CHRISTOPHER K. RIDDER
744 Mountain Blvd. • Oakland, California 94611
(510) 547-4631 • chris@cridder.com

November 30, 1999

Secretary, Federal Trade Commission
Room H-159, 600 Pennsylvania Avenue N.W.
Washington, D.C. 20580
profile@ftc.gov

Re: Online Profiling Project - Comment, P994809 / Docket No. 990811219-9219-01

Dear Mr. Secretary:

I am submitting this reply comment in response to the DoC's and FTC's Federal Register Notice Requesting Public Comment and Announcing a November 8, 1999 Public Workshop on Online Profiling, and in response to NTIA's solicitation of reply comments by November 30, 1999. Although I was unable to attend the workshop, I thank the Commission for the opportunity to nevertheless present some thoughts on the issue. I am writing this comment solely as an interested citizen, and not on behalf of any other person or organization. I will also be submitting these comments as coursework for my Cyberlaw class at the University of California at Berkeley School of Law (Boalt Hall).

My submission focuses on the Notice/Awareness prong of the fair information practices identified by the FTC, as it applies to privacy policies currently in use by large corporations engaged in online profiling. The paper highlights some of the notice issues that I believe are most pressing on the web today, and provides some examples. I conclude that, despite some industry progress and promising new technologies enabling consumers to control their privacy online, such efforts will not be sufficient to protect consumer privacy in an uncertain 21st century.

I welcome comments from anyone on my submission, and look forward to further developments in this area.

Respectfully submitted,

Chris Ridder

cc: Martha K. Landesberg
Division of Financial Practices, FTC
(202) 326-2825, mlandesberg@ftc.gov

Wendy S. Lader,
NTIA, U. S. Department of Commerce
(202) 482-1880, wlader@ntia.doc.gov

Reply Comments to the November 8, 1999 Workshop on Online Profiling

Online Profiling Project - Comment, P994809 / Docket No. 990811219-9219-01

Submitted by: Christopher K. Ridder[1]

I would like to thank the Commission for the opportunity to submit these comments. As a law student with an abiding interest in cyberlaw, and as someone who has been using the Internet since 1989, I've been following developments in online profiling for some time. Like many who have already commented, I see both the promise and the specter inherent in the Internet's ability to enable two-way communication. And like most American consumers who know something of the surveillance capability that is just beginning to be realized by private actors in our society, I am concerned.

I've been following the Commission's work in this area with great interest, as well as industry's efforts to institute effective self-regulation measures. These efforts have recently yielded a profusion of privacy policies.[2] They have led to the creation of seal programs.[3] Some Internet architectural measures designed to assist consumers in protecting their privacy are in place or coming soon.[4] Yet despite these advances, we still have a long way to go in terms of achieving consistent use of fair information practices in consumer profiling.

My comments here will center on online privacy policies, the recent profusion of which seems to have provided a substantial part of the FTC's justification in its 1999 Report for recommending

---

[1] For more information about the author, *see* <http://www.cridder.com>.

[2] *See, e.g.,* Mary J. Culnan, Ph.D., *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Comm'n,* app. A at 5 (June 1999) <http://www.msb.edu/faculty/culnanm/gippshome.html> (hereinafter "GIPPS") (Reporting that 44% of web sites surveyed had a privacy policy). *Compare* Federal Trade Comm'n, *Privacy Online: A Report to Congress* (1998), at 41 (hereinafter "1998 Report") <http://www.ftc.gov/reports/privacy3/index.htm> (reporting that 14% of web sites surveyed had privacy policies). *But see* Ram Avrahami / The NAMED, *Comments on the Georgetown Internet Privacy Policy Survey* <http://www.msb.edu/faculty/culnanm/GIPPS/named.PDF> (suggesting that comparisons between the two are dubious).

[3] *See, e.g.*, Truste <http://www.truste.org/>; BBBonline<http://bbbonline.org/>; CPA WebTrust <http://www.cpawebtrust.org>.

[4] *See, e.g.,* P3P <http://www.w3.org/P3P/>; The Anonymizer <http://www.anonymizer.com>; Zero Knowledge Systems <http://www.zeroknowledge.com>.

that legislation protecting privacy not be enacted at this time.[5] In my opinion, a larger number of policies should not be the standard by which we gauge the effectiveness of industry self-regulation. Rather, we should look to the substantive nature of those policies. It is here that we find the strongest support for a suggestion that you have heard frequently from industry critics – that despite an increasing number of policies, self-regulation has failed to provide even the most basic assurances that consumers' personal data will be safe in the 21st century.

