Understanding Privacy Threats Online:
Developing Agency Expertise about Privacy-Eroding Practices

by Frank Pasquale
Professor of Law, Seton Hall Law School
Visiting Fellow, Princeton Center for Information Technology Policy

Abstract

Privacy needs to be at the center of internet policymaking. Yet before they promulgate substantive rules, key administrators must develop an institutional competence for *continually monitoring* rapidly-changing business practices. While the Federal Trade Commission and the Federal Communications Commission have articulated principles for protecting privacy, they have not engaged in the monitoring necessary to enforce these guidelines. This essay promotes institutions designed to develop better agency understanding of privacy-eroding practices. Whether public or private, such institutions would respect legitimate needs for business confidentiality while promoting individuals' capacity to understand how their reputations are shaped by dominant intermediaries.

Internet service providers and search engines have mapped the web, accelerated e-commerce, and empowered new communities. They also pose new challenges for privacy regulators. Google's secrecy about its business practices is well-known, and often frustrates regulators. The Federal Communications Commission (FCC) recently found that another intermediary–Comcast (the nation's largest broadband service provider)—engaged in problematic network management practices. Such network management practices may eventually involve "packet-sniffing" that seriously compromises user privacy. But it took a dogged engineer and investigative reporters months of sleuthing to provoke the agency to investigate.[1] The average customer is not capable of detecting untoward conduct by intermediaries. If intermediary misconduct only negatively affects third parties, users have almost no incentive even to try to detect it.[2]

Just as Danny Weitzner presciently called for an "independent panel of technical, legal and business experts to help [the FTC] review, on an ongoing basis the privacy practices of Google,"[3] the FCC needs to develop the capacity for understanding the ranking practices of the entities it regulates. This capacity could, in turn, enable litigants to submit focused queries to a nonbiased third party that could quickly give critical information to courts mired in discovery disputes in search-related lawsuits. It could also enhance public understanding of intermediaries' data practices.

Competition Erodes Privacy

Leading scholars have modeled privacy as a purchasable commodity: as with other products, individuals have varying preferences and abilities to pay for more or less privacy. On this economistic view, firms will emerge to compete to offer more or less privacy or will provide customers with various "privacy settings" to permit them to tailor their online services. Unfortunately, each of these assumptions is problematic, especially when we reflect on the zero-sum nature of reputational capital in many settings.

Competition is often elevated as a solution to the privacy problem, but few Internet intermediaries do (or even can) compete to grant users more privacy. Instead, carriers are beginning to compete in ways that are corrosive to privacy. As Paul Ohm has documented, "[b]roadband ISPs have . . . search[ed] for new sources of revenue . . . [by] 'trading user secrets for cash,' which Google has proved can be a very lucrative market."[4] While user protests have deterred the most abusive practices, Ohm predicts that "ISPs, faced with changes in technology, extraordinary pressures to increase revenues, and murky ethical rules, will continue aggressively to expand network monitoring." Antitrust law has been slow to recognize privacy as a dimension of product quality, and the competition that it

promotes can do as much to trample privacy as to protect it. Intermediary competition is supposed to provide users with more companies offering more options. However, competition is based primarily on immediately experienced aspects of the service, such as price and speed. The prospect of altering the terms of service for an intermediary like Facebook or Google is beyond the ambition of almost all users.

Even intermediaries with intimate knowledge of users' communications with family and friends have tended to assert almost unlimited powers over user-generated content. The social networking site Facebook attempted to legitimate this power by creating a system that allowed its users to "vote" for changes to the terms of service before they are implemented.[5] However, University of Cambridge researchers have released a detailed report which concludes that Facebook's system is merely "democracy theatre" with little practical effect on the company's operations.[6]

These examples exemplify a common theme: as the use and reuse of personal information becomes more deeply rooted in intermediary business practices, the tension between competition and privacy becomes more pronounced. For example, if a user of one social network wants to join another, she will often be reluctant to do so because of "switching costs"; she has already invested some time and effort in creating her existing profile. The chief way of reducing those costs is to require data portability, which would allow users to take their list of contacts, applications, pictures, and other items with them when they want to leave. However, such a rule (or protocol for data storage) can render the rest of the user's social graph vulnerable to unwanted exposure on the network the user migrates to.7 Randal Picker has described the deep tension between competition and privacy that results, arguing that this tension creates an incentive for greater consolidation of

user information.[8] Given these patterns of industry practice and consumer behavior, privacy regulators' monitoring of oligopolistic online entities will be more effective than waiting for the elusive concept of "privacy competition."

