PASSING BEYOND IDENTITY ON THE INTERNET: ESPIONAGE & COUNTERESPIONAGE IN THE INTERNET AGE

Marcy Peek*

INTRODUCTION

In the Internet Age, the means of parsing the identities of consumers have gone digital, and corporate decision-makers routinely use aspects of a person's identity such as age, gender, race, income, and past purchasing behavior to steer information and marketing messages to and away from individuals in cyberspace.[1] Previous assertions that the Internet would represent the ultimate Utopia of race, gender, and class-neutrality have been debunked as legal and social scholars have mapped the many ways in which discrimination occurs online.[2] Similarly, assertions that the World Wide Web would enable the ultimate democracy by and for the people, and that it would dismantle traditional, entrenched boundaries—and the gulf between the "haves" and the "have-nots"—have proven erroneous as these scholars have mapped the many ways in which online profiling and identity-mapping occur. As one scholar notes, "[o]n the Internet, every Web site we visit, every store we browse in, every magazine we skim, and the amount of time we spend skimming it, create electronic footprints that increasingly can be traced back to us, revealing detailed patterns about our tastes, preferences, and intimate thoughts."[3]

Commentators have described such online profiling by different terms; the two most common are "Weblining" and online "steering." "Weblining" refers to "redlining"[4] activities that occur not offline, but rather, in cyber-

---

* Assistant Professor of Law, Whittier Law School, Costa Mesa, California; J.D. *cum laude* 1997, Harvard Law School; B.A. 1993, Yale University.

1. *See generally* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998) (discussing the potential for commercial exploitation of personal data obtained through online transactions).

2. *See generally* Jerry Kang, *Cyber-Race*, 113 Harv. L. Rev. 1130 (2000).

3. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 7 (2000).

4. "Redlining is 'mortgage credit discrimination based on the characteristics of the neighborhood surrounding the would be borrower's dwelling.'" Cara Hendrickson, *Racial Desegregation and Income Deconcentration in Public Housing*, 9 GEO. J. ON POVERTY L. & POL'Y 35, 44 n.71 (2002) (citing Thomas v. First Fed. Sav. Bank, 653 F. Supp. 1330, 1337 (N.D. Ind. 1987)). Another scholar describes redlining as:

> [A] policy whereby a bank effectively draws a red line around low and moderate income communities within its market area and, as a matter of policy, refuses to lend to individuals within those communities. Congress passed the [Community Reinvestment Act] because the practice of red-lining denies credit to individuals

space. In other words, instead of lenders and financial institutions using "real world," offline methods to discriminate financially against individuals based on their residence or situated locale,[5] these same institutions use online methods to accomplish the same result.[6] Similarly, "steering" refers to the practice whereby companies direct individuals to or away from marketing messages or offers based on predetermined identity characteristics; online steering refers to these discriminatory practices taking place online.[7]

Of course, e-commerce businesses would argue that such practices are entirely economically rational and efficient, and that even discriminatory profiling based on characteristics such as race, gender, and ethnicity is acceptable because of economic efficiency.[8]

This essay is concerned with methods of resisting discriminatory steering and marketing in cyberspace. I argue that, where data marketing and steering activities by commercial entities engender the marginalization of certain groups of individuals, technological techniques of resistance and counterespionage—namely "identity passing"—should be implemented by marginalized persons to counteract online profiling.

---

within the red-lined area, even though those individuals might own sufficient assets to collateralize a mortgage.

David K. Hales, *Reallocating Credit: An Economic Analysis of the New CRA Regulation*, 15 ANN. REV. BANKING L. 571, 571 (1996) (footnote omitted). In addition, the Community Reinvestment Act of 1977, Pub. L. No. 95–128, 91 Stat. 1147 (codified as amended at 12 U.S.C. §§ 2901–2908 (2000)), ended redlining as a widespread practice on the part of regulated banks and thrifts, by requiring "each appropriate Federal financial supervisory agency to use its authority . . . to encourage such institutions to help meet the credit needs of the local communities in which they are chartered." 12 U.S.C. § 2901(b). "The mechanism for enforcement was to be 'encouragement' from the federal agencies that routinely supervised depository institutions in detail, together with a significant economic sanction for continued refusal to respond favorably to the 'encouragement.'" Robert C. Art, *Social Responsibility in Bank Credit Decisions: The Community Reinvestment Act One Decade Later*, 18 PAC. L.J. 1071, 1073 (1987). Furthermore, racial and ethnic discrimination in housing credit and finance was made illegal by federal law in the Equal Credit Opportunity Act of 1977, 15 U.S.C. §§ 1691–1691(f) (2000), and the Fair Housing Act of 1968, 42 U.S.C. §§ 3601–3619 (2000).

5. *See generally* Willy E. Rice, *Race, Gender, "Redlining," and the Discriminatory Access to Loans, Credit, and Insurance: An Historical and Empirical Analysis of Consumers Who Sued Lenders and Insurers in Federal and State Courts, 1950–1995*, 33 SAN DIEGO L. REV. 583 (1996) (discussing redlining statutes and enforcement activities).

6. *See generally* Gary A. Hernandez et al., *Insurance Weblining and Unfair Discrimination in Cyberspace*, 54 SMU L. REV. 1953, 1953 (2001) (describing insurance providers use of "Weblining" to profile potential customers).

7. *See* Isaac v. Norwest Mortgage, 153 F. Supp. 2d 900, 903 (N.D. Tex. 2001) (arguing that defendant mortgage lender used "an Internet site to steer potential purchasers to [residential] areas in which the person's race predominates").

8. *See* RICHARD A. EPSTEIN, FORBIDDEN GROUNDS: THE CASE AGAINST EMPLOYMENT DISCRIMINATION LAWS 9 (1992) (arguing that Title VII anti-discrimination laws should be repealed in favor of competitive markets). *But cf. infra* note 42 (noting that the economic defensibility of a practice does not make it legally or socially justifiable).

Such methods are grounded in the principles of anti-subordination jurisprudence. As opposed to the approach of formal equality, which focuses on whether similarly situated persons are treated similarly, the anti-subordination approach focuses on substantive principles, anti-oppression, and substantive results. Therefore, under this approach, societal tools that serve to lessen opportunities or engender domination are called into question, rather than merely unfair formal processes.

I argue that where online profiling disempowers and excludes marginalized groups, it represents a form of subordination based in information control. Therefore, the practical technique of identity passing via technological manipulation must be utilized by individuals in order to counteract these oppressive activities.

Finally, I contend that unlike the stigmatized phenomenon of offline passing, the act of passing online removes this act of resistance from the realm of what is sometimes deemed an attempted denial of one's socially constructed "identity," and moves it further into the realm of one of the most cherished values in American society—the right to privacy and anonymity.[9] This is because cyberspace allows for the constant manipulation of the identity tags that are presented to profilers; in essence, it allows for the *ad infinitum* retooling of one's identity as presented to the world. Once identity tags are subject to constant change, identity passing can be construed as a form of self-controlled anonymity rather than a stigmatized form of identity denial.

Although the concept of fluidity of identity online has been criticized by some commentators as simply another example of the misguided drive toward assimilation and colorblindness, I argue that in the context of exclusionary information control and profiling practices, fluidity of identity is a powerful means of resisting subordination.

I. ONLINE PROFILING: THE PROBLEM OF WEBLINING AND STEERING

A. The Phenomenon of Online Profiling

At the dawn of the Internet age, laymen and scholars alike heralded its possibilities for community and equality. Hopes for the democratizing in-

9. Of course, privacy has many meanings. Three oft-cited conceptions of privacy are: privacy-as-anonymity, privacy-as-autonomy (and control over one's life and personal information), and privacy-as-confidentiality. *See, e.g.*, James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 23 n.84 (2003) (citing DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 7–8 (1989)) (delineating thirteen distinct aspects of privacy deserving of protection).

fluence of the Internet and technology abounded, particularly among liberal social and legal scholars.

But as the Internet grew in size and influence, it also grew in commercial appeal. Almost as soon as the Net took hold as a national and global phenomenon, it became privy to the same corporate hegemonies that have historically controlled the majority of corporate America. Not surprisingly, with this monopolization and homogenization of the Internet, the concept of the "community of the commons" and similar ideals based in principles of Utilitarianism, such as Open Source Code, became less and less of a reality.[10]

Of particular importance to this piece, the Internet has allowed commercial decision-makers to manipulate technology in such a way as to identify persons according to a multitude of variables and categories. This ability to profile Internet users is perhaps one of the most significant, yet ignored consequences of the Internet and, indeed, of the Information Age.

Heretofore, individuals have been socially "marked," often by means of physical appearance. Society uses external indicators to describe a person's "identity"[11] via categories such as race,[12] gender, sexual preference, occupation, and class.

Of course, as society and technology have progressed, ways of marking individuals with "identity tags" have also evolved. Thus, for example, credit reports now assign individuals a number that effectively sums up that person's past work, credit, income, and spending history—and potential marketers, employers, and lenders can access this information simply by typing in a person's Social Security number. Similarly, in the workplace, resumes and letters of reference have taken the place of community knowledge, because the world is much too spread out and people are too disconnected for employers to know each potential employee's background.