Substantively, many privacy policies are toothless.[6] Many are designed with the bare minimum of disclosures. Frequently, they are silent on which type of information is collected, as opposed to used. Nearly all say that they are subject to change – the only notice of this change being modification of the web site, and a suggestion that browsers check back periodically. And perhaps most serious – privacy disclosures are generally limited to the online activities of a company. They fail to disclose to what extent the company collects information outside of the web context, and they fail to disclose whether offline information is correlated with data gleaned from the Internet.

Sadly, though perhaps not surprisingly so, many privacy policies ride a fine line between vacuous and misleading. Both the FTC and some of the watchdog organizations that have commented here have acted in the case of seriously misleading policies, especially where children's data has been involved.[7] Unfortunately, I don't believe that industry has an incentive to remedy the vacuousness problem until fair information practices are defined more strictly, and until a baseline of privacy protection is implemented through federal legislation.

---

[5] *See* Federal Trade Comm'n, *Self-regulation and Privacy Online: A Report to Congress* (July 1999), at 6 (hereinafter "1999 Report") <http://www.ftc.gov/os/1999/9907/privacy99.pdf >.

[6] Moreover, there is little incentive for industry to self-regulate to the level that will provide consumers with meaningful protection. *See, e.g.*, *Testimony of Deirdre Mulligan Staff Counsel Center for Democracy and Technology before the House Committee on Commerce Subcommittee Telecommunications, Trade, and Consumer Protection* (July 13, 1999) (describing inherent problems with industry self-regulation, and recommending legislation enabling the FTC to make baseline privacy regulations, designed to work in tandem with industry self-regulation efforts and end-user privacy-enhancing technologies) <http://www.cdt.org/testimony/mulligan071399.shtml>. *See also*, Roger Clarke, *Internet Privacy Concerns Confirm the Case for Intervention*, COMMUNICATIONS OF THE ACM 42, 2 at 60-67 (February 1999) <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html >.

As many other commentors here have outlined, the ability to compile detailed dossiers on American consumers has reached an unprecedented level, and these capabilities are further increasing at an alarming rate. Today, as more sites implement "cookie synchronization" agreements,[8] and as companies begin to merge large online and offline databases of customer information, both the breadth and depth of electronic dossiers on American citizens is expanding rapidly. These are capabilities that many consumers are probably not aware of. Nevertheless, numerous surveys document that consumers increasingly believe that data privacy is a serious problem.[9]

Quality vs. quantity

> …9.5% of the 337 Web sites that collect at least one type of personal information[] contained *at least one* survey item for all five elements of fair information practices: notice, choice, access, security and contact information.[10] (emphasis added).

If fewer than 10% of these web sites contain as few as one of each survey item, how many sites are likely to contain privacy policies that truly are in line with fair information practices?[11] So far, few web sites have met the substance of the self-regulation challenge. In this comment, I will highlight a few problems that I believe are pervasive, and intractable absent further regulation,[12] in the area of Notice/Awareness.

---

[7] *See, e.g., In re* GeoCities, Docket No. C-3849 (Feb. 12, 1999) (Final Decision and Order available at <http://www.ftc.gov/os/1999/9902/9823015d&o.htm >); *In re* Liberty Financial, Case No. 9823522 (May 1999) (proposed consent agreement available at <http://www.ftc.gov/os/1999/9905/lbtyord.htm >).

[8] *See Comments of Jason Catlett, Junkbusters*, submitted in advance of the November 8, 1999 Online Profiling Workshop, Docket No. 990811219 -9219-01 ("Although cookies were intended to be site-specific, networks are using a technique sometimes called cookie synchronization to be able to effectively "share" cookies and the information associated with them on the server side across multiple sites.").

[9] *See, e.g.,* Lorrie Faith Cranor, et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* at 5 (1999) (hereinafter "AT&T Study") <http://www.research.att.com/projects/privacystudy> (reporting that 87% of surveyed experienced U.S. Internet users stated that they were somewhat or very concerned about threats to their privacy online). *See also* Louis Harris & Assoc., Inc., Nat'l Consumers League: *Consumers and the 21st Century* at 4 (1999) (reporting that 70% of U.S. respondents were uncomfortable providing personal information to businesses online).

[10] GIPPS at 6.

