



ONLINE PROFILING: A REPORT TO CONGRESS

PART 2 RECOMMENDATIONS

FEDERAL TRADE COMMISSION
JULY 2000

FEDERAL TRADE COMMISSION*

Robert Pitofsky	Chairman
Sheila F. Anthony	Commissioner
Mozelle W. Thompson	Commissioner
Orson Swindle	Commissioner
Thomas B. Leary	Commissioner

BUREAU OF CONSUMER PROTECTION

Division of Financial Practices

* The Commission vote to issue this Report was 4-1, with Commissioner Swindle dissenting, and Commissioner Leary concurring in part and dissenting in part. Separate statements by Commissioners Thompson, Swindle and Leary are attached to this Report.

TABLE OF CONTENTS

I.	Introduction	1
II.	Fair Information Practices and the Network Advertising Initiative Principles	1
A.	Background	1
B.	Profiling	3
C.	Fair Information Practices and Profiling	3
D.	The NAI Principles	4
1.	Notice	4
2.	Choice	6
3.	Access	7
4.	Security	8
5.	Enforcement	8
6.	Additional Consumer Protections	9
III.	Recommendations	9
IV.	Conclusion	11
	APPENDIX A: NAI Principles	

I. INTRODUCTION

On June 13, 2000, the Federal Trade Commission (hereinafter “FTC” or “Commission”) issued *Online Profiling: A Report to Congress*.¹ The report described the nature of online profiling, consumer privacy concerns about these practices, and the Commission’s efforts to address these concerns. The Commission did not make recommendations at that time, because a dialogue with the network advertising industry regarding self-regulatory principles was still ongoing. The Commission promised, however, to supplement its report with specific recommendations to Congress after it had an opportunity to fully consider the industry’s self-regulatory proposals and how they interrelate with the Commission’s previous views and recommendations on online privacy generally. This report presents the Commission’s recommendations.

II. FAIR INFORMATION PRACTICES AND THE NETWORK ADVERTISING INITIATIVE PRINCIPLES

A. Background

As noted in Part 1 of this report, there are a set of core fair information practice principles that have guided the Commission with respect to online privacy issues.² First summarized in the Commission’s 1998 report, *Privacy Online: A Report to Congress* (“1998 Report”),³ these fair information practice principles predate the online medium; indeed, agencies in the United States, Canada, and Europe have recognized them in government reports, guidelines, and model codes since 1973.⁴ The core principles are:

¹ Available at <<http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>>. (“Profiling Report (Part 1)”).

² Profiling Report (Part 1) at 19-20.

³ 1998 Report at 7-14, available at <<http://www.ftc.gov/reports/privacy3/index.htm>>.

⁴ 1998 Report at 7-11. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977); Organization for Economic Cooperation and

(1) **Notice** – data collectors must disclose their information practices before collecting personal information from consumers;⁵

(2) **Choice** – consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;⁶

(3) **Access** – consumers should be able to view and contest the accuracy and completeness of data collected about them;⁷ and

(4) **Security** – data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.⁸

The Commission also identified **Enforcement** – the use of a reliable mechanism to identify and impose sanctions for noncompliance with these fair information practices – as a critical ingredient in any governmental or self-regulatory program to ensure privacy online.⁹

Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995); U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995); *The European Union Directive on the Protection of Personal Data* (1995); and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

⁵ 1998 Report at 7-8; *see also* Federal Trade Commission, *Self-Regulation and Online Privacy: A Report to Congress* (1999) [hereinafter “1999 Report”] at 3-4; *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000) (“2000 Report”) at 4.

⁶ 1998 Report at 8-9; *see also* 1999 Report at 3-4; 2000 Report at 4.

⁷ 1998 Report at 9; *see also* 1999 Report at 3-4; 2000 Report at 4.

⁸ 1998 Report at 10; *see also* 1999 Report at 3-4; 2000 Report at 4.

⁹ 1998 Report at 10-11; *see also* 1999 Report at 3-4; 2000 Report at 4.

B. Profiling

As Part 1 of this report also explained, many of the banner ads displayed on Web pages are not selected and delivered by the Web site visited by a consumer, but by network advertising companies that manage and provide advertising for numerous unrelated Web sites. In general, these network advertising companies do not merely supply banner ads; they also gather data about the consumers who view their ads. Although the information gathered by network advertisers is often anonymous (*i.e.*, the profiles are linked to the identification number of the advertising network's cookie on the consumer's computer rather than the name of a specific person), in some cases, the profiles derived from tracking consumers' activities on the Web are linked or merged with personally identifiable information. This consumer data can also be combined with data on the consumer's offline purchases, or information collected directly from consumers through surveys and registration forms.