The classic laissez-faire approach here is to assume that the market will address any lingering privacy concerns. Firms will meet a market demand for privacy as individuals exit services that become too invasive of their privacy. However, established social dynamics render that faith in uncoordinated action suspect. Given the steady decline in individuals' expectations of privacy, both privacy and the reputations built on personal information might better be considered irreducibly social goods than some quanta of enjoyments individuals trade off for money.[9] Once commodified, privacy and reputational integrity are inevitably parceled out to rich and poor on differential terms. Moreover, given the frequently abstract "benefits" that privacy and reputational integrity afford, they are often traded away for competitive economic advantage.[10] This process further erodes the societal expectations of privacy that underwrite respect for reputational integrity.[11]

A collective commitment to privacy is far more valuable than a private, transactional approach that all but guarantees a race to the bottom.[12] Network neutrality regulations can include rules that will protect the privacy that market competition, left on its own, will inevitably erode. Ohm even predicts that privacy concerns will "reinvigorate [the] stagnant debate [over network neutrality] by introducing privacy and personal autonomy into a discussion that has only ever been about economics and innovation."[13]

Toward Better Understanding of Privacy-Eroding Practices

Public anxieties about search engines have coalesced around the threats to privacy they pose but ISPs pose at least as great a threat to privacy as Google does, as they have the

opportunity to collect data not just on searches, but on *all* their users' time on the web. Where do we go from here? Public interest groups have made some inroads in holding ISPs accountable, but even they appear reluctant to take the next step to recognize the parallel power of a dominant search engine like Google. Public interest groups will soon have no choice but to confront this dominance, given that the obstacles to holding Google accountable, trade secret protection for its ordering algorithms, will also interfere with network neutrality regulation. Like search engines, carriers face an information overload problem, with spam, viruses, and high-demand applications threatening to overwhelm their networks. They are likely to make key network-management practices as confidential as search engine rankings, and trade secret protection has already been deployed in other technological settings to block critical review of questionable corporate behavior.

The degree of expertise necessary to recognize these externalities in the new online environment is likely to be possessed by only the most committed observers. Only a dedicated group of engineers, social scientists, and computer scientists can be adept enough at understanding search engine decisions as a whole to understand privacy-eroding data practices.

There are some institutional precedents for the kind of monitoring that would be necessary to accomplish these goals. For example, the French Commission Nationale De L'Informatique et des Libertes (CNIL) has several prerogatives designed to protect the privacy of French citizens.[14] For example, CNIL "ensure[s] that citizens are in a position to exercise their rights through information" by requiring data controllers to "ensure data security and confidentiality," to "accept on-site inspections by the CNIL," and to "reply to any request for information."[15] CNIL also grants individual persons rights to obtain

information about the digital dossiers kept on them and their use. For example, CNIL states that French law provides that:

> Every person may, on simple request addressed to the organisation in question, have free access to all the information concerning him in clear language.
>
> Every person may directly require from an organisation holding information about him that the data be corrected (if they are wrong), completed or clarified (if they are incomplete or equivocal), or erased (if this information could not legally be collected).
>
> Every person may oppose that information about him is used for advertising purposes or for commercial purposes.[16]

While the United States does not have the same tradition of protecting privacy prevalent in Europe,[17] the institutional mechanisms pioneered by CNIL could prove worthwhile models for U.S. agencies.