---

10. *See, e.g.*, Lawrence Lessig, *The Architecture of Innovation*, 51 DUKE L.J. 1783, 1788 (2002) (explaining how the Internet is a "kind of commons" because it is available for anyone to use without permission).

11. *Cf.* Ellen M. Weinauer, *"A Most Respectable Looking Gentleman": Passing, Possession, and Transgression in* Running a Thousand Miles for Freedom, *in* PASSING AND THE FICTIONS OF IDENTITY 37, 37–38 (Elaine K. Ginsburg ed., 1996) (discussing how William Craft's book *Running a Thousand Miles for Freedom* questions our assumptions of a person's identity based on physical characteristics).

12. In regard to race, this is true both inter-racially and intra-racially. As Judy Scales-Trent, a self-identified Black woman, notes:

> I am so carefully trained in the art of detecting race markers. Most black Americans are: we rely on these physical markers for self-preservation. We scrutinize the person's body, looking for a telltale cast to the skin, certain facial features, a specific hair texture. But there have been many times when even I did not know.

JUDY SCALES-TRENT, NOTES OF A WHITE BLACK WOMAN: RACE, COLOR, COMMUNITY 88–89 (1995).

Thus, pieces of paper containing a summary of identity tags such as class, education, and the like are used to pre-screen individuals.

This use of summary data is important, because identity tags exist precisely for inclusionary and exclusionary purposes.[13] The entity or persons doing the tagging and defining the relevant categories want to know whether the person at issue should be admitted to whatever club, social circle, marketing group, organization, or other societal grouping is at issue.

On the Internet, individuals are identity-tagged via technology. Through various means[14] such as "cookies,"[15] Web bugs,[16] and personal data input such as zip codes, corporate marketers can obtain a person's demographic and other information and "tag" an individual on the basis of such information.[17] This identity tag determines what pop-up, banner, tex-

---

13. *See generally* ERVING GOFFMAN, STRATEGIC INTERACTION 22–23 (1969) (using passports as an example of an identity tag because they "bond an individual to his biography").

14. Roger Clarke, *Information Privacy on the Internet: Cyberspace Invades Personal Space* ("Information technologies have been generating a technological and marketing imperative towards individuals being expected to identify themselves on a routine basis, when conducting transactions that have hitherto been anonymous or pseudonymous.") *at* http://www.anu.edu.au/people/Roger.Clarke/DV/IPrivacy.html (May 2, 1998).

15. A cookie is simply a text file identifier that is placed on your hard drive by a Web page server. It is essentially your identification card that tells the Web page "who you are" every time you return. MERRIAM-WEBSTER DICTIONARY, *available at* http://www.m-w.com/cgi-bin/dictionary (last visited Oct. 10, 2003).

16.

> "Web bugs," also known as "clear GIFs" or "1-by-1 GIFS." . . . are tiny graphic image files embedded in a Web page, generally the same color as the background on which they are displayed. They are one pixel in height by one pixel in length—the smallest image capable of being displayed on a monitor—and are invisible to the naked eye. The Web bug sends back to its home server (which can belong to the host site, a network advertiser or some other third party): the IP (Internet Protocol) address of the computer that downloaded the page . . . ; the URL . . . of the page on which the Web bug appears; the URL of the Web bug image; the time the page containing the Web bug was viewed; the type of browser that fetched the Web bug; and the identification number of any cookie on the consumer's computer previously placed by that server. Web bugs can be detected only by looking at the source code of a Web page and searching in the code for 1-by-1 IMG tags that load images from a server different than the rest of the Web page. At least one expert claims that . . . Web bugs can also be used to place a cookie on a computer or to synchronize a particular email address with a cookie identification number, making an otherwise anonymous profile personally identifiable.

Online Profiling: Benefits and Concerns Before the Senate Comm. on Commerce, Sci. and Transp., 106th Cong. (Jun. 13, 2000) (prepared statement of the Federal Trade Commission), *reprinted in* PRACTISING LAW INST., E-COMMERCE ANTITRUST & TRADE PRACTICES: PRACTICAL STRATEGIES FOR DOING BUSINESS ON THE WEB 297, 303 n.27 (Harry S. Davis & Rebecca P. Dick co-chairs, 2001) [hereinafter *Online Profiling*].

17. *See generally* Hernandez, et al., *supra* note 6, at 1965 (describing a situation where a company categorizes your desirability based on your zip code).

tual, and static ads you see, what information you are steered to, and what information is fed to and away from you.

Such information includes advertisements that would traditionally be deemed unproblematic, such as weight-loss ads or magazine subscription advertisements. However, informational steering includes activities that have traditionally been deemed problematic—because of their discriminatory potential—such as steering certain categories of persons to opportunities for financial discounts, lending opportunities, and preferential low-interest rates.[18] For example, in *Isaac v. Norwest Mortgage*, a mortgage lending company (now Wells Fargo) purportedly used its Internet site to steer potential customers to residential locations in which their race was predominant.[19]

Significantly, the banner ads displayed on the Web sites that you visit online are generally not selected or delivered by that particular Web site, but rather by a handful of network advertising companies "that manage[] and provide[] advertising for numerous unrelated Web sites."[20] These networks do not simply serve up the advertisements that you view online—"they also gather data about the consumers that view their ads."[21]

The end result is that your identity and status is digitally announced over the Internet every time you surf the Net,[22] and marketing messages are

---

18. *See* Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 944–45 (2002) (describing the variety of information that financial institutions gather to develop profiles of their customers, and the potential for abuse of this information).

19. Isaac v. Norwest Mortgage, 153 F. Supp. 2d 900, 906 (N.D. Tex. 2001) (holding that plaintiffs had standing to sue lender under the Fair Housing Act.).

20. *Online Profiling*, *supra* note 16, at 303.

21. *Id.*

22. One online commentator has observed that:

> One of the concerns of privacy advocates is the idea that, as your personal data accumulates and more and more attempts are made to collect, collate, and use that data, a picture of you based on what you do online develops, and those using your data may make decisions affecting your life and livelihood based on that picture. Businesses already routinely track e-mail and Internet activity of their employees while they're at work, and we know that companies such as WebTV, DoubleClick, and Amazon are watching what we're doing at home. How long will it be before someone in Human Resources is charged with the task of researching a potential employee's Internet persona during the hiring process? Will flame wars and X-rated surfing during an idle moment in the "privacy" of your own home be someday held against you? Will the courts let your soon-to-be-ex spouse subpoena your surfing records in a custody/divorce case? Will you even be given a chance to explain?

WebTV Addict, *World Wide Web of Deceit: The Real You*, *at* http://www.net4tv.com/voice/Story.cfm?storyID=2287 (May 7, 2000) (on file with *Vermont Law Review*).

funneled to and away from you on that basis.[23] One organization has objected to this new paradigm by arguing that such profiling tactics, "undermine[] individuals' expectations of privacy[24] by fundamentally changing the Web experience from one where consumers can browse and seek out information anonymously, to one where an individual's every move is recorded."[25] Indeed, "there is a 99% chance that, during a one-month period, a consumer surfing the busiest sites on the Web will visit a site that collects personal identifying information."[26] As a result, "[i]n cyberspace, there is no real wall between public and private. And the version of you being constructed out there—from bits and pieces of stray data—is probably not who you think you are."[27]

Consumer profiling is, of course, not a new phenomenon.[28] It started with simple methods of offline marketing techniques such as junk mail and

---

23.

> [T]he World Wide Web has initiated a paradigm shift regarding the ease and detail of collecting, augmenting, and analyzing the necessary [customer] data. New technology in "data mining" has made it easier for Internet based companies to accumulate data from public records and sales histories, to combine it with information on an individual's Internet usage, and to create a highly detailed profile of an individual.

Hernandez et al., *supra* note 6, at 1970 (footnote omitted).

24. *See generally id.* (documenting the detailed individual profiles companies keep). Notably, in *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Court found an expectation of privacy in detailed computerized records and stated that, "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

25. *Public Workshop on Online Profiling: Testimony of the Center for Democracy and Technology Before the Federal Trade Commission, at* http://www.cdt.org/testimony/991108mulligan.shtml (Nov. 8, 1999) [hereinafter *Public Workshop*] (testimony of Deirdre Mulligan on behalf of the Center for Democracy and Technology).

26 David G. Ries, *Protecting Consumer Online Privacy—An Overview, at* http://www.pbi.org/Goodies/privacy/privacy_ries.htm (May 2001) (quoting *Privacy Online: Fair Information Practices in the Electronic Marketplace Before the Senate Comm. on Commerce, Science and Transportation*, 106th Congress, 9 (May 25, 2000) (prepared statement of the Federal Trade Commission)).

27. Jeffrey Rosen, *The Eroded Self*, N. Y. TIMES MAG., Apr. 30, 2000, at 46, *available at* http://www.nytimes.com/library/magazine/home/20000430mag-internetprivacy.html (last visited Jan. 20, 2004).

28. As Professor Jeffrey Rosen has observed:

> There is nothing new about the fear that technologies of surveillance and communication are altering the nature of privacy. . . .
>
> At the beginning of the 21st century, the Internet has vastly expanded the aspects of private life that can be monitored and recorded. As a result, cyberspace has increased the danger that personal information originally disclosed to friends and colleagues may be exposed to, and misinterpreted by, a less-understanding audience.