The purpose of collecting and analyzing this data is to allow the advertising networks to make a variety of inferences about each consumer's interests and preferences. The result is a detailed profile that attempts to predict the individual consumer's tastes, needs, and purchasing habits and enables the advertising companies' computers to make split-second decisions about how to deliver ads directly targeted to the consumer's specific interests. Nonetheless, network advertising companies are most often invisible to consumers. All that consumers see are the Web sites they visit. Unless the Web sites visited by consumers provide notice of the ad network's presence and data collection, consumers may be totally unaware that their activities online are being monitored.

C. Fair Information Practices and Profiling

Implementing fair information practices in the context of profiling by network advertisers presents numerous challenges. Some of these challenges stem from the invisible, third-party relationship of network advertisers to consumers. Other challenges result from the presence of multiple network advertisers on particular Web sites. Yet more challenges arise from the variations between the practices and business models of the individual network advertising companies and the many different categories of information that can be used for profiling purposes. Despite these

challenges, the Commission believes that it is essential to implement the fair information practice principles in this context.

At the Online Profiling Workshop in November 1999,¹⁰ industry members announced the formation of the Network Advertising Initiative (NAI), an organization comprised of the leading Internet Network Advertisers – 24/7 Media, AdForce, AdKnowledge, Avenue A, Burst! Media, DoubleClick, Engage, and MatchLogic – to develop a framework for self-regulation of the online profiling industry. Following the workshop, the NAI companies submitted working drafts of self-regulatory principles for consideration by FTC and Department of Commerce staff. After lengthy discussions, a set of principles has emerged that the Commission finds reasonably implement the fair information practice principles. A copy of the principles is attached as an appendix to this report.

D. The NAI Principles

1. Notice

The threshold issue in applying fair information practices to online profiling is how to achieve transparency when consumers are largely unaware they are being profiled.¹¹ Consumers cannot make informed decisions about whether to permit the collection of their information unless they know it is being collected and they understand how the information will be used. As noted at the Public Workshop, transparency is an issue concerning both the collection and use of non-personally identifiable information (“non-PII”) and personally identifiable information (“PII”).¹² The greatest

¹⁰ On November 8, 1999, the FTC and the United States Department of Commerce jointly sponsored a Public Workshop on Online Profiling. A transcript of the Workshop is available at <<http://www.ftc.gov/bcp/profiling/index.htm>> and public comments received in connection with the Workshop can be viewed on the Federal Trade Commission’s Web site at <<http://www.ftc.gov/bcp/profiling/comments/index.html>>.

¹¹ The NAI members use the term “online preference marketing” or “OPM” rather than “profiling” because the process involves “collecting data over time and across Web pages to determine or predict consumer characteristics or preferences for use in ad delivery on the Web.” NAI Principles at 2.

¹² See Profiling Report (Part 1) at 12-13.

transparency is achieved by providing disclosure of notice and choice options to consumers on the Web site they are visiting (the so-called “host” or “publisher” Web site) on which the network advertiser is placing cookies or otherwise collecting information. Consumers who may not even be aware of network advertisers are unlikely to visit the network advertiser’s site to obtain notice and choice.

Under the NAI Principles, consumers will receive notice of network advertisers’ profiling activities on host Web sites and their ability to choose not to participate in profiling. Where personally identifiable information is collected for profiling, a heightened level of notice, “robust” notice will be required at the time and place such information is collected and before the personal data is entered.¹³ Where non-personally identifiable information is collected for profiling, clear and conspicuous notice will be in the host Web site’s privacy policy.¹⁴ Under the NAI Principles, NAI companies will contractually require that host Web sites provide these disclosures and will make reasonable efforts to enforce those contractual requirements.¹⁵

¹³ See NAI Principles at 8-10. A sample Robust Notice is attached as a “mock up” to Appendix D of the NAI Principles.

¹⁴ See NAI Principles at 5. An Internet Protocol (“IP”) address, the address that allows a network advertiser to deliver an ad, is treated as non-PII under the NAI Principles. At present, IP addresses are generally considered non-personally identifiable information. Many IP addresses are “dynamic,” changing each time a consumer connects to the Internet, as opposed to “static,” or unique to that consumer’s computer. It is extremely difficult to link dynamic IP addresses to an individual, although using Internet service provider log files, it is technically possible. As technology evolves, however, there may be a trend toward use of static IP addresses, including the increased use of DSL and cable modems. Static IP addresses are more likely to become personally identifiable because they are linked in an individual’s computer. If IP addresses become individual identifiers, an IP address may be considered “data used to identify, contact, or locate an individual,” *i.e.*, personally identifiable information. See NAI Principles at 7.