[11] *See* 1998 Report at 7-11 (identifying the core principles of privacy protection common to the government reports, guidelines, and model codes that have emerged since 1973: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.). *See also*, 1999 Report, n. 17 (listing the sources used to derive the core principles).

[12] This obviously assumes that industry-funded privacy seal programs will not provide the enforcement mechanisms required to establish industry self-regulation. Although beyond the scope of this comment, the Commission is aware of the high-profile failures of Truste to admonish RealNetworks, Microsoft and others, with anything other than the

Notice/Awareness

Collection, as opposed to use, of information

Companies should be required to disclose what information is *collected*. Companies and databases change over time. When companies merge, so do their databases. Moreover, companies with multiple, yet currently separate, databases could elect to merge and/or sell them at some future point. Although it is probably impossible to predict how these companies' databases would be handled in the future, customers would at least have as much information as anyone if they knew what information was being stored about them.

Data is persistent. Data migrates through many systems as it is bought and sold, and as companies merge. Americans have a right to know what data is being stored about them, so they can be aware of the potential risk of its disclosure in an unpredictable future. Moreover, although companies may not use all of the information they collect today, it is certainly discoverable through a subpoena or court order. Americans should be able to identify which information resulting from private surveillance activities might be used against them at a later date.

Many privacy policies leave the company an "out", failing to make representations sufficient to bind the company to the practices it implies. Absent regulation, companies will have no incentive to bind themselves, because they want the freedom to change their practices. Yet strong, believable representations are critical to consumer confidence in the trustworthiness of privacy policies. For example, barnesandnoble.com's privacy policy with regard to its Author Chat service says they collect your **"…**name and where you're from (for example, 'Joe from Chicago') and your question, but no other information is formally stored in the archive of the chat."[13] Such a statement doesn't

---

proverbial slap on the wrist. Moreover, seal programs do not necessarily comport with the fair information practice principles.

[13] <http://www.barnesandnoble.com/help/nc_privacy_policy.asp?userid=*OMITTED*&srefer=> (Note that one can't even view this privacy policy from the home page without first providing the web site with a unique user ID).

foreclose the possibility that "other" information is stored informally, or that it could be stored somewhere other than the chat archive.

Deletion of information is especially a problem with regard to opting out of a service after one has already registered. Many sites give users the option of discontinuing the further use of personal information. However, most make no representation that data already provided to them will be deleted. Moreover, any data previously provided to third parties must be handled in separate transactions – if consumers can even find those third parties, and if they permit deletion of previously stored information.

For example, AltaVista advertises, "If you do not wish demographic or profile information to be shared, then you may opt-out [sic] at the time of registration."[14] Such a statement lacks clarity about whether there's an option to opt out subsequent to registration. More important, the statement says nothing about whether information will be deleted – only that it will no longer be shared.

Aggregation of databases

As databases are aggregated, and as data mining technology improves, the quality of profiles increases dramatically. Outright sale of information, while possible, is far from necessary for such consolidation to occur. Some companies may choose to merge their own database information. For example, if Safeway were to create a successful online grocery store, it would be extremely beneficial to merge its online clickstream data with its in-store club card information. Yet far more ominous developments are already occurring, such as the recent approval of the DoubleClick/Abacus merger.[15]

[14] AltaVista privacy policy, <http://doc.altavista.com/legal/privacy.shtml>.

[15] *See, e.g., Comments of Andrew Shen, Electronic Privacy Information Center (EPIC)*, submitted in advance of the November 8, 1999 Online Profiling Workshop, Docket No. 990811219-9219-01 ("Abacus Direct is an offline company that collects information about consumers' purchasing habits through a database that tracks catalog subscriptions and purchases. Through this database, Abacus knows your credit card numbers, personal address, telephone number and information about your household income, family makeup and other habits. The merger of these companies puts a lot of information, including both personal and demographic data, in the hands of advertisers. In just one month -- December of

Many Americans would be shocked to learn that in the future, if not today, detailed psychographic profiles could be readily available. [16] As these databases become ever more detailed, one could imagine them frequently becoming targets of subpoenas, law enforcement investigations or hackers. Insurance companies, employers and others could use online profiles to discriminate. If consumers knew the potential consequences, would they still consent to intrusive monitoring?

