Comments Submitted in the FTC/NTIA Workshop on Online Profiling

By Solveig Singleton

These comments will address the following questions:

> **I.** What are the costs and benefits, to both industry and consumers, of online profiling?
>
> **II.** Are consumers' privacy interests implicated by the collection, compilation, sale and use of information collected by online profiling companies?
>
> **III.** What self-regulatory efforts have online profiling companies undertaken to address concerns raised by their collection, compilation, sale, and use of consumer information? How do these efforts address the fair information practice of notice, choice, access, security, and enforcement? What are the costs and benefits, to both consumers and businesses, of such self-regulatory efforts.

I. What are the costs and benefits, to both industry and consumers, of online profiling?

Benefits. Let's begin with an analogy. Suppose you are a shopkeeper in a mall where the lights are on--but your eyes are covered by a blindfold. Your ears are blocked so you can't casually respond to comments customers make about your display. You don't know whether any given customer looks like a shady character--maybe a shoplifter. You can't even guess whether he's a local or a tourist--a one-time visitor or a regulator, businessman or housewife, German or Spanish, old or young, where he goes in the store and how long he stays there. This is what electronic commerce would be like without online profiling.

Online, we're all strangers dealing with ever more distant strangers. In this world, profiling is a natural substitute for the incredible array of information we get through gossip, face-to-face encounters, and traditional not-very-detailed compilations of public records.

Traditionally, the benefits to consumers from profiling begin with **lower prices for goods and services.** In the offline world of direct marketing, a company can use profiling and targeted marketing to bring its cost-per-order from as high as ten dollars to as low as two dollars. The cost-per-order is the amount that a company must spend on outreach in order to obtain one new customer. These cost savings are reflected in the prices that consumers pay.

Does this apply in the online world, where targeted email business is a brand new business model, and the cost of sending out an additional email is near zero (unlike a piece of mail)? Yes. Many electronic merchants wait for the customer to come to them--but profiling will still make a difference in the prices that consumers pay. First, a direct effect: Profiling increases the effectiveness of banner advertising, making companies willing to pay more to web sites that run their ads. This helps fund the site's costs of operation. And the companies online advertising need not imitate the wasteful "broadcast" model of trying to reach 100 percent of consumers to reach the four percent who would be interested in one's product.

But the indirect effects of profiling in enhancing competition are probably more important. That is, **profiling will allow consumers to buy goods and services that would otherwise not be offered--and from companies that would otherwise not exist; this competition-enhancing effect is multiplied when detailed online profiles are combined with offline profiles.**

First, suppose you are developing an e-commerce product. Prodigy, one of the first to offer online grocery shopping service (unsuccessfully) learned the hard way that consumer surveys are a poor guide to what people actually want. As Chet Thompson of Prodigy once noted, "Market surveys told Prodigy that people wanted to do their grocery shopping by computer. They didn't." The key to minimizing the risk of new products or services before starting a large-scale test is to get some clue as to whether there is a meaningful demand for the service will be--and that means having access to information about actual behavior, not self-reported behavior.

Profiling companies can use profiles to get ideas for new products and services and to assess the potential demand for these services. Are there enough women between 5'7" and 5'10" to make a market for "medium-tall" clothing? How much do they spend? No one knows for sure, but profiling might get a company close enough to a likely answer to attract investment or find its first customers.

Second, **the use of profiles in marketing makes it easier for small companies to break into markets dominated by big competitors.** Consider the example of a new commercial web site, with no customers yet and no big name. A consumer using a search engine might find the new company…or not. This company is at a disadvantage compared to its established competitors with household names. Online profiling will enable the development of highly targeted email, allowing companies to garner new customers without the problems and stigma of "spam." Consumers will no longer have to rely solely on less-than-perfect search engines to learn about a product that interests them. And new companies with a low profile will have an alternative to these engines as well.

In the offline world, matching precise online data with a consumer's real identity could mean even bigger gains for new operations. It is more costly to advertise a store in newspapers, on the radio, or by using direct mail than to make one's reputation than on the Web. Imagine that you've opened a store that sells baby clothes. Your established competitors are Hecht's, Macy's, and so on. Being able to buy a list of local people who have recently had babies--or who have surfed for baby clothes online--might mean the difference between the success or failure of your business. Trying to use a data-poor list that does not enable precise targeting could mean the end of the venture.

Even for established companies, a cost-per-order of nine dollars might be too much; lowering the cost to two or three dollars could pull a company back from the edge of bankruptcy (as it did with the Triple-Edge Windshield Wiper company).

The debate about privacy has moved forward with very little information about how information is actually used in the economy and how much this benefits consumers. I know of no sophisticated economic studies that quantify the precise impact of profiling--or regulation--on consumer welfare, prices and competition. Until those studies are done, the benefits of profiling within the economy must remain abstract and anecdotal--not nearly as exciting as horror stories, and harder to grasp.