¹⁵ Personally identifiable information will always be collected pursuant to a contract between an individual NAI company and a host Web site under the Principles. However, NAI companies do not always have a direct contractual relationship with the host sites on which they collect non-personally identifiable information. In the absence of a direct contractual relationship, NAI has no ability to require a host Web site to post a notice about data collection by network advertisers, although it has agreed to make reasonable efforts to ensure that publishers post such notices. See

2. Choice

Once informed about the network advertiser’s information collection practices, consumers should be able to decide whether to participate in profiling. Under the NAI Principles, the choice method depends on the type of information being collected and the consumer’s knowledge about, and level of control over, the original collection of information.¹⁶ They provide that:

- Material changes in the information practices of a network advertising company, cannot be applied to information collected prior to the changes in the absence of affirmative (opt-in) consent of the consumer.¹⁷
- Previously collected non-personally identifiable data (“clickstream”) cannot be linked to personally identifiable information without the affirmative (opt-in) consent of the consumer.¹⁸

NAI Principles at 5.

¹⁶ There are traditionally two models for choice – “opt-in” and “opt-out.” Opt-in regimes require affirmative steps by the consumer to *allow* the collection and/or use of information. Opt-out models require affirmative steps to *prevent* the collection and/or use of information.

The Commission believes that both regimes have a role to play in online privacy. Opt-in procedures may be more appropriate where the information at issue is particularly sensitive – for example, the collection and use of children’s personal information or sensitive medical information. *See, e.g.*, 15 U.S.C. §§ 6501-06 (COPPA). As noted below, hybrids may also have a role, combining elements of both opt-in and opt-out.

The guiding principle for these consent mechanisms is to ensure that consumers are able to make informed choices about their privacy preferences and can exercise those choices in a reasonable manner. As the Commission’s experience with these mechanisms evolves, it will continue to evaluate their effectiveness.

¹⁷ *See* NAI Principles at 6.

¹⁸ *See* NAI Principles at 7-8. However, under the NAI Principles, network advertisers will not merge non-personally identifiable information with personally identifiable information if the non-personally identifiable information was collected pursuant to a privacy policy that stated that such information would *never* be merged with personally identifiable information. *See* NAI Principles at 8.

- “Robust” notice and opt-out choice (appearing at the time and place of information collection and before data is entered) is required for prospective use of personally identifiable information for profiling, including the merger of personally identifiable online and offline data.¹⁹
- Clear and conspicuous notice and opt-out choice (appearing in the publishers’ privacy policy with a link to the network advertiser or an NAI opt-out Web page) is required for prospective use of non-personally identifiable information for profiling.²⁰
- On sites where multiple network advertising companies collect information (generally non-personally identifiable information), consumers will be able to opt-out of profiling by any or all of the network advertisers on a single page accessible from the host Web site’s privacy policy.²¹

3. Access

The third prong of fair information practices, access, is also addressed by the NAI Principles, which promise that consumers will be given reasonable access to personally identifiable information and other information that is associated with personally identifiable information retained by a network advertiser for profiling.²² As the Commission’s 2000 Report stated, “[w]hile Access is widely recognized as an important fair information practice, the Commission believes that Access presents

¹⁹ See NAI Principles at 8-10. Where past expectations about the nature and use of information would be changed (*e.g.* in cases of a material changes in privacy policy or a merger of previously non-identifiable clickstream with personally identifiable information), opt-in choice has been required. By contrast, where only future expectation are implicated (*e.g.*, the prospective merger of PII and non-PII), opt-out choice has been provided.

²⁰ See NAI Principles at 4-6.

²¹ See NAI Principles at 5.

²² See NAI Principles at 8.

unique implementation issues that require consideration before its parameters can be defined.”²³

4. Security

Consistent with the principle of Security, under the NAI proposal, network advertisers will make reasonable efforts to protect the data they collect for profiling purposes from loss, misuse, alteration, destruction, or improper access.²⁴ In the context of security, network advertisers should be subject to the same standards as all businesses that operate on the Internet. Therefore, if, in the future, legislative standards are developed they should apply to network advertisers and other Internet businesses equally.²⁵

5. Enforcement

The bedrock of any effective self-regulatory or legislative scheme is enforcement. In a self-regulatory context, this means that nearly all industry members subject themselves to monitoring for compliance by an independent third party and to sanctions for non-compliance, which may include public reporting of violations or referral to the FTC. Enforcement may be provided by a seal organization, such as BBBOnline or TRUSTe.

Under the NAI Principles, network advertisers have committed to working with an independent third party enforcement program (*e.g.*, a seal program) to ensure compliance with the

²³ 2000 Report at 17; *see generally* Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security (May 15, 2000) (“ACOAS Report”).

²⁴ *See* NAI Principles at 3.

²⁵ ACOAS Report at 19-26.

Principles.²⁶ If no such program is available within six months, the NAI companies will submit to independent compliance audits the results of which will be made publicly available.²⁷

6. Additional Consumer Protections

Finally, the NAI Principles provide additional protections for consumers beyond