U.S. policymakers may also continue to experiment with public–private partnerships to monitor problematic behavior at search engines and carriers. For instance, the National Advertising Division (NAD) of the Council of Better Business Bureaus is a "voluntary, self-regulating body" that fields complaints about allegedly untruthful advertising.[18] The vast majority of companies investigated by NAD comply with its recommendations, but can resist its authority and resolve the dispute before the FTC.[19] Rather than overwhelming the agency with adjudications, the NAD process provides an initial forum for advertisers and their critics to contest the validity of statements.[20] NAD is part of a larger association called the National Advertising Review Council (NARC), which promulgates procedures for NAD, the Children's Advertising Review Unit (CARU), and the National Advertising Review Board (NARB).[21]

Instead of an "Innovation Environment Protection Agency (iEPA)" (the agency Lawrence Lessig proposed to supplant the FCC), I would recommend the formation of an

Internet Intermediary Regulatory Council (IIRC) to assist both the FCC and FTC in carrying out their present missions.[22] Like the NARC, the IIRC would follow up on complaints made by competitors, the public, or when it determines that a practice deserves investigation. If the self-regulatory council failed to reconcile conflicting claims, it could refer complaints to the FTC (in the case of search engines, which implicate the FTC's extant expertise in both privacy and advertising) or the FCC (in the case of carriers). In either context, an IIRC would need not only lawyers, but also engineers and programmers who could fully understand the technology affecting data, ranking, and traffic management practices.

The IIRC would research and issue reports on suspect practices at Internet intermediaries, while respecting the intellectual property of the companies it investigated. An IIRC could generate official and even public understanding of intermediary practices in a qualified way. An IIRC could develop a detailed description of safeguards for trade secrets, which would prevent anyone outside its offices (including the complainant) from accessing the information.[23] Another option would be to allow IIRC agents to inspect such information without actually obtaining it. An IIRC could create "reading rooms" for its experts to utilize, just as some courts allow very restrictive protective orders to govern discovery in disputes involving trade secrets. The experts would review the information in a group setting (possibly over a period of days) to determine whether a given intermediary had engaged in practices that could constitute a violation of privacy or consumer protection law. Such review would not require any outside access to sensitive information.

I prefer not to specify at this time whether an IIRC would be a private or public entity. Either approach would have distinct costs and benefits explored (in part) by a well-

developed literature on the role of private entities in Internet governance.[24] Regardless of whether monitoring is done by a governmental entity (like CNIL) or an NGO (like NARC), we must begin developing the institutional capacity to permit a more rapid understanding of intermediary actions than traditional litigation permits.[25]

It is not merely markets and antitrust enforcement that are insufficient to constrain problematic intermediary behavior—the common law is also likely to fall short. Examination of carrier and search engine algorithms subject to very restrictive protective orders would amount to a similar barrier to accountability. Moreover, it makes little sense for a court to start from scratch in understanding the complex practices of intermediaries when an entity like the IIRC could develop lasting expertise in interpreting their actions.

Rumors about a person's sexual experiences, health status, incompetence, or nastiness can percolate in blogs and message boards for years. Search engines can then increase the salience of such information, making a single mistake or scandal the dominant image of a person online. Even more chillingly, the subject of such innuendo may never know its influence on important decisionmakers. While many web users assume that they understand how the results generated by their name or business appear generally, we are really only aware of how such results are presented to us *individually*. Personalization permits search engines to present custom-tailored results based on users' past behavior. The degree of expertise necessary to recognize these externalities in the new online environment is likely to be possessed by only the most committed observers.

This potent combination of expertise and externalities is a classic rationale for regulation. As Danny Weitzner's proposal for "extreme factfinding" (in the context of the Google–DoubleClick merger review) recognized, only a dedicated group of engineers,

social scientists, and computer scientists can be adept enough at understanding search engine decisions as a whole to understand any particular claim of invasion of privacy. Someone needs to be able to examine the finer details of the publicly undisclosed operation of culturally significant automated systems.[26]

Conclusion

ISPs 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. When web users attempt to find information or entertainment, they have little assurance that a carrier or search engine is not engaging in unfair data practices.

Those skeptical of the administrative state may find a proposal to "watch the watchers" problematic. They think of intermediaries as primarily market actors, to be disciplined by market constraints. However, the development of dominant Web 2.0 intermediaries was itself a product of particular legal choices about the extent of intellectual property rights and the responsibilities of intermediaries made in legislative and judicial decisions in the 1990s. As intermediaries gained power, various entities tried to bring them to heel—including content providers, search engine optimizers, trademark owners, and consumer advocates. In traditional information law, claims under defamation and copyright law might have posed serious worries for these companies. However, revisions of communications and intellectual property law in the late 1990s provided safe harbors that can trump legal claims sounding in each of these other areas. Some basic reporting responsibilities are a small price to pay for continuing enjoyment of such immunities.