But the case for the benefits of profiling is strengthened by empirical research done on analogous activities. First, the benefits and costs of profiling in credit reporting are well documented. Sophisticated economic models are used to estimate the changes in business operating costs that would result from a proposed legal change--and to identify the size of the group of consumers who the industry would no longer be able to serve if the change were made. Second, as Jack Calfee writes in his book *Fear of Persuasion*, economists have also learned how mass advertising benefits consumers by substantially heightening price and quality competition.

The results of studies of credit reporting give us reason to presume that broader uses of profiling in the economy could be very beneficial. The advertising studies suggest that more targeted advertising would heighten competition even more.

Summing up the benefits to consumers and business from profiling, these would include:

- Improved product development--a greater chance of success for new ventures and new products.

- An end to wasteful junk mail sent to masses of unlikely prospects.

- Lower costs and lower prices, particularly when online profiles are combined with offline data.

- A chance for small, low-profile ventures to move forward by buying access to strategic information.

- Improved banner advertising economics--and a healthier web economy.

Costs. This section analyzes the costs to consumers from profiling; there are certainly costs to businesses, as well--the cost of building a secure storage infrastructure, the costs of buying access to a list, for example. This type of cost--or the opportunity cost that a business bears when choosing to develop data infrastructure or to invest in broadcast advertising--are not problematic from a public policy standpoint. The company is investing its own money, presumably on the theory that its investment in profiling will be beneficial in the long run.

What about the costs to consumers? Some of these costs are real. Ironically, the costs most frequently asserted in the debate over privacy are largely imaginary.

One real aspect of cost is the risk of identity theft--which is already illegal. A second real risk is that of information falling into the hands of stalkers and child molesters. These are risks that are also (in practice, more so than profiling) associated with newspaper articles, telephone books, individual credit card accounts, real estate records, chat rooms, school buildings, waste-paper baskets, and so on. With respect to profiling, the best answer to these risks is improved security for databases--the use of biometric data to restrict access to accounts, for example. Generally, the more a merchant knows about its customer, the harder it will be for an interloper to mimic all the proper responses--name and social security name can be recited easily, but a photographic likeness is harder to fool.

Note that profiling helps catch bad guys, too. For example, credit card reporting lowers the costs of fraud to business and consumers by identifying people with a history of not paying their bills. Profiling services could also help people ensure that their baby sitter is not a child molester.

For the most part, however, these practical questions have taken a back seat to costs in the form of amorphous "threats to privacy." Privacy is quite a different issue than security--the best answer to security concerns might be to use biometrics, not to gather less or no information. "Threats to privacy" are costs that exist largely in people's minds in the form of vague unease felt for a few seconds when making one's first purchase online, revived by journalistic hype about "Big Brother" and the prodding of survey takers. Is this state of the jitters a real "cost" to be redressed by government

action, or technophobia that will ease with experience and experiments with new business practices? An online survey by Jovan Philyaw of DigitalConvergence.com found that consumers tend to worry less about privacy the longer they had spent online.

But, more importantly, businesses are within their rights in collecting and trading information about real events and real people. It would be wrong to intervene simply because this makes some people nervous. We don't grant folks a general right to be protected from everything that makes them vaguely uneasy.

II. Are consumers' privacy interests implicated by the collection, compilation, sale and use of information collected by online profiling companies?

No. This is a controversial answer, so I will explain. First, I distinguish privacy concerns from security concerns. The best solutions to security problems is the sharing of more information, better verification procedures, the use of photos or even biometric data to control access to databases, and so on. Privacy, on the other hand, is generally understood to disfavor the collection or storage of information at all without the litany of notice, consent, access, etc. The alleged right of consumer access to databases, indeed, adds to security problems**. Security and privacy will frequently find themselves at loggerheads.** Whatever regulatory or business issues are raised by the need for greater security, they should be disentangled from the debate about privacy.

Second, "interests" above must mean legitimate interests--interests that should be recognized and perhaps sanctioned in some official way. Someone who does not pay his debts probably has an interest in avoiding detection, but this is not an interest to which most of us would be sympathetic.

We then face the question of the legitimacy of consumer's claimed interests in privacy, the claimed right of notice, consent, access, and so on. **The claimed privacy interests are deeply problematic, because they conflict at a very fundamental level with the free flow of information.**

When a consumer ventures out onto the street or online to interact with other people, he can generally assume (as when moving into a new neighborhood) that anyone he encounters is likely to learn something about him from his behavior, or comment on it to other people. If he participates in a transaction online or offline, there are two entities involved in the transaction--himself, and the representatives of the company.

We would not grant the company the right to prohibit the customer from talking about the transaction with his friends or other businesses. There is no reason that the

consumer should expect to control facts or opinions that the company learns from the transaction. **The claim that an individual in a sense "owns" data about himself turns the default rule in favor of the free flow of information on its head.** It is like giving him the right to copyright information about himself. But it is far broader than any copyright. Copyright has never extended to **facts or to ideas**.

American citizen's privacy interests, with a few very narrow common law exceptions, generally have closely followed their property rights. You are protected under the Constitution from illegal searches and seizures, and from other intrusive laws. But the constitution does not apply to the private sector. No one may legally break into your house and steal your private letters--or hack your web site and extract your credit card data.

