

Ten Questions Concerning Consumer Privacy Online

(and the answers Web marketers don't want you to hear....)

On November 1, 2006 the Center for Digital Democracy (CDD) and the U.S. Public Interest Research Group (U.S. PIRG), two leading public-interest advocacy groups working on behalf of a more diverse and competitive online environment, filed a complaint (FTC filing available at: <http://www.democraticmedia.org/PDFs/FTCadprivacy.pdf>) with the Federal Trade Commission, calling for an immediate, formal investigation of online advertising practices and their impact on consumer privacy. The response to our complaint was both encouraging (numerous articles in the media, and an endorsement from U.S. Representative Ed Markey (D-MA)) and predictable (industry representatives disavowed any wrongdoing).

The digital media system is rapidly evolving to collect and utilize ever greater more precise personalized information. Offline databases and sources are also used to add to such online profiles. As more Americans use "triple play" services for their communications needs, our very personal mobile phone/device and interactive cable/telephone TV data will be melded into what is captured on PC's.

To clarify the issues at stake in our complaint, we've prepared the following overview of our call for new consumer and privacy protections online:

1. Why did CDD/U.S. PIRG file this complaint?

We are concerned that policies governing consumer privacy on the Internet have failed to keep pace with developments that continue to re-shape the online world. In our complaint we focus on data-collection, user-tracking, and audience-profiling technologies which operate without a consumer's knowledge or consent. The everyday consumer doesn't tolerate this kind of surveillance in the real world, and they shouldn't be subjected to it in cyberspace, either. Its effect has also been to put enormous amounts of consumer information into the hands of sellers, leaving buyer-consumers at risk of unfair pricing schemes and with fewer choices than the Internet is touted to provide.

2. What did you ask the FTC to do?

We made four basic requests of the FTC:

- ❖ **Investigate** the online marketplace in light of new developments in the field,
- ❖ **Expose** marketing practices that compromise user privacy,
- ❖ **Issue** the necessary injunctions to halt current practices that abuse consumers, and
- ❖ **Create** policies and recommend federal legislation that prevents such abuses in the future.

3. Why did you single out Microsoft? Aren't Google and Yahoo (and others) equally culpable?

The complaint does not grant immunity to any online marketer or website, and we provide countless examples of

questionable practices on the part of dozens of companies, large and small. We fully expect that once the FTC begins its investigation, other companies, including Google and Yahoo, will be accorded similar scrutiny.

Nevertheless, considering the size and scope of Microsoft's empire, and a number of bold claims it has recently made, for example, for its new adCenter service—"MSN reaches nearly two out of three Web customers, and MSN Search reaches over 40 million a month."—we felt that it was appropriate to use the comprehensive public information available about its practices as a detailed example of the issues we raise in the complaint.

4. Won't your solution destroy everyone's business model and make it impossible to do business on the net?

We are well aware of the important role that advertising plays online and, indeed, in our economy generally. Nor is it our intent to make Web marketing illegal. What we opposed, however, and what we believe is the duty of the FTC to prevent, is the predatory targeting of advertising to specific individuals, based on data gleaned from online monitoring, and/or combined with data from other sources, online and off, *without consumer knowledge and consent*.

5. Has the Internet data system changed, and are things getting worse?

The Internet continues to evolve, and no one would deny that it's a faster, more convenient, and more interesting place today than it was ten years ago. Our concern is simply that the Web's default state is now "Privacy/Off--Surveillance/On." When we log on to the Internet, no one asks us whether we're willing to share a record of our travels and transactions. Instead, such data are routinely recorded, compiled, and analyzed (unless, of course, we

manage to find and read through a typically long, arcane privacy policy that *may* offer us a chance to "opt out" of this system of digital dossiers). The standard, we believe, should be "opt in," meaning that information can be collected online *only* if we give our explicit consent, and only if we are fully informed of how that information will be used (and whether it will be shared with others).

6. If they're simply trying to make their ads more precise, what is wrong with that?

Precision is one thing, invasion of privacy quite another. We've come to expect, for example, an online bookseller to pitch *For Whom the Bell Tolls* after we inquire about *The Old Man and the Sea*. But when *all* of our searches and mouse-clicks are collected and analyzed, and when such information is exchanged among various websites and compiled in vast databases, we believe we should have the right to say "no thanks." And we should have that right *before* any surveillance takes place.

7. But most online marketers are careful to collect only non-personally-identifiable information. What's the harm of that?

While your actual *social security number* may not be attached to the extensive online dossiers that are compiled and analyzed, unique *identification numbers* are assigned to each visitor, and those numbers serve the same purpose: marketers know exactly who you are, where you've gone, and what you've done online. By segmenting visitors into targeted groups, marketers are also corralling your next online movement--by controlling and limiting what's headed your way, in the form of packaged, personalized content. Plus, this information imbalance benefits sellers at the expense of buyer-consumers.

8. Don't privacy policies solve these problems?

Aside from the Children's Online Privacy Protection Act (which applies only to Internet users 13 and under) and the general strictures concerning "unfairness and deception" in Section 5 of the FTC Act, online travelers are left to their own devices when it comes to guarding their privacy. Typical of such "devices," unfortunately, is Microsoft's 3,400-word privacy statement, a complex, convoluted document that (in combination with a "Supplemental Privacy Information" that includes *ten separate privacy statements*) few consumers can be expected to read, much less understand. It is clear, in short, that we need *national* safeguards to protect consumers from invasive and

predatory advertising practices online, rather than the conflicted attempts at industry self-regulation that invariably promises more than is delivered.

9. What are some actual examples of practices that the FTC should investigate and where can consumers learn more about them?

Our 50-page FTC filing is full of detailed examples. Listed here are five excerpts from the online companies' own documentation, typical of the surveillance practices that have become all-too-common on the Web today.

DeepMetrix (www.deepmetrix.com), which Microsoft acquired in May 2006, offers a sophisticated data-mining package: "With LiveSTATS.BIZ... you can analyze the click streams for first-time visitors, loyal customers... visitors from a specific country like the USA or Poland, and so on...See IP addresses and time stamped action sequences for each visit... Zoom in on specific visitors and unusual visits that require your detailed attention."

Unica (www.unica.com) tells its clients that "... you will want to learn as much as possible about individual visitors, including their names, companies, email addresses, telephone numbers, and geographic location so you can leverage this information..."

Atlas Solutions (www.atlassolutions.com) has developed "... technology to capture actual user behavior... which fields users interact with, how far down a page they scroll, or how engaged are they with the web page."

BlueLithium (www.bluelithium.com) offers AdPath technology, which allows advertisers to "follow prospects across the 1,000+ site of the BlueLithium network..."

Coremetrics (www.coremetrics.com) explains that their Lifetime Individual Visitor Experience Profiles, or LIVE Profiles represent, "...a complete record of all individual visitor interactions with client web sites."

10. What happens next? And what can Internet consumers do to join the fight for online privacy?

The complaint submitted by the CDD and U.S. PIRG is only the first step in a full scale campaign to press for meaningful consumer privacy protections online. Visit our websites to learn more about the current problems and solutions to privacy and consumer dangers in the online marketplace.

The Center for Digital Democracy (www.democraticmedia.org) is a Washington-based nonprofit organization dedicated to maintaining the diversity and openness of the media, focusing especially on the new broadband communications systems.

U.S. Public Interest Research Group (www.uspirg.org) serves as the federation of state PIRGs, which are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of the American public.