Any policy analysis of dominant intermediaries should recognize the sensitive cultural and political issues raised by them. While economics proceeds on a paradigm of maximizing consumer welfare, this goal is but one of many dimensions along which intermediary performance should be measured. Qualified transparency of intermediary practices would assist policymakers and courts that seek to address the reputational impact of their dominance. New practices like deep packet inspection raise privacy concerns as great, or greater, than Transportation Security Administration screening or EZ-Pass monitoring. Someone must watch the watchers.

Dominant search engines and ISPs are the critical infrastructure for contemporary culture and politics. As these intermediaries have gained more information about their users, they have shrouded their own business practices in secrecy. Internet policy needs to address the resulting asymmetry of knowledge and power. While the FTC and the FCC have addressed privacy in the past, they have not engaged in the monitoring necessary to ensure respect for it. Monitoring based on a principle of qualified transparency would fill this regulatory gap.

References

[1] For a concrete example of the type of investigation required to detect problematic network management practices, see Daniel Roth, *The Dark Lord of Broadband Tries to Fix Comcast's Image*, WIRED, Jan. 19, 2009, at 54, *available at* http://www.wired.com/techbiz/people/magazine/17-02/mf_brianroberts ("It took [a disgruntled Comcast customer] six weeks of short-burst sleuthing [to conclude that] Comcast appeared to be blocking file-sharing applications by creating fake data packets that interfered with trading sessions [because] [t]he packets were cleverly disguised to look as if they were coming from the user, not the ISP."). *See also* Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, Memorandum Opinion and Order, 23 F.C.C.R. 13028 (2008) [hereinafter Comcast Complaint].

[2] For example, if a searcher is indifferent to a certain range of results that a search engine produces, but the search engine unfairly discriminates among the ranking of the results in that range, neither the searcher nor the search engine has an incentive to stop the discrimination. In a world of satisficing searchers, the possible range of results could be large for many queries. Moreover, as search results are increasingly personalized, searched-for entities have a less clear idea of whether their sites are actually reaching searchers.

[3] Danny Weitzner's Blog, What to do About Google and Doubleclick? Hold Google to Its Word with Some Extreme Factfinding About Privacy Practices, http://dig.csail.mit.edu/breadcrumbs/blog/5?page=2 (Oct. 8, 2007, 11:24 EST) ("In the 1990s, the FTC under Christine Varney's leadership pushed operators of commercial websites to post policies stating how they handle personal information. That was an innovative idea at the time, but the power of personal information processing has swamped the ability of a static statement to capture the privacy impact of sophisticated services, and the level of generality at which these policies tend to be written often obscure the real privacy impact of the practices described. It's time for regulators to take the next step and assure that both individuals and policy makers have information they need."). This proposal could be integrated into current FTC practices. *See* Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S J. L. & POL'Y FOR INFO. SOC'Y 723, 727 (2007–2008) (describing an "impressive array of actions . . . to prosecute unfair or deceptive trade practices").

[4] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1420 (arguing that "nothing in society poses as grave a threat to privacy as the ISP, not even Google," and describing the many commercial pressures leading carriers to "monetize[] behavioral data at the expense of user privacy").

[5] Posting of Mark Zuckerberg to the Facebook Blog, Governing the Facebook Service in an Open and Transparent Way, http://blog.facebook.com/blog.php?post=56566967130 (Feb. 26, 2009, 11:20 EST).

[6] JOSEPH BONNEAU ET AL., DEMOCRACY THEATRE: COMMENTS ON FACEBOOK'S PROPOSED GOVERNANCE SCHEME (Mar. 29, 2009), http://www.cl.cam.ac.uk/~jcb82/2009-03-29-facebook-comments.pdf. Bonneau's report has been endorsed by the Open Rights Group. Posting of Jim Killock to Open Rights Group Blog, Facebook's Theatrical Rights and Wrongs, http://www.openrightsgroup.org/blog/2009/facebooks-theatrical-rights-and-wrongs (Apr. 1, 2009) (endorsing Bonneau's study about Facebook's privacy practices).