But **businesses ought to be free to collect and trade facts and analysis concerning about transactions in which they engage with other businesses--**without asking anyone's consent or otherwise giving them veto power over the transaction. Sometimes, they will decide not to do this, in order to develop customer trust and loyalty. But this is a sophisticated matter of business ethics, not something we may demand of them as a matter of law.

We might want to change the default rule that gives people the general right to make observations about other human beings**… but if we are going to do so--it had better be for a really, really good reason.** Not in response to spectral fears that have not, apparently, done much to keep folks offline line.

III. What self-regulatory efforts have online profiling companies undertaken to address concerns raised by their collection, complation, sale, and use of consumer information? How do these efforts address the fair information practice of notice, choice, access, security, and enforcement? **What are the costs and benefits, to both consumers and businesses, of such self-regulatory efforts?**

This section will focus on the last question alone, leaving it to others to describe in detail existing opt-out and other mechanisms. The answer is that self-regulation, like traditional command and control regulation, can have some substantial and familiar regulatory costs, include the perennial risk of lagging behind technology. Under these circumstances, self-regulation will have many of the same harmful effects as regulation for consumers and business alike:

- The goals that the self-regulation is supposed to achieve are set from above, rather than evolving from the bottom up.

- Businesses are not free to opt out of the system of self-regulation to experiment with new business models or technologies--or simply because they don't see a need for it in their market niche.

But, by contrast, self-regulation built from the bottom up, however, can be relied on to enhance consumer choice when there is a real demand for the reassurance it provides--proved by consumer actions online, not by surveys. A prime example is kosher food labels. Not every company offers a kosher rating, but for those consumers who seek the ratings out, there's an extraordinary range to choose from.

In the data collection area, one characteristic of demands made on e-commerce merchants respecting privacy "self-regulation" has been that the goals of the regulation are assumed to be *known*. Regulators have insisted that a system of self-regulation must ensure that customers have notice of how their data is being used, that they have a choice about whether it is not be collected or not, and so on.

In the real world, however, no one really knows what state of affairs "ought" to obtain with respect to privacy. The question of when human beings will need to reveal information to gain trust, will be willing to offer trust without information, and will need to respect confidentiality to gain trust is a bafflingly complex question.

The goals of systems of self-regulation will evolve and change over time, and will vary widely across the e-commerce marketplace. Entrepreneurs will make informed guesses about privacy policies to allay their customer's fears (if any) of doing business online. Some entrepreneurs will get it wrong, and lose ground; others will get it right, succeed, and be imitated by late-comers. But entrepreneurs must be permitted to take their cues from the results of engaging in the marketplace, not from top-down commands.

What about those who don't participate in self-regulation? Given the vast numbers of start-ups, wild experiments, and small businesses that will be the next generation of pioneers in e-commerce, it would be unlikely that all of them will automatically concede the importance of having a privacy seal on their sites, unless and until they see significant indication of customer demand for it. Perhaps some sites that participate will have some sinister purpose in mind, but most of them will simply be ordinary businesses who simply don't share the vision of a privacy imperative.

It would be a grave mistake to assume that because a business doesn't post a notice of their profiling practices, it ought to become a target of regulation. Lacking a privacy policy simply isn't even close to being evidence that that site poses a danger to consumers, in any real sense. Treating these sites as legitimate enforcement targets would be wrong, and insulting to hundreds of honest entrepreneurs. And enforcement

efforts will be far more effective if they can be targeted against actual perpetrators of identity theft, fraud, and so on. Requiring enforcers to disperse their focus to hundreds of sites simply because those sites don't post some kind of notice would be an incredible waste of time.

Self-Regulation and Consumer Access to Databases

One thing that systems of self-regulation have not generally done is introduce access to databases for consumers. What is the significance of this?

In some cases, errors in databases can amount to defamation by a business that has negligently or deliberately made an error in reporting to a database like a credit report. Thus it makes a certain amount of sense that people ought to have a legal right to ensure that the information in a database like a credit report is accurate.

Even in the fairly clear case of a credit report, however, the case for mandated access is not as straightforward as it appears. The costs to the credit industry--and thus to consumers--of maintaining the access mechanisms are enormous. There is an increased risk that someone improper will use that mechanism to get information they shouldn't have. And, finally, no one wants their database to be inaccurate. So companies in the database business have a strong incentive to get it right. (the two methodologically flawed studies showed rates of error in credit reports as high as 30 percent notwithstanding--Arthur Andersen's properly conducted survey of a truly random sample of consumers showed rates of serious error are probably around 3 percent).

Outside credit reporting, however, erroneous data in databases rarely will amount to a violation of someone's rights. I don't care if I'm accidentally listed somewhere as a hockey fan. The vast majority of transactional data that is collected is trivial and harmless; access mechanisms would simply be an absurdity that would prevent new information services from coming into existence.

It is a fortunate thing for the credit industry that it was invented before the time of the current frenzy about profiling--we might still be living back in the days when poor and middle-class people could get credit only from a friendly storekeeper or a local banker. Inventing such a system from scratch in a world where an expensive consumer access to the database was required from the very early days of the system might have resulted in a world with no credit reporting at all.