Perhaps this explains why DoubleClick, in its pre-merger privacy policy, said merely that it was intending to merge with Abacus, that it had no plans to integrate the companies' databases, but that if it did, it would include an updated privacy statement. Such an updated statement was posted upon approval of the merger. Few people who know a lot about the industry would be surprised at what the representations are today:

> All advertising messages delivered to online consumers identified by Abacus Online will be delivered by DoubleClick's patented DART technology… [The] Abacus Online database includes the user's name, address, retail, catalog and online purchase history, and demographic data. The database also includes the user's non-personally-identifiable information collected by Web sites and other businesses with which DoubleClick does business. [17]

The site further notes that this information is collected in a single location, although it is unclear with whom it may be shared.

Also of note is that privacy policies generally apply only to online activities. Offline profiling efforts, which may be correlated with databases containing online information, are generally not included. For example, Safeway makes no disclosures concerning the extent to which its "club card" data is collected or used. [18] General Electric recently made the news when it embedded a secret tracking code in an offline survey, designed to match respondents with real investors.[19] GE's policy has not changed since that story broke. It still provides, "At times we conduct on-line surveys to

---

1998 -- 45.8% of all online users in the United States, reaching 48 million people, received a cookie from DoubleClick. Abacus possesses more than 88 million five-year buying profiles.")

[16] *See generally*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193.

[17] *Id.*

[18] *See* <http://www.safeway.com/> (Users must click on "privacy policy" from the home page).

better understand the needs and profile of our visitors. When we conduct a survey, we will try to let you know how we will use the information at the time we collect information from you on the Internet."[20] Companies that collect personal information offline should disclose the full scope of such collection in their Internet privacy policies, especially where correlation may occur.

Web bugs, cookies and other "obscure" profiling technologies

Consumers are probably unaware of the full range of profiling capabilities that exist, and are currently in use, on the web. Future developments in this area may be difficult to anticipate, but are certainly coming soon. Few sites disclose the implications of cookies, and many completely omit statements concerning their use. Few sites disclose URL tracking, whereby URLs are embedded with personal information, such as referral chains and user IDs.

Leading edge marketers are presumably not eager to disclose such capabilities. The FTC only learned about "web bugs"[21] on November 8, 1999[22] – a technique that has probably been in use for some time. If sophisticated people who have been monitoring this situation for years don't know about such technologies, how much should consumers be expected to know? I know of no privacy policy that currently mentions web bugs, or their practical applications.

FedEx, for example, is reported to have web bugs on its site which provide information to DoubleClick.[23] Yet the only relevant representation in its privacy policy appears to be, "None of the information collected by FedEx is shared with other organizations for commercial purposes."[24]

---

[19] *See* Ted Leventhal, *GE Survey Secretly 'Brought Good Names To Light'*, PRIVACY TIMES, June 4, 1999 <http://privacytimes.com/ge.htm>.
[20] <http://ge.com/privacy.htm>.
[21] *See* Richard M. Smith, *The Web Bug FAQ* (November, 1999) <http://www.tiac.net/users/smiths/privacy/wbfaq.htm> (describing web bugs as generally invisible graphics on a web page or email message designed to monitor the IP address, preset cookie values and other information about the viewer).
[22] *See* Robert O'Harrow Jr, *Fearing A Plague Of "Web Bugs"*, THE WASHINGTON POST, November 15, 1999.
[23] *See The Web Bug FAQ*, *supra* n. 21.
[24] <http://www.fedex.com/us/about/privacypolicy.html >.

Transfer of information to third parties

Consumers generally don't want information transmitted to third parties.[25] Many privacy policies state that they won't transfer to third parties, other than "affiliates." It's unclear whether there's a consistent definition of an affiliate, although traditionally this applies to wholly-owned subsidiaries. These can change over time, however, and the final disposition of consumer profiles is not predictable. Moreover, even a web site that declares in its privacy policy that it won't share data with third parties – doesn't always declare that third parties have placed monitoring technology, such as banner ads that set cookies on the site.