[7] James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1194 (2009) (arguing against broad regulation requiring data portability on social networks because "it creates horizontal privacy trouble"). Grimmelmann notes that "[e]veryone who has access to 'portable' information on social network site *A* is now empowered to move that information to social network site *B*. In the process, they can strip the information of whatever legal, technical, or social constraints applied to it in social network site *A*. . . . mandatory data-portability rules create a privacy race to the bottom for any information subject to them." *Id.*

[8] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1, 11–12 (2008) ("An uneven playing field that allows one firm to use the information that it sees while blocking others from doing the same thing creates market power through limiting competition. We rarely want to do that. And privacy rules that limit how information can be used and shared across firms will artificially push towards greater consolidation, something that usually works against maintaining robust competition.").

[9] Charles Taylor, *Irreducibly Social Goods*, *in* PHILOSOPHICAL ARGUMENTS 127, 139 (1995) (critiquing both subjectivism and methodological individualism and insisting that irreducibly social goods "exist[] not just for me and for you, but for us, acknowledged as such").

[10] Cass Sunstein and Robert H. Frank suggested in their work on cost–benefit analysis and relative position that those who trade off safety or other intangibles will have additional resources to outcompete peers who refuse to do so. *See* Robert H. Frank & Cass R. Sunstein, *Cost-Benefit Analysis and Relative Position*, 68 U. CHI. L. REV. 323, 327 (2001) (discussing "the central importance of relative economic position to people's perceptions of their own well-being").

[11] *Id.* at 323. The theory of safety in Sunstein and Frank's work applies just as well to privacy. *Id.* at 326 ("[W]hen a regulation requires all [individuals to purchase] additional safety, each . . . gives up the same amount of other goods, so no [one] experiences a decline in relative living standards. [The upshot is that] an individual will value an across-the-board increase in safety more highly than an increase in safety that he alone purchases.").

[12] Siva Vaidhyanathan, *Naked in the Nonopticon*, CHRON. HIGHER EDUCATION, Feb. 15, 2008, at B7 ("When we complain about infringements of privacy, what we really demand is some measure of control over our reputation in the world. Who should have the power to collect, cross-reference, publicize, or share information about us, regardless of what that information might be? . . . 'Self help' [in this context] merely ratchets up the arms race of surveillance.").

[13] Ohm, *supra* note 4, at 1; *see also id.* ("[T]his Article injects privacy into the network neutrality debate—a debate about who gets to control innovation on the Internet. Despite the thousands of pages that have already been written about the topic, nobody has recognized that we already enjoy mandatory network neutrality in the form of expansive wiretapping laws.").

[14] Law No. 78-17 of January 6, 1978, J.C.P. 1978, III, No. 44692. English translation of law as amended by law of August 6, 2004, and by Law of May 12, 2009, *available at*http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf, French language text modified through Law No. 2009-526 of May 12, 2009, J.O., May 13, 2009, *available at* http://www.cnil.fr/la-cnil/qui-sommes-nous/, French language consolidated version as of May 14, 2009, *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&fastPos=1&fastReqId=826368234&categorieLien=cid&oldAction=rechTexte. Commission Nationale de l'Informatique et des Libertés (CNIL), founded by Law No. 78-17 of January 6, 1978, *supra*, is an independent administrative French authority protecting privacy and personal data held by government agencies and private entities. Specifically, CNIL's general mission consists of ensuring that the development of information technology remains at the service of citizens and does not breach human identity, human rights, privacy, or personal or public liberties.

[15] CNIL, Rights and Obligations, http://www.cnil.fr/english/the-cnil/rights-and-obligations/ (last visited Mar. 12, 2010). Specifically, Chapter 6, Article 44, of the CNIL-creating Act provides:

> The members of the "Commission nationale de l'informatique et des libertés" as well as those officers of the Commission's operational services accredited in accordance with the conditions defined by the last paragraph of Article 19 (accreditation by the commission), have access, from 6 a.m to 9 p.m, for the exercise of their functions, to the places, premises, surroundings, equipment or buildings used for the processing of personal data for professional purposes, with the exception of the parts of the places, premises, surroundings, equipment or buildings used for private purposes.

Law No. 78-17 of January 6, 1978, J.C.P. 1978, III, No. 44692, ch. 6, art. 44, *available at* http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf, at 30.