Id. at 50–51.

direct marketing. The next level was much more sophisticated, and involved corporations such as financial institutions profiling and evaluating you as a customer, labeling you on the basis of such information, and making snap judgments based on the resulting profiles that determine whether, for example, you are left on hold with your bank for a lengthy five minutes—or a mere five seconds.[29] Similarly, such crude profiles enabled companies to determine whether you were worthy of receiving the select discounts reserved for their best, A-rated customers, or whether you were cut off as a customer altogether.[30]

It is the unique data storage and data mining power of the World Wide Web, combined with the relatively recent ability to combine vast amounts of online, impersonal data with offline data, which makes the new online profiling so powerful, and thus so invasive. Because of new data mining techniques that use neural networks—information processors that mimic human brain behavior to predict a consumer's future online behavior based on past behavior[31]—companies can now easily collect and analyze customer data and public records that previously sat unanalyzed in computer databases. This offline personal data is combined with the personal data gathered online about an individual to produce a highly detailed identity map of a consumer.[32] Once this identity mapping is complete, Web sites and advertising networks use this information, along with unique computer identifiers, to track and monitor individuals' online activities across multiple Web sites in order to predict the purchasing and online traffic behavior of millions of individual consumers.[33]

---

29. *See id.* (discussing the threats online profiling pose to an individual's everyday affairs).

30. Marcia Stepanek, *Weblining*, BUSINESSWEEK ONLINE, Apr. 3, 2000, *at* http://www.businessweek.com/2000/00_14/b3675027.htm (last visited Jan. 20, 2004).

31. *See infra* note 51 (describing neural networks as mechanisms that mimic the human brain).

32. Acxiom Corporation, one of the leading data collectors in the United States, offers a product called InfoBase. Acxiom describes the "InfoBase Enhancement" product as a "database of demographic, lifestyle and behavioral marketing information." The product apparently works by matching company's prospect or customer lists with the extended profiles of those customers that Acxiom has obtained by aggregating the information elsewhere. As Acxiom's product literature explains:

> Data enhancement is the process of overlaying, or supplementing, a marketer's existing customer data or prospect list with additional consumer demographic and lifestyle information such as hobbies or interests and type of car driven. In almost all instances data providers use comparative "string" matching to bring together only similar customer records. However, InfoBase Enhancement now uses the most accurate and reliable method of matching customers and enhancement information—a knowledge-based approach to analyze information in order to match similar, dissimilar and historic representations of a client's records.

Press Release, Acxiom, New Infobase Enhancement Adds Power of AbiliTec to Set New Standards in Match Rates, *at* http://www.acxiom.com/default.aspx?ID=2304&Country_Code=USA (Sept. 9, 2003).

33. For example, Professor Jeffrey Rosen described the activities of a major online ad network in the following way:

As the Center for Democracy and Technology has reported, "[i]n addition to long lists of collected information, a profile may contain 'inferential' or 'psychographic' data—information that the business infers about you based on the behavioral data collected. From this amassed data, elaborate inferences may be drawn, including the individual's interests, habits, associations, and other traits."[34]

Similarly, Time Magazine recently reported, today's psychographics involves the supplementation of:

> [C]onventional marketing data with informed assumptions about personality traits and human behavior gleaned from other disciplines, including psychology, sociology and probability theory. Using computers to organize and manipulate vast storehouses of such consumer information, [market researchers] believe they are getting much better at sorting people into categories of like-minded individuals. And once the sorting is done, they are getting better at predicting how people are likely to behave.
>
> . . . .
>
> The psychographics movement is all about building better pigeonholes . . . .[35]

Even more disturbing, because modern technology allows companies to share such identifying information seamlessly,[36] the demographic information that you innocently—or unknowingly—give to one company may be digitally passed to another company . . . and yet another.[37] Thus, your

---

> DoubleClick, the Internet's largest advertising-placement company, has been compiling anonymous data on our browsing habits by placing "cookie" files on millions of our hard drives. Cookies are electronic footprints that allow Web sites and advertising networks to monitor our online movements with granular precision. Some web sites can monitor the search terms you enter and the articles you skim. After DoubleClick sends you a cookie, you will find yourself receiving targeted ads when you visit the Web sites of its 2,500 clients.

Rosen, *supra* note 27, at 48.

34. *Public Workshop*, *supra* note 25. *See also Online Profiling*, *supra* note 16, at 303 (describing the way in which advertisers use data to compile detailed profiles of individuals in order to target their specific interests).

35. Pamela Paul, *Sell it to the Psyche*, TIME, Oct. 2003 (Bonus Section *Inside Business*).

36. *See, e.g.*, *id.*

> Developments in database technology have made the job easier and cheaper for market-research firms to link databases, creating more detailed consumer profiles. When Hyundai decided to give the psychographic treatment to car buyers earlier this year, it chose LifeMatrix partly because that company's data are linked with information stored at Mediamark Research, which tracks what consumers read.

Id.

37. *See* Hernandez et al., *supra* note 6, at 1965–66 ("Originally, these were readable only by the computer that placed them there, but recent technology has enabled more and more companies to

"preferred" or "non-preferred" status may be digitally announced over the Internet every time you log into a major Web site. In sum, these practices "undermine[] individuals' expectations of privacy by fundamentally changing the Web experience from one where consumers can browse and seek out information anonymously, to one where an individual's every move is recorded."[38]

Almost invisibly, one-dimensional profiles of consumers have become three-dimensional in the Internet Age, and by their silence, consumers have unknowingly allowed private companies to continue this assault on their privacy.

B. The Problematic Aspects of Online Profiling

Companies engaged in the business of online identity profiling argue that such profiling is just traditional American business at work. Such data mining and marketing techniques, they insist, allow targeted personalization and efficiency of marketing efforts as have never before been possible. Indeed, this data warehousing and profiling has become the key strategy upon which many e-businesses, such as Amazon.com, are based.[39] It allows exponentially better customer service and better targeting of prospects. Moreover, it allows companies to precisely predict customer behavior.[40] While data profiling certainly may be financially beneficial for private industry, these processes are problematic for many reasons.[41]

First, cyber-surfers are largely oblivious to the data mining occurring in the background as they surf from Web site to Web site, and they are certainly oblivious to the matching of their offline personal data to their online

---

read and share this information amongst themselves.").

38. *Public Workshop*, *supra* note 25.

39. *See generally* Stepanek, *supra* note 30 (describing Weblining and why companies use personal data to direct specific messages to or away from you).

40. Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 720 (2001).

41. Of course, many practices that are financially lucrative and economically defensible may also be ethically or socially unsound and thus, illegal. *See* Recent Legislation, *Civil Rights—Gender Discrimination—California Prohibits Gender-Based Pricing*—CAL. CIV. CODE §51.6 (West Supp. 1996), 109 HARV. L. REV. 1839, 1843 (1996) (noting that "[u]ltimately, considerations of economic efficiency should be balanced against considerations of justice and nondiscrimination. As scholars have noted, American society has determined that economic efficiency alone cannot justify discriminatory practices"). Such practices are also often the result of misguided conclusions based on erroneous stereotypes that have gone untested in the marketplace. *See* Ian Ayres, *Fair Driving: Gender and Race Discrimination in Retail Car Negotiations*, 104 HARV. L. REV. 817, 850 (1991); *see also* Art, *supra* note 4, at 1080 ("The problem with unrestrained use of location as a primary criterion in mortgage credit decisions is that, in some instances, discrimination against a particular neighborhood may not be rationally based or, even though rational, may produce results that are socially unacceptable.").

personal information. Unless the Web site provides notice regarding an ad network's presence and data collection, consumers are usually totally unaware that most of their online activity is being monitored via their computers' unique identifiers.

This online profiling, steering, and passing of information among companies is virtually always invisible to the user,[42] and "the tendency in the United States is to develop technology that increases data collection and decreases the transparency to citizens of such monitoring."[43]

Second, the matching of *offline* to personal *online* information is an especially troubling practice; the sheer power of the matching process is incredible, due to the in-depth level of identity tracking it enables. As one commentator argues, "the prospect that your real identity might be linked to permanent databases of your online—and off-line—behavior is chilling, because the databases could be bought, subpoenaed or traded by employers, insurance companies, ex-spouses and others who have the ability to affect your life in profound ways."[44]

Third, if an individual were discriminated against on the basis of online profiling, it would be exceedingly difficult to prove that discrimination had occurred.[45] This is especially troubling because American anti-discrimination laws generally require that intent be established for a plaintiff to prevail;[46] even when proof is not hidden in technological black boxes such as the neural networks used in online data mining and profiling,[47] intent is notoriously difficult to prove.[48]

Fourth, there is no accountability in the technological process behind Weblining and online steering. An individual has no opportunity to view the personal data held by data collectors or to rectify inaccuracies. Moreover, background decisions, steering methods, and discriminatory practices

---

42. *See, e.g.*, Hernandez et al., *supra* note 6, at 1965 ("New technology can make [zip code redlining] particularly surreptitious, because it is no longer necessary for an internet user to enter their zip code on that particular site or even on that day. Through the use of 'cookies,' websites deposit information about the Internet user on his or her hard drive.").