AltaVista and barnesandnoble.com provide a useful illustration of the inconsistency typical of disclosures regarding the cookies set by banner advertisers. AltaVista's privacy policy states the following:

> "AltaVista uses an outside company to serve advertising on our site. The outside advertising company uses cookies to ensure that you do not see the same advertisements too often. Cookies that are received with advertisements are read and placed by our advertising company and AltaVista does not have access to them. "[26]

The company certainly plays fast and loose with the reasons banner advertisers use cookies. Is it to give me more exciting ads, or to compile detailed marketing information? I suppose the answer is in the eye of the beholder. I also have serious reservations about the statement that AltaVista does not have access to the cookies. Although they may not have direct access, they may w ell have an agreement to share the information in the cookie. If this is true, it is functionally the same as if they had access, from a privacy perspective. For comparison, here's the barnesandnoble.com disclosure:

> "barnesandnoble.com wants you to be awar e that when you click on links and/or ad banners that take you to third-party web sites, you will be subject to the third parties' privacy policies."[27]

---

[25] *See* AT&T Study at 2, 10 (noting that this is an area of particular concern for U.S. consumers).
[26] <http://doc.altavista.com/legal/privacy.shtml>
[27] <http://www.barnesandnoble.com/help/nc_privacy_policy.asp?u serid=*OMITTED*&srefer=>

This disclosure fails to even mention cookies. Moreover, it implies that advertisers collect no information about consumers until they click through.

Subject to change without notice

Perhaps the most serious notice issue arises in the virtually standard term used in privacy policies that they are subject to change without notice. Such a statement is usually accompanied by a suggestion that customers should check back periodically to see if the company has decided to use previously collected information in a different way. Such a practice, in failing to provide adequate notice, seriously undermines choice and consent.

Here are three examples: "barnesandnoble.com may update this policy from time to time; please check this page periodically for changes."[28] "Saturn reserves the right to alter our privacy principles as business needs require. Any alterations to these principles will be posted on our web sites in a timely manner."[29] "FedEx reserves the right to amend the privacy policy at any time with or without notice. Please check back frequently in the event of changes." [30]

Information collected under a privacy policy today should remain be governed by the terms of that policy forever, absent explicit consent. In the event of a merger, the most restrictive provisions should apply unless the subject consents. Consumers should be able to rely on the representations made by companies about how their information will be used, at the time of its collection. Asking consumers to check back periodically is not a fair information practice, because it fails to provide adequate notice of potentially serious retroactive changes.

Conclusion

Many of the industry commentors have discussed the holy grail of one to one marketing, and its growing importance to the evolution of ecommerce. If there's one thing everyone agrees on with

[28] *Id.*
[29] <http://www.saturn.com/about/privacy.html>
[30] <http://www.fedex.com/us/about/privacypolicy.html >

regard to this issue, it's that the profiles we're talking about are extremely valuable – both to industry and to consumers who care about their privacy.

However, it's important to keep in mind that there is much more at stake here than merely ensuring that consumers are confident enough in their privacy rights to hand out their credit card numbers online. Privacy is not only an inherent human right, it is a legal right in this country as well[31] – a right that demands an analysis that goes beyond considerations of economic efficiency. Our inquiry should be forward-looking, and take into account the long-term implications of online profiling, not merely the short-term benefits to be gained from "targeted advertising". In 30 years, how will companies use the detailed psychographic profiles they've amassed? How sophisticated will futuristic data mining techniques be, and to what extent will they be able to create new information from old data? How secure will this information be from hackers and identity thieves?

I agree with your non-industry commentors, and over 70% of Americans, that some form of legislation is required to protect privacy.[32] Although the industry appears to be making a concerted effort to self-regulate, such attempts are virtually certain to fall short of satisfying the information practices endorsed by the FTC. Industry self-regulation will always play an important role in the management of online profiles, but even in combination with consumer self-help technologies,[33] it is woefully insufficient. I urge you to recommend legislation that would codify the fair information practices the Commission has outlined, so that every American can be assured of at least a certain baseline of protection.

---

[31] *See generally*, Jonathan P. Cody, *Protecting Privacy Over The Internet: Has The Time Come To Abandon Self-Regulation?* 48 CATH. U. L. REV. 1183 (1999) (exploring the development of a privacy right in the United States, examining the success of self-regulatory efforts, and recommending formal adoption of fair information practices.).

[32] *See* Georgia Institute of Technology, *10th GVU WWW User Survey* (December, 1998) <http://www.gvu.gatech.edu/user_surveys/survey-1998-10/> (reporting that most respondents agreed strongly (40.6%) or somewhat (30.8%) that there should be new laws to protect privacy on the Internet).

[33] A full discussion of the technical self-help measures is beyond the scope of this comment. For a viewpoint critical of P3P, *see* Jason Catlett, *Open Letter to P3P Developers*, September 13, 1999 <http://www.junkbusters.com/standards.html>.