev.* 1 (2006).
33. Tal Zarsky, Law and Online Social Networks, 18 Fordham Intell. Prop. Media & Ent. L.J. 741, 780 ("The state should take a proactive role in battling gaming practices transpiring in social networks and move to bring legal action against those engaging in these practices. In doing so, the state could rely on existing legal doctrines and laws, such as fraud, misrepresentation and various laws addressing unfair business practices").
34. Jon D. Michaels, All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror, 96 *Cal. L. Rev.* 901 (2008) (describing in detail favors granted to FedEx and other companies for participation in fusion centers, which combine public and private data about individuals into unified dossiers upon request of homeland security officials); Jack Balkin, The National Surveillance State, 93 *Minn. L. Rev.* 1 (2008).
35. Lior Strahilevitz, Reputation Nation: Law in an Era of Ubiquitous Personal Information, 102 *NW. U. L. Rev.* 1667 (2008).
36. Liz Pulliam Weston, Eight Secret Scores That Lenders Keep, *MSN Money*, available at http://articles.moneycentral.msn.com/Banking/YourCreditRating/8SecretCreditScoresThatLendersKeep.aspx?page=all (describing "complex and largely secret scoring systems"); Liz Pulliam Weston, Your Credit Score, Your Money & What's at Stake (Updated Edition): How to Improve the 3-Digit Number that Shapes Your Financial Future (FT Press, 2009).
37. NAMIC Online, NAMIC's State Laws and Legislative Trends: State Laws Governing Insurance Scoring Practices 1 (2004), available at http:// www.namic.org/reports/credithistory/credithistory.asp.
38. Frank M. Fitzgerald, Comm'r, Office of Fin. and Ins. Serv., "The Use of Ins. Credit Scoring in Auto. and Home Owners Ins.: A Report to the Governor," the Legislature and the People of Mich. (2002), available at www.michigan.gov/documents/cis_ofis_credit_scoring_report_52885_7.pdf; Haw. Rev. Stat. §431:10C–207 (2005).
39. For example, see Birny Birnbaum, Insurer's Use of Credit Scoring for Homeowner's Insurance in Ohio: A Report to the Ohio Civil Rights Commission, 2 (Jan. 2003), available at http://www.cej-online.org/report_to_ohio_civil_rights_commission.pdf.
40. Robert Berners, "Hospitals X-Ray Patient Credit Scores: More and More Are Buying Credit Data to See If the Sick Can Afford Treatment," Businessweek, (December 1, 2008) available at http://www.businessweek.com/magazine/content/08_48/b4110080413532.htm?chan=magazine+channel_what%27s+next.
41. Jonathan Zittrain, The Future of the Internet and How to Stop It (Yale Univ. Press, 2008) 218.
42. Kevin Arrington, Rapleaf Tags, posting to the TechCrunch blog, available at http://www.techcrunch.com/tag/rapleaf/.

43. The next few paragraphs are based on the decision Browne v. Avvo, 525 F. Supp. 2d 1249 (W. D. Wa. 2007).
44. James Grimmelmann, The Structure of Search Engine Law, 90 Iowa L. Rev. 545 (2007).
45. See e.g. Suzuki Motor Corp. v. Consumers Union of United States, Inc., 330 F.3d 1110 (9th Cir. Cal. 2003).
46. See e.g. Complaint & Settlement Announcement, Washington State Medical Association v. Regence BlueShield (2006).
47. See e.g. Bose Corp. v. Consumers Union, 466 U.S. 485 (1984); David J. Grais and Kostas D. Katsiris, Not "The World's Shortest Editorials: Why the First Amendment Does Not Shield the Rating Agencies from Liability for Over-rating CDO's, available at http://www.graisellsworth.com/Rating_Agencies.pdf.
48. See Surgistrategies, Lawsuit: Insurance Commission Physician Tiering Program Flawed, available at http://www.surgicenteronline.com/hotnews/insurance-commission-physician-tiering.html.
49. Id.
50. Id.
51. Physicians and Regence BlueShield Settle Lawsuit, Press Release, August 8, 2007.
52. Id.
53. Id.
54. Attorney General Cuomo Announces Doctor Ranking Agreement with GHI and HIP: Five Insurers in Three Weeks Adopt Model Created Together with National Medical and Consumer Groups, Press Release, November 20, 2007.
55. Molly McDonough, "Cuomo's Doctor-Ranking Model Gains Political Traction," ABA Journal (November 26, 2007) available at http://www.abajournal.com/news/article/cuomos_doctor_ranking_model_gains_political_traction/.
56. Email from Linda Lacewell, chair of the New York Attorney General's Health Care Task Force, to Frank Pasquale, October 27, 2008 ("CIGNA and other plans have agreed to disclose their methodologies to the public").
57. Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).
58. Robert Post, Recuperating First Amendment Doctrine, Stan. L. Rev. 47 (1995) 1249, 1250; Fredrick Schauer, The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience, Harv. L. Rev. 117 (2004) 1765, 1769.
59. Central Hudson Gas & Electric Co. v. Public Service Comm., 447 U.S. 557 at 561–563 (1980).
60. Id.; see also Metromedia v. City of San Diego, 453 U.S. 490 (1981). The regulation must be reasonably tailored to protect the asserted state interest.
61. Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942); Nimmer for locus classicus; Eldred v. Ashcroft, 537 U.S. 186 (2003).