43. Reidenberg, *supra* note 40, at 723.

44. Rosen, *supra* note 27, at 49.

45. *See, e.g.*, Stepanek, *supra* note 30 ("[Consumers] will never be shown their data. And scientists who devise these programs admit that they can't vouch for their accuracy, or even say how they reach a specific conclusion.").

46. *See generally* Barbara J. Flagg, *"Was Blind, but Now I See": White Race Consciousness and the Requirement of Discriminatory Intent*, 91 MICH. L. REV. 953, 961–62 (1993) (discussing the requirement of discriminatory intent in American anti-discrimination and constitutional law).

47. *See infra* notes 51, 52.

48. *See* Shayna S. Cook, *Repairing the Legacy of* I.N.S. v. Elias-Zacarias, 23 MICH. J. INT'L L. 223, 244 (2002) (attributing the difficulty of proving discriminatory intent in the context of asylum adjudications to the amount of unknown and, perhaps, unavailable information).

may be—and often are—based on false and/or out-of-date information.[49] Worse, scientists overwhelmingly agree that data systems are virtually always fraught with inaccuracies.[50]

The "neural networks" used by data mining companies to predict consumer behavior were originally developed for use in artificial intelligence projects; they basically mimic human brain behavior to predict a customer's future online behavior based on his or her past behavior. As discussed, the data mining companies obtain this information on past behavior by merging data from multiple Web sites and then combining it with personal data from other sources such as public information and other offline information. But the fundamental problem with neural networks is that they are essentially "black boxes," i.e., once they start running, the engineers who built them have no idea what assumptions and conclusions about human behavior the neural networks are making.[51] Moreover, these neural networks in many

---

49. Professor Jeffrey Rosen argues that:

> [P]rivacy protects us from being misdefined and judged out of context. This protection is especially important in a world of short attention spans, a world where information can easily be confused with knowledge. When intimate personal information circulates among a small group of people who know you well, its significance can be weighed against other aspects of your personality and character. . . . But when your browsing habits or e-mail messages are exposed to strangers, you may be reduced, in their eyes, to nothing more than the most salacious book you once read or the most vulgar joke you once told. And even if your Internet browsing isn't in any way embarrassing, you run the risk of being stereotyped as the kind of person who would read a particular book or listen to a particular song. Your public identity may be distorted by fragments of information that have little to do with how you define yourself. In a world where citizens are bombarded with information, people form impressions quickly, based on sound bites, and these brief impressions tend to oversimplify and misrepresent our complicated and often contradictory characters.

Rosen, *supra* note 27, at 48–49.

50. *See* Gertz, *supra* note 18, at 956 n.59 ("Neural networks have been criticized as 'black boxes' that produce a decisioning system that is impossible to audit for discriminatory criteria.").

51. In explaining the process of neural networks, which were in fact precisely designed to operate like black boxes in order to mimic the operation of the human brain, one source explains that the relationship between the "input" data and the "output" data is poorly understood:

> Neural networks are an information processing technique that offer [sic] solutions to problems that cannot be explicitly formulated. Neural networks mimic the mechanisms of human brains: they learn from examples and store the knowledge for future use. Here, the example fed into a neural network consists of the values of descriptive variables of a system (inputs) and the corresponding responses of the system (outputs). Through learning from a certain number of such examples, the neural network can adjust its own architecture to capture the intrinsic relationship between the inputs and outputs. This kind of "black-box" type functionality makes the neural network attractive to situations where the relationship between the inputs and outputs is poorly understood, which usually is the case in biological systems.

Wei Shou Hu's Group, Current Research, Neural Network *at* http://www.hugroup.cems.umn.edu/

ways are no more "scientific" in terms of the decision-making processes than a human decision-maker would be, because they incorporate human biases.[52]

Fifth, online profiling is problematic because much of this personal data is especially sensitive. For example, medical, legal, sexual orientation, religious affiliation, and racial or ethnic background are but a few categories of sensitive—and in some cases, potentially damaging—identity characteristics that individuals would not want captured without their explicit knowledge and consent.

As the Federal Trade Commission has argued,

> The result [of online profiling] is a profile far more comprehensive than any individual Web site could gather. Although much of the information that goes into a profile is fairly innocuous when viewed in isolation, the cumulation over time of vast numbers of seemingly minor details about an individual produces a portrait that is quite comprehensive and, to many, inherently intrusive.[53]

C. Online Profiling as a Discriminatory Tool

It is crucial to understand that online profiling represents something larger than just junk mail and direct marketing; it is also a representation of the ways in which hierarchies of *information access* are played out every day in cyberspace, and the ways in which the steering of persons to or away from information and opportunities is accomplished via a process that works precisely because it is invisible. As is widely understood, information and knowledge are power. In the context of online profiling, "Weblining systematically limits the cultural and economic choices presented to different groups. . . . [Some people and consumers are] judged to be of minimal value [and] will never have the products and services channeled to

---

Research/plant/neural.htm (last visited Sep. 8, 2003) (on file with *Vermont Law Review*). *See also* Artificial Neural Network Investing, *Product Information, at* http://www.neuralinvesting.com/infopredict.htm (last visited Sept. 6, 2003) ("The black box theory is very important in understanding what a [neural network] is doing. With the black box theory you have input on one side, a process that happens inside the black box which you can't see, then an output from the other side.").

52. *See* Gertz, *supra* note 18, at 961 n.91 ("Neural networks are known for making generalizations that are not contextually defined and thus could produce inapposite conclusions that exceed the most egregious form of discrimination.").

53. *Online Profiling*, *supra* note 16, at 304.

[them]—or the [same] economic opportunities—that flow to others over the Net."[54] Weblining creates situations in which

> products might be offered at higher prices to consumers whose profiles indicate that they are wealthy, or insurance might be offered at higher prices to consumers whose profiles indicate possible health risks. This practice . . . raises many of the same concerns that "redlining" and "reverse redlining" do in offline financial markets.[55]

Redlining is understood as not only having a negative economic effect on the "disenfranchised," but also as creating a more subtle dynamic of "stigmatization [that] decreases one's ability to 'secure basic rights of citizenship.'"[56]

For example, in regard to race, one commentator points out that "too many African-Americans cannot gain access on anything approaching equal terms to social resources that are essential for human flourishing, but that are made available to individuals primarily through informal, culturally mediated, race-influenced social intercourse."[57] Similarly, another commentator argues that, "[b]eyond the individual forms of racism that stereotyping, bias, and hostility represent lie the vast terrains of institutional racism—the maintenance of institutions that systematically advantage whites."[58]

Significantly, those on opposite sides of the (albeit, ever-narrowing) "digital divide" have different levels of knowledge regarding online surveillance and web-lining[59] and, often, different levels of technological expertise in regard to combating such practices. At least one commentator has described this as a privacy divide which falls along socioeconomic lines: "[a]nonymity isn't dying—it's moving to a pricier neighborhood. As pay-for-privacy develops, people who can't afford anonymity are forced to wander the Net in full-disclosure mode."[60]

---

54. Stepanek, *supra* note 30.

55. *Online Profiling*, *supra* note 16, at 304 n.43.

56. Hernandez et al., *supra* note 6, at 1956.

57. GLENN C. LOURY, THE ANATOMY OF RACIAL INEQUALITY 168 (2002).

58. Flagg, *supra* note 46, at 959.

59. *Cf.* Hernandez et al., *supra* note 6, at 1958 (noting that in instances of Weblining, "the poor who would benefit the most from discounts are the most likely to be without awareness or access to them").

60. John Simons, *The Coming Privacy Divide*, INDUS. STANDARD, Feb. 28, 2000, *at* http://www.newamerica.net/index.cfm?pg=article&pubID=146 (last visited Jan. 20, 2004).

Thus, the ultimate problem is not just that online profilers intrude into our privacy zones and survey our personal space[61] via "inherently unfair and deceptive" methods,[62] nor is it just that, as at least one commentator has argued, with the taking of our personal information they take from us a feeling of dignity and humanity.[63] Rather, in the new paradigm, corporations and those holding the power of information distribution and access have the technological capability to determine who has access to information, opportunities, financial offers, and certain economic advantages.[64] As one critic has remarked, "[t]he more personal data that e-retailers compile, the easier it becomes, for example, to engage in online price discrimination. These are schemes in which consumers receive different price quotes on goods depending on where they live or how much money they make."[65]

The seamless online process of diverting less-desirable persons along one informational route, and more-desirable consumers along another is the modern day form of the outlawed practice of redlining.[66] In the insurance context, for example, once a customer is profiled, a website can then:

> [I]mmediately link[] "desirable" customers to a webpage where they can purchase a policy. "Undesirable" customers are channeled to an informational site that does not give them the opportunity to apply for insurance. Similarly, a webpage could offer basic insurance to all Internet users, while also offering a "special" discount only to those within particular zip codes. Profiling can be performed so seamlessly that the potential customer doesn't know that he has been denied access or given an offer not available to others.[67]

---

61. Indeed, "statistics [] demonstrate that many consumers are not willing to allow [online] profiling *regardless of whether notice and choice are given.*" FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 16 (June 2000).

62. *Id.* at 14.

63. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1116 (2002) (suggesting that privacy is an essential part of a person's individuality, and of the concept of personhood); *see also* ROSEN, *supra* note 3, at 214 ("Spying on people covertly is an indignity, much like the indignity of harassment itself. It fails to treat its objects as fully deserving of respect, and instead treats them like animals in a zoo, deceiving them about the nature of their own surroundings.").