[16] CNIL, Rights and Obligations, *supra* note 15.

[17] James Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1155 (2004) (comparing U.S. and European privacy law).

[18] Seth Stevenson, *How New Is New? How Improved Is Improved? The People Who Keep Advertisers Honest*, SLATE, July 13, 2009, http://www.slate.com/id/2221968.

[19] *Id.* ("When an ad is brought to their attention, the NAD's lawyers review the specific claims at issue. The rule is that the advertiser must have substantiated any claims before the ad was put on the air, so the NAD will first ask for any substantiating materials the advertiser can provide. If the NAD lawyers determine that the

claims aren't valid, they'll recommend that the ad be altered. The compliance rate on this is more than 95 percent. But if the advertiser refuses to modify the ad (this is a voluntary, self-regulating body, not a court of law), the NAD will refer the matter to the Federal Trade Commission. One such FTC referral resulted in an $83 million judgment against a weight-loss company.").

[20] *Id.*

[21] NATIONAL ADVERTISING REVIEW COUNCIL, THE ADVERTISING INDUSTRY'S PROCESS OF VOLUNTARY SELF-REGULATION: POLICIES AND PROCEDURES §2.1(a) (July 27, 2009) ("The National Advertising Division of the Council of Better Business Bureaus (hereinafter NAD), and the Children's Advertising Review Unit (CARU), shall be responsible for receiving or initiating, evaluating, investigating, analyzing (in conjunction with outside experts, if warranted, and upon notice to the parties), and holding negotiations with an advertiser, and resolving complaints or questions from any source involving the truth or accuracy of national advertising."). Though billed as "self-regulation," it is difficult to see how the policy would have teeth were it not self-regulation in the shadow of an FTC empowered by the Lanham Act to aggressively police false advertising. The FTC has several mechanisms by which to regulate unfair business practices in commerce. *See, e.g.*, 15 U.S.C. § 45(b) (2006) (giving the commission the authority to register an official complaint against an entity engaged in unfair business methods).

[22] It could include a Search Engine division, an ISP division focusing on carriers, and eventually divisions related to social networks or auction sites if their practices begin to raise commensurate concerns.

[23] This is the way that the NAD proceeds. It provides specific procedures under which the participants can request that certain sensitive information be protected. *See* NAT'L ADVERTISING REVIEW COUNCIL, THE ADVERTISING INDUSTRY'S PROCESS OF VOLUNTARY SELF-REGULATION § 2.4(d)–(e), at 4–5 (2009), http://www.nadreview.org/07_Procedures.pdf (discussing procedure for confidential submission of trade secrets).

[24] *See, e.g.*, Philip J. Weiser, *Internet Governance, Standard Setting, and Self-Regulation*, 28 N. KY. L. REV. 822, 822 (2001) (examining "in particular the nature and limits of a key private regulator of the Internet: standard-setting organizations and their institution of open, interoperable standards").

[25] Google has already recognized the need for some kind of due process in response to complaints about its labeling of certain websites as "harmful" (due to the presence of viruses or other security threats at the sites) via the Stop Badware program. Zittrain, Future of the Internet, at 171 ("Requests for review—which included pleas for help in understanding the problem to begin with—inundated StopBadware researchers, who found themselves overwhelmed in a matter of days by appeals from thousands of Web sites listed. Until StopBadware could check each site and verify it had been cleaned of bad code, the warning page stayed up."). Google's cooperation with the Harvard Berkman Center for Internet Research to run the Stop Badware program could prefigure future intermediary cooperation with NGOs to provide "rough justice" to those disadvantaged by certain intermediary practices.

[26] In the meantime, Google has been developing a tool that would help consumers detect if their Internet service provider was "running afoul of Net neutrality principles." Stephanie Condon, *Google-Backed Tool Detects Net Filtering, Blocking*, CNET NEWS, Jan. 28, 2009, http://news.cnet.com/8301-13578_3-10152117-38.html ("[The tool, M-Lab,] is running three diagnostic tools for consumers: one to determine whether BitTorrent is being blocked or throttled, one to diagnose problems that affect last-mile broadband networks, and one to diagnose problems limiting speeds."). It remains to be seen whether Google itself would submit to a similar inspection to determine whether it was engaging in stealth marketing or other problematic practices.