64. Such identity tagging in cyberspace is "threatening to the private space of even those who have nothing to hide; and much more sinister to those many people who have experienced repression from other individuals, organisations, or nation-states." Clarke, *supra* note 14.

65. Simons, *supra* note 60.

66. Hernandez et al., *supra* note 6, at 1965 ("With the emergence of the Internet, insurance companies will have new opportunities [to exclude] potential customers based on their geographic location.").

67. *Id.*

This is a vastly different universe than the one envisioned by many scholars as the Internet revolution was in full swing, a cyberworld in which low barriers to entry would make the Internet the province of the common people, and in which individuals would have a never-ending stream of information sources.[68] Indeed, it is a much different paradigm than some commentators are currently presenting, in which individuals have the power to decide what information they will or will not consume from an ever-expanding array of informational outlets,[69] and in which information "middlemen"—informational decision-makers, so to speak—are purged from the process.[70] This envisioned shifting of the balance of power from a cluster of information sources to individual consumers of information[71] is misguided because it fails to take into account the myriad of ways in which informational power dynamics occur online. The current reality is that although "[t]he Net was once trumpeted as 'the great equalizer,' casting off the burdens of racial, religious or economic discrimination," technological advances and advantages have created a cyberspace in which opportunities and information-flow stratify across lines, making it "possible—and perhaps profitable—for companies to recreate the biases many of us encounter in the physical world."[72]

Of course, there is a distinction to be drawn between traditional forms of (and variations on) media outlets—such as offline newspapers and online magazines—and information produced by marketers, advertisers, and the like. But this distinction does not render the argument of informational power unsound. Rather, it merely echoes the contentions of many commentators and scholars who have documented not only the consolidation of the major media companies and thus the major sources of news and information,[73] but also the narrowing divide between traditional information outlets

---

68. *See generally* Stephen A. Weiswasser, *Role of Technology in Communication*, 21 FORDHAM. INT'L L.J. 439, 440 (1997) (acknowledging and criticizing the view that the Internet will succeed as a mass communication medium).

69. *See* Benjamin Compaine, *Think Again: Global Media*, FOREIGN POL'Y, *at* http://www.foreignpolicy.com/story/cms.php?story_id=1921 (last visited Jan. 20, 2004) (arguing that "[t]he notion of the rise of a handful of all-powerful transnational media giants is . . . vastly overstated").

70. ANDREW L. SHAPIRO, THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 55, 57 (1999).

71. MIKE GODWIN, CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE 91–92 (1998).

72. Simons, *supra* note 60.

73. *See generally* C. Edwin Baker, *Media Concentration: Giving up on Democracy*, 54 FLA. L. REV. 839 (2002) (discussing the extent of consolidation of media companies and problems posed). *But see* Compaine, *supra* note 69 (arguing that "the notion of the rise of a handful of all-powerful transnational media giants is . . . vastly overstated").

such as the mass media, on the one hand, and commercial distributors of information on the other.

II. TOOLS OF RESISTANCE

A. Anti-Subordination Theory & Cyber-Resistance

Normatively, the argument could be made that the solution to discriminatory tactics and steering online is redressed through the traditional anti-discrimination laws and by legislative recourse.[74] That is to say, discrimination online could be redressed just as it is offline: through the judicial process and legislative solutions. But this approach is too narrow from a critical perspective, because American anti-discrimination law as judicially interpreted is formalistic in principle and often ineffective in application.

Critical scholars argue that anti-discrimination law and principles are applied in a misguided and results-oriented fashion, i.e., formalistically. "Under formal equality, the law treats similarly situated persons the same" and requires "that goods should be distributed according to merit and all individuals are able to compete equally if treated equally."[75]

Formalism assumes an inherent neutrality and objectivism in American law. The move made by post-modernist critical scholars has been to envi-

---

74. I do not argue that our current laws do not address some discriminatory forms of steering and redlining tactics; clearly, such activities conducted online should be deemed illegal if they would be deemed illegal offline (although this is uncharted judicial territory). Thus, for example, the Equal Credit Opportunity Act (ECOA), 15 U.S.C. § 1691(a)–(f) (2000)—which governs credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or because an applicant derives income from public assistance—targets lenders who engage in discriminatory acts such as offering less favorable loan rates to residents of minority neighborhoods. *See* Hernandez et al., *supra* note 6, at 1964 (arguing that "weblining . . . may incur the displeasure of courts and regulators"). The ECOA should clearly be just as enforceable online in regard to such predatory activities as it is offline. (Also, the Truth in Lending Act, 15 U.S.C. §§ 1601–1667 (2000)—and its implementing Regulation Z, 12 C.F.R. § 226—require that accurate disclosure of the cost and terms of credit be provided to consumers before the consummation of the transaction. Moreover, the Fair Debt Collection Practices Act, 15 U.S.C. § 1692 (2000), prohibits certain unfair and deceptive collection practices by third party debt collectors.) In addition, laws have recently been enacted in a handful of states to prohibit specific Weblining tactics, such as insurance redlining. Thus, for example, California's Proposition 103 forbids special discounts to customers in specified states who purchase insurance policies online; such selective discounts are forbidden under the California law because they cannot be uniformly offered to the public. *See* CAL. INS. CODE § 1861.02 (West 1998) (limiting insurance discounts to drivers based upon driving record, number of miles driven annually, and number of years of driving experience, to the exclusion of discounts based on customer zip codes). New York also forbids such selective discounts presumably because they discriminate against people who do not have online access. N.Y. INS. LAW § 2324(a) (McKinney 2000 & Supp. 2003).

75. Arlene B. Mayerson & Silvia Yee, *The ADA and Models of Equality*, 62 OHIO ST. L.J. 535, 538 (2001).

sion a system of justice in which discrimination is viewed not through the lens of formal categorizations, but rather through the lens of a contextualized, person-centered analysis of subordination and oppression.

Critical jurisprudence—particularly as elucidated by critical race theorists—asks us to "look[] to the bottom"[76] and examine the oppressive nature of practices and human relations from the perspective of the disadvantaged and disenfranchised instead of merely asking whether formal equality has been achieved. Formalism as a jurisprudential mode of analysis views literal, formal, one-to-one equality as an end in and of itself. But the critical principles of feminists and critical race theorists direct us to question practices and institutions that perpetuate systems of privilege and the subordination of marginalized or disadvantaged groups and to "expos[e] the [biased] nature of ostensibly neutral norms"[77]—not merely the ultimate perceived neutrality of the distribution of rights. Indeed, the anti-subordination principle is inherent in the concept that some practices—such as redlining—while perhaps economically defensible, are also deemed "unfairly discriminatory" by society and thus illegal.[78]

The principles of anti-subordination and anti-oppression, rather than formalism, must be applied to the practice of online profiling to truly understand its oppressive aspects. Such principles allow us to avoid the mistake of "overlook[ing] structural disadvantage" and instead "call[] for *equalizing treatment* by redistributing power and resources in order to rectify inequities and to achieve real equality."[79]

Utilizing an anti-subordination approach to online steering, we can begin to understand that oppression lies in the privilege that is a part of institutional practices such as profiling and Weblining, and that is such a deep part of the background society that it is rendered invisible. In fact, under the anti-subordination concept of oppression, intent and deliberate action—so vital to Fourteenth Amendment claims—become unnecessary inquiries, and we can instead look to the more important questions regarding informational domination and the institutionalized patterns of power inherent in the practice of online profiling.

Thus, for example, the precepts behind anti-subordination critiques of anti-discrimination law are that the focus of laws and lawmakers should be on the substantive result achieved, not on the formal process, or mere indi-

---

76. Mari J. Matsuda, *Looking to the Bottom: Critical Legal Studies and Reparations*, 22 HARV. C.R.-C.L. L. REV. 323, 324–35 (1987).

77. Kimberlé Williams Crenshaw, *Race, Reform, and Retrenchment: Transformation and Legitimation in Antidiscrimination Law*, 101 HARV. L. REV. 1331, 1331 (1988).

78. Hernandez et al., *supra* note 6, at 1953.

79. Cheryl I. Harris, *Whiteness as Property*, 106 HARV. L. REV. 1707, 1788 (1993).

vidual offenders. For instance, in the context of equal protection analysis, anti-subordination theorists argue that our anti-discrimination law focuses on a rigid conception of equality that forces marginalized and powerless groups into a comparison mode of analysis, i.e., it asks whether one person is equally situated vis-à-vis another person.

Employing the anti-subordinationist approach exposes the faulty reasoning inherent in applying formalistic principles to Weblining and online steering practices. For example, from a traditional, formal perspective, all persons in the informational marketplace are deemed to stand in equal stead to each other and to have equal opportunity and access to information flow. Hence, that marketers choose to market differentially to certain persons is of no consequence and is, in fact, in keeping with the American law of supply and demand. Such a "restrictive vision . . . treats equality as a process, downplaying the significance of actual outcomes."[80]

In contrast, the anti-subordination approach calls into question societal tools, advantages, and disadvantages that serve to lessen opportunities or engender subordination, oppression, or exclusion of certain individuals or certain classes of individuals. Accordingly, online profiling practices should be deemed problematic when they facilitate and serve to perpetuate hierarchies and inequalities in society. This is particularly true where such practices are part of a broader institutionalized system of privilege that is so inherent in our society that it has become invisible and thus *a priori* acceptable.

If I am deemed not to "matter" economically, if I do not have access to certain information, or if I am simply allowed limited purchasing access and power as a result of online profiling, not only have I been a victim of institutionalized systems of information hierarchies, but I have been subjected to a system of "exclusivity . . . predicated not on any intrinsic characteristic, but on the existence of the symbolic 'other.'"[81] As Professor Jerry Kang has remarked, "personal information is what the spying business calls 'intelligence,' and such 'intelligence' helps shift the balance of power in favor of the party who wields it."[82]

To ignore the oppressive aspects of informational profiling and steering is to make the formalistic and, I argue, wrongheaded argument that such practices simply reflect rational economic practices rather than tactics that engender multiple forms of subordination. It is also to make the misguided and hegemonic assumption that the existing way of doing things is inevitable and inherently correct.

---

80. Crenshaw, *supra* note 77, at 1342.

81. Harris, *supra* note 79, at 1789.

82. Kang, *supra* note 1, at 1215 (footnote omitted).

In other words, we must examine "all the ways in which the system seems at first glance basically uncontroversial, neutral, acceptable."[83] The lack of acknowledgement of the oppressive effects of information steering echoes

> Antonio Gramsci's notion of "hegemony," i.e., that the most effective kind of domination takes place when both the dominant and dominated classes believe that the existing order, with perhaps some marginal changes, is satisfactory, or at least represents the most that anyone could expect, because things pretty much have to be the way they are.[84]

B. Identity Passing in Cyberspace

I argue for the utilization of online passing as a means of resisting profiling in cyberspace.

In the online context, because the decision-makers and information outlets have discrete categories by which people are type-cast and sorted,[85] an online consumer can simply "pass" by "expressing" to the decision-makers that she is, for example, whoever she wants the data collectors and profilers to *think* she is.[86] Because the decision-makers are entirely dependent on the information provided by the consumer/subject, they must use the subject's expression of her identity tags—what Erving Goffman called "sign-vehicles"[87]—to sort her identity. This is but one variation of the classic mistake, particularly peculiar in cyberspace, of "mistaking information for knowledge."[88] In other words, Essentialism and practices based therein "suffer[] from the phenomenon of the synecdoche . . . where the part comes to stand for the whole."[89]

The notion of identity passing online is an example of wielding the "master's tools" in order to "dismantle the master's house."[90] Because in-

---

83. Robert W. Gordon, *Some Critical Theories of Law and Their Critics*, *in* THE POLITICS OF LAW: A PROGRESSIVE CRITIQUE 641, 647 (David Kairys ed., 3d ed. 1998).

84. *Id.* at 647–48.

85. *See generally* Rosen, *supra* note 27 (explaining how companies and individuals are able to invade our privacy by tracing our online activities).

86. *See* Margaret Chon, *Erasing Race?: A Critical Race Feminist View of Internet Identity-Shifting*, 3 J. GENDER RACE & JUST. 439, 451–62 (1999-2000).

87. ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 1 (The Overlook Press 1973) (1959).

88. ROSEN, *supra* note 3, at 200.

89. *Id.* at 202.

90. *See* Paul Butler, *Racially Based Jury Nullification: Black Power in the Criminal Justice System*, 105 YALE L.J. 677, 680 & n.10 (1995) (citing AUDRE LORDE, SISTER OUTSIDER 110 (1984))

formation gatherers use stock, stereotyped notions of identity, they fail to understand or digitally capture the intersectional, complex nature of identity. Of Essentialism and intersectionality, Trina Grillo wrote:

> Each of us in the world sits at the intersection of many categories: She is Latina, woman, short, mother, lesbian, daughter, brown-eyed, long-haired, quick-witted, short-tempered, worker, stubborn. At any one moment in time and in space, some of these categories are central to her being and her ability to act in the world. Others matter not at all. Some categories, such as race, gender, class, and sexual orientation, are important most of the time. Others are rarely important. . . .
>
> . . . .
>
> . . . [W]e all stand at multiple intersections of our fragmented [] selves.[91]

Online purveyors and disseminators of information, advertisements, access, and preferential passes are no less guided by stereotypes and biases than the typical person. As one commentator on the dynamics of human behavior notes:

> Our cognitive miserliness emerges in the tendency to use categories and stereotypes to form impressions about people, regardless of the person's own behavior. . . . [T]he impression you make is also the result of your observers' preconceived biases and stereotypes. . . . We choose the speediest route we can to form an impression, even if it leads to some misperceptions and mistakes. Often, that route means pigeonholing an individual based on the person's apparent similarity to a social category that already has, in our minds, personality attributes associated with it.[92]

In truth, we cannot hope to "know" someone's "identity" by mining and monitoring their data and their activities. Of racial identity, for example, one scholar presents the following conundrum: "[H]ow can you and I be sure when the players themselves do not know? Do not know *yet*? May never know?"[93]

(arguing that racially-based jury nullification is an example of using the master's tools to dismantle his house, and noting that his use of Audre Lorde's phrase is a "corruption" of her argument that "the master's tools can 'never' dismantle the master's house").

91. Trina Grillo, *Anti-Essentialism and Intersectionality: Tools to Dismantle the Master's House*, 10 BERKELEY WOMEN'S L.J. 16, 17–18 (1995).

92. PATRICIA M. WALLACE, THE PSYCHOLOGY OF THE INTERNET 21 (1999).

93. SCALES-TRENT, *supra* note 12, at 89.

Therefore, because online profilers and data collectors rely on a cluster of readily identifiable identity tags by which they categorize individuals online, profiled persons can manipulate the process by "passing." This subversion is a specific example of what at least one commentator has called putting on "virtual blinders"[94] in cyberspace, thereby utilizing the power of the cyberspace realm "as a force for good—to reconstruct the right to read and speak anonymously."[95]

The act of passing, in general, is effective because society's conception of a person is centered in that person's representation of herself.[96] As Goffman observed, it is in an individual's interest

> to control the conduct of the others, especially their responsive treatment of him. This control is achieved largely by influencing the definition of the situation which the others come to formulate, and he can influence this definition by expressing himself in such a way as to give them the kind of impression that will lead them to act voluntarily in accordance with his own plan.[97]

This informational manipulation is just as pertinent in the online world as it is offline.[98]

At least one court has recognized the power of passing online, remarking that "false identification [is a way] to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy."[99]

Indeed, people of color, gays, and lesbians—to name prominent examples—are often quite adept at employing such "passing" techniques to their

---

94. ROSEN, *supra* note 3, at 168; *see* Lori Kendall, *Meaning and Identity in "Cyberspace": The Performance of Gender, Class, and Race Online*, 21 SYMBOLIC INTERACTION 129, 149 (1998) (observing that "the lack of physical markers can result in freedom from harassment").

95. ROSEN, *supra* note 3, at 168.

96.

> The original meaning of the word "person," as the sociologist Marcel Mauss notes in his essay on the evolving notion of personhood, was exclusively that of a mask. In Pueblo Indian cultures, Mauss observes, the symbol of personhood was the mask that members of the clan wore in sacred dramas.

Id. at 218.

97. GOFFMAN, *supra* note 87, at 3–4 (footnote omitted).

98. Laurence Summers, United States Treasury Secretary, points out that, "[a]s identity becomes more digital, it becomes possible to reproduce and take on the identity of another (person) much more rapidly." NAT'L NOTARY ASS'N, A POSITION ON DIGITAL SIGNATURE LAWS AND NOTARIZATION, *available at* http://www.nationalnotary.org/userimages/digitalSignature.pdf (last visited Sept. 9, 2003).

99. Am. Civil Liberties Union v. Miller, 977 F. Supp. 1228, 1233 (N.D. Ga. 1997); *see also* Anita L. Allen, *Lying to Protect Privacy*, 44 VILL. L. REV. 161, 170–71 (1999) (indicating that "there are several distinguishable dimensions of privacy that a person might seek to secure through deception").

advantage,[100] precisely because it has often been situationally advantageous.[101] As I have argued, because those in the privileged position of "observer" rely on Essentialistic, preconceived notions[102] to identify race, class, gender, and other socially-constructed categories, passing is a matter of using technology to adopt certain identity tags as defined by profilers.[103] Hence, the data collectors' failure to recognize the complexity of individuals, and the intersectional nature of human identity, allows the subject group to "pass."[104]

Of course, just as identity is intersectional, those in the position of privilege and those in a subordinated status shift and change according to context.[105] While the subject/object relationship may change, the dynamic of online profiling does not.[106]

---

100. *See* Kitty Calavita, *The Paradoxes of Race, Class, Identity and "Passing": Enforcing the Chinese Exclusion Acts, 1882–1910*, 25 LAW & SOC. INQUIRY 1, 26–31 (2000). "Much as . . . others . . . have discussed the ways that indigenous peoples may take over the colonial law and culture that is imposed on them and fashion it as a tool of resistance, so Chinese immigrants were able to exploit the contradiction between cultural assumptions about the intrinsic nature of identity and the reality of its social construction." *Id.* at 2; *see* Kenji Yoshino, *Covering*, 111 YALE L.J. 769 (2002) (analyzing three forms of assimilation—conversion, passing, and covering—practiced by homosexuals).

101. *Cf.* Mari J. Matsuda, *Voices of America: Accent, Antidiscrimination Law, and a Jurisprudence for the Last Reconstruction*, 100 Yale L.J. 1329, 1332 (1991) (discussing the covering or downplaying of foreign accents, and the way in which "prejudice and status assumptions are tied inextricably to speech evaluation").

102. Indeed, the most "obvious" stereotypes and categories are generally used to build initial assumptions and impressions of another person. "At any moment in time, some of your social categories are more accessible than others, and you will be more likely to use the ones closest to the surface to form an impression of a newcomer. This effect is known as *priming*." WALLACE, *supra* note 92, at 25.

103. Of course, members of privileged groups can, and do, pass as members of underprivileged groups for various reasons. *See, e.g.*, Kali Tal & Gene Lyman, *Room Full of Mirrors: Virtual Tourism and First World Technogaze*, *at* http://www.freshmonsters.com/kalital/Text/Articles/artbyte.html (last visited Sept. 2, 2003) (describing a type of "identity tourism" where "in ostensibly all-black forums, black netters can tell story after story of catching out whites who attempt to pass").

104. In regard to race, one scholar has observed that:

> Blackness and whiteness as they emerge in the passing narrative belie the possibility of identity or authenticity that would allow one to be unequivocally black or white. Passing insists on the fallacy of identity as a *content* of social, psychological, national, or cultural attributes, whether bestowed by nature or produced by society; it forces us to pay attention to the *form* of difference itself. In the case of race in the United States, difference is named and produced on the "color line." Passing plays on this line, exposing racial difference as a continually emerging distinction empty of any essential content.

Samira Kawash, *The Autobiography of an Ex-Coloured Man: (Passing for) Black Passing for White*, *in* PASSING AND THE FICTIONS OF IDENTITY 59, 63 (Elaine K. Ginsburg ed., 1996); *see also* Weinauer, *supra* note 11, at 38 (discussing cross-dressing in William Craft's, *Running a Thousand Miles For Freedom* as a means of escaping slavery, and thus, passing).

105. *See* Grillo, *supra* note 91, at 17 ("When something or someone highlights one of [an individual's] categories and brings it to the fore, she may be a dominant person, an oppressor of others. Other times . . . she may be oppressed herself."); *see also id.* at 29.

106. *Id.* at 21.

C. The Dynamics of Passing and Counterespionage in Cyberspace

Passing is, in some ways, much easier in cyberspace than in physical spaces. The old adage that "on the Internet, nobody knows you're a dog" holds true to some extent.[107] But the crucial wrenches in the process of passing, vis-à-vis online information decision-makers and disseminators, are the technological advantages of the data miners and the invisibility of the process.

Thus, the passing dilemma in cyberspace, just as in physical space, becomes a problem of ascertaining the pertinent identity markers[108] being used by the observers. The process of such information gathering by observers is what Erving Goffman called "uncovering," whereas "counter-uncovering" is the process by which those observed defend against such identification.[109] If the observed persons can accurately identify the identity markers (the "sign-vehicles") utilized by the informational gatekeepers, it theoretically becomes a relatively simple matter to conduct the Goffman-esque act of "counterespionage"—that is, to first ascertain the test of identity used by the observers and then to subvert these tests by altering expressions of identity in order to slip through or confuse the observers' "gates" . . . and thus successfully "pass."[110]

Under Goffman's theory, acts of "espionage" and "counter-espionage" are directly related to "the individual's capacity to acquire, reveal and conceal information."[111] More specifically, "[j]ust as it can be assumed that it is in the interests of the observer to acquire information from a subject, so it is in the interests of the subject to appreciate that this is occurring and to control and manage the information the observer obtains."[112] If passing, whether online or offline, can be construed as lying, [113] the notion of lying to protect our true identity as a morally acceptable practice rings true:

---

107. *See* Jeffrey Rosen, *I-Commerce: Tocqueville, the Internet, and the Legalized Self*, 70 FORDHAM L. REV. 1, 9 (2001) (quoting Peter Steiner, Cartoon, THE NEW YORKER, July 5, 1993, *available at* http://www.cartoonbank.com) (adding that "no one knows your race, gender, or religion either").

108. *Cf.* WALLACE, *supra* note 92, at 22 ("[i]n the [cyberspace] social niches, the pressure to divulge age, and also gender if it isn't obvious, is relentless. We seem almost paralyzed in a social interaction until we know these two simple facts.").

109. GOFFMAN, *supra* note 13, at 19. Goffman's espionage and counter-espionage are, respectively, methods of spying or espionage—the process of revealing information about others—and methods of resisting such espionage.

110. *See* Yoshino, *supra* note 100, at 773 ("[A]ssimilation is not a simple performance on the part of an agent, but rather a dialectic between an agent and her audiences.").

111. GOFFMAN, *supra* note 13, at 4.

112. Calavita, *supra* note 100, at 10 (quoting GOFFMAN, *supra* note 13, at 10).

113. *Cf.* Allen, *supra* note 99, at 162 (defending the act of "lying to protect sexual privacy [as] consistent with the widespread moral belief and religious doctrine that lying sometimes is a morally justifiable response to others seeking information to which they have no right").

> Sometimes we lie because we do not expect other people to appreciate what we regard as our true identities and the private lives in which our true identities emerge. Sometimes we lie because telling the truth can lead to rejection, ridicule, censure or punishment. Lying can keep the world out and allow us to escape the offensive meanings others assign to our conduct.[114]

Of course, just as the observed attempts to "cover" his or her identity by passing, the observer will counteract by attempting to "uncover";[115] this dance is generally followed by the countermove of "counter-uncovering" by the observed.[116] Just as information gatherers and disseminators use information control to their advantage, so too may the "tagged" individual exert her own form of informational power. Such information "control upon the part of the individual . . . sets the stage for a kind of information game—a potentially infinite cycle of concealment, discovery, false revelation, and rediscovery."[117]

Because persons in a marginalized or disadvantaged position are also often at an informational and technological disadvantage relative to online profilers,[118] counterespionage measures and online passing become a matter of overcoming the barriers of technological access, knowledge and prowess.

While the profilers will develop more sophisticated mechanisms for categorizing and sorting individuals as passing techniques are exposed, the inherent problem in such Essentialist decision-making projects remains,[119] and therefore the decision-makers' attempt to acquire reliable "identity" information from the subject—in short, the entire endeavor of the project—fails. The Essentialism dilemma renders the data miners unable to account for or accurately capture the complexities and fluidity of identity, or the intersectionality of identities and experiences. Of course, the immediate problem could be mitigated by the fine-tuning of questions, until a much more narrowly parsed picture of the subject emerges. But the paradox of

---

114. *Id.* at 177–78.

115. *But cf.* Yoshino, *supra* note 100 (finely parsing the distinctions between different forms of passing, including "covering," and noting that there are distinct forms of passing).

116. GOFFMAN, *supra* note 13, at 19; *See also* Yoshino, *supra* note 100, at 773 (describing assimilation as a dialect between "an agent and her audiences").

117. GOFFMAN, *supra* note 87, at 8.

118. Similarly, those without societal power are often those subject to intrusive privacy violations by the government and other entities. *See* Anita L. Allen, *Coercing Privacy*, WM. & MARY L. REV. 723, 742 (1999) (arguing that "the nominally private sphere may not provide meaningful opportunities for privacy and private choice to certain people and groups").

119. *Cf.* SCALES-TRENT, *supra* note 12, at 91 ("My role is to point out the paradoxes, to emphasize the contradictions until the system collapses of its own inanity.").

the discriminatory project based on identity tags endures: the task of sorting identity always fails because identity is fluid and contextual,[120] and because identity can be manipulated in response to the identity tags utilized by the decision-makers. "[T]he 'problem' of identity, a problem to which passing owes the very possibility of its practice, is predicated on the false promise of the visible as an epistemological guarantee."[121] Any attempt to "fix" another's identity is an attempt to find her authentic, essential identity,[122]—in short, her essence—but, because identity cannot be fixed and knowable, such attempts will always prove fruitless.[123] Ultimately, online profiling fails because it "assumes that the experience of being a member of the group under discussion is a stable one, one with a clear meaning, a meaning constant through time, space, and different historical, social, political, and personal contexts."[124]

D. Rethinking the Implications of Passing

Unlike the phenomenon of offline passing,[125] e.g., passing as a heterosexual or as a White person, the act of passing online displaces this act of resistance from the stigmatized realm[126] of what some would deem an attempted, assimilation-based denial[127] of one's socially constructed "identity",[128] into the realm of what many Americans consider a core value: the

---

120. *See* SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET 15 (1995) ("In my computer-mediated worlds, the self is multiple, fluid, and constituted in interaction with machine connections.").

121. Amy Robinson, *It Takes One to Know One: Passing and Communities of Common Interest*, 20 CRITICAL INQUIRY 715, 716 (1994).

122. *See* Weinauer, *supra* note 11, at 38 (discussing how William Craft, in *Running a Thousand Miles For Freedom*, settles on gender as his protagonist's essential identity).

123. *See* Grillo, *supra* note 91, at 19 (arguing against Essentialism, which is "the notion that there is a single woman's, or Black person's, or any other group's, experience that can be described independently from other aspects of the person—that there is an 'essence' to that experience").

124. *Id.*

125. "The scholar G. Reginald Daniel considers passing for white one strategy of resistance for Americans of both European and African descent. He calls it a way of 'subverting the racial divide' by going underground." SCALES-TRENT, *supra* note 12, at 96.

126. *See* LISA NAKAMURA, CYBERTYPES: RACE, ETHNICITY, AND IDENTITY ON THE INTERNET 53 (2002) (discussing race as an elective aesthetic in cyberspace through the use of "heads").

127. *See generally* Kenji Yoshino, *Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of "Don't Ask, Don't Tell,"* 108 YALE L.J. 485 (1998) (discussing the judiciary's encouragement of assimilation by withholding equal protection from members of groups whose "defining traits can be altered or concealed").

128. *See, e.g.*, GAYLE WALD, CROSSING THE LINE 185 (2000) (contending that there are "potential pitfalls of [] a predetermined 'blindness' to collective identities that are at once sites of self-recognition and self-identification and also regulated and enforced by racial ideology"); Grillo, *supra* note 91, at 26 (pointing out the common "fear that multiracial people want to 'get out of' being Black, [and] that [the multiracial movement] is a new form of passing"); Yoshino, *supra* note 100, at 819–20

right to privacy and anonymity. This reconceptualization of passing as an effective means of safeguarding privacy and anonymity is possible precisely because cyberspace allows for the constant manipulation of the identity tags that are presented to profilers; in essence, it allows for the retooling of one's identity as presented to the world *ad infinitum*[129] by constant morphing of identity and by experiencing self-presentation as a fluid process. Once identity manipulation is a daily option and identity tags are subject to constant change,[130] identity passing becomes less a form of stepping into a new identity[131] and more a form of self-controlled anonymity.[132]

Historically, "[t]he right to speak and read anonymously has played a central role in the history of free expression in America."[133] Partially rooted in the constitutional protections against illegal search and seizures grounded in the Fourth Amendment,[134] the value placed on anonymity has guided American norms of citizenship, privacy, and speech.[135]

Similarly, the ability to shape others' perception of oneself by rendering oneself anonymous[136] has roots in the concept of privacy articulated by Louis Brandeis and Samuel Warren: the right to control "to what extent [our] thoughts, sentiments, and emotions shall be communicated to others."[137] As one scholar explains:

(quoting John D'Emilio as stating that "[a]mong activists, coming out of the closet became the gay equivalent to a biblical injunction. Those who remained in the closet had a shadow cast over their moral character. Their integrity was suspect, their courage lacking, their identity uncertain").

129. *See* TURKLE, *supra* note 120, at 14 ("[C]omputer-mediated communication can serve as a place for the construction and reconstruction of identity.").

130. *See* NAKAMURA, *supra* note 126, at 53. The author argues that in online chat rooms, in which individuals are able to choose their own physical appearance, "race is constructed as a matter of aesthetics, or finding the color that you like, rather than as a matter of ethnic identity or shared cultural referents. This fantasy of skin color divorced from politics, oppression, or racism seems to also celebrate it as infinitely changeable and customizable." *Id.*

131. *But see* Kendall, *supra* note 95, at 148–49 (arguing that "anonymity online cannot be classified as an absence of identity characteristics. . . . [A]nonymity carries with it a presumptive identity of whiteness"); *id.* at 149 (arguing that interactions in cyberspace "merely sidestep, rather than call into question, essentialized views of race").

132. *Cf.* Allen, *supra* note 99, at 172. Allen observes that "lying can be motivated by a desire to conceal and facilitate independent choices relating to aspects of life that we usually tag 'private.' People commonly lie to protect their *independence*. *Id.*

133. ROSEN, *supra* note 3, at 168.

134. *See id.* at 169 (noting that the right to read anonymously is rooted in the Fourth and First Amendments).

135. *Cf.* Allen, *supra* note 99, at 172 ("In constitutional law, privacy often signifies independence or autonomy.").

136. *See id.* at 175 ("With lies we desperately try to preserve our freedom and our identities—our actual identities rather than the masks we must wear as a price of admission to conventional mainstream society.").

137. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890).

> In a world of ethnic balkanization and identity politics, in which reasoned deliberation seems difficult because, we're sometimes told, none of us can transcend our racially and sexually and economically determined perspectives, the promise of selective anonymity seems liberating. There's no possibility of being victimized by stereotypes when you speak anonymously.[138]

Thus, the phenomenon of online passing can be lifted out of the realm of stigma,[139] stereotyping,[140] and shame associated with the notion of identity-rejection, and into the realm of personal freedom and transcendence of restrictive and limiting identity tags and stereotyped roles.

While some commentators have criticized the notion of fluidity of identity as a means of escaping stereotypes and harassment online, their argument is concerned with the problem of erasing race[141] and gender (as two examples) in social spaces—whether online[142] or off—for assimilationist purposes, e.g., the problematic aspects of adopting online prostheses in graphical or textual online environments for the purpose of suppressing race or gender in social interactions such as chatrooms.[143] Where, however, passing is employed as a means of countering exclusionary information and economic practices, identity passing in cyberspace takes on a new meaning. Just as economic institutions are forbidden from redlining in real estate

---

138. ROSEN, *supra* note 3, at 178–79.

139. Kali Tal, *The Unbearable Whiteness of Being: African American Critical Theory and Cyberculture*, *available at* http://www.freshmonsters.com/kalital/Text/Articles/whiteness.html (last visited Sept. 8, 2003).

> In cyberspace, it is finally possible to completely and utterly disappear people of color. I have long suspected that the much vaunted "freedom" to shed the "limiting" markers of race and gender on the Internet is illusory, and that in fact it masks a more disturbing phenomenon—the whitinizing of cyberspace. The invisibility of people of color on the Net has allowed white-controlled and white-read publications like WIRED to simply elide questions of race.

Id.

140. *But see* Lisa Nakamura, *Race In/For Cyberspace: Identity Tourism and Racial Passing on the Internet*, *at* http://www.humanities.uci.edu/mposter/syllabi/readings/nakamura.html (last visited Sept. 9, 2003) (arguing that role playing and "identity tourism" on the Internet exacerbate stereotypes).

141. *See generally* RACE IN CYBERSPACE (Beth E. Kolko et al. eds., 2000) (arguing, *inter alia*, that whiteness is the default setting for online culture).

142. *See, e.g.*, Miranda Mowbray, *Does Online Gender Masking Work?*, 11 INT'L J. OF COMM. 105 (2001), *available at* http://www.hpl.hp.com/techreports/2002/HPL-2002-47.pdf (asserting that gender masking may be useful for protecting against online harassment).

143. *See, e.g.*, NAKAMURA, *supra* note 126, at 53 (discussing race as simply a matter of aesthetics in chatrooms); Nakamura, *supra* note 140 (arguing that in online chat communities, "players who choose to perform . . . racial play are almost always white, and their appropriation of stereotyped male Asiatic samurai figures allows them to indulge in a dream of crossing over racial boundaries temporarily and recreationally").

transactions, the subversion of identity tagging online via passing reflects the notion that in certain contexts, taking race out of the equation is a proper means of resisting subordination.

As postmodern scholars have argued, we should all be free to escape the "encumbrances of identity,"[144] particularly where such an escape effectively combats institutional exclusionary practices. Such an ability to transcend limiting "sign-vehicles" is, in many ways, a fundamental aspect of self-expression:

> We are trained in this country to think of all concealment as a form of hypocrisy. But we are beginning to learn how much may be lost in a culture of transparency—the capacity for creativity and eccentricity, for the development of the self and soul, for understanding, friendship and even love.[145]

CONCLUSION

As many commentators have warned, "[i]n the decentralized and global environment of the Internet, the law's impact will be limited. In an area such as privacy, where the government's actions have often been detrimental rather than supportive, we must ask if other options—such as technology may provide stronger protection."[146] Thus, the argument for online passing and technological anonymity is not an exhaustive one; rather, it is a practical argument grounded in the realities of the ever-shifting landscape of the online arena and the present failure of the law to keep pace with activity that takes place in the shadows of cyberspace.

The notion of passing in cyberspace is one that will be transformed into reality only when those who are subordinated by forms of information control have the technological knowledge and skills to implement such passing practices successfully. In some ways, attainment of this technological savvy will be a function of a further narrowing of the shrinking digital divide, but it is more fundamentally a function of eradicating the chasm between those in control of information and access, and those who are the victims of hierarchies of information power and control.

---

144. *See* Allen, *supra* note 118, at 754–55 (arguing that "[w]ithout adequate privacy, there can be no meaningful identities to embrace or escape, and no opportunities to engage in meaningful reflection, conversation, and debate about the grounds for embracing, escaping, and modifying particular identities").

145. Rosen, *supra* note 27, at 129.

146. Jerry Berman & Deidre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 581 (1999).

practices successfully. In some ways, attainment of this technological savvy will be a function of a further narrowing of the shrinking digital divide, but it is more fundamentally a function of eradicating the chasm between those in control of information and access, and those who are the victims of hierarchies of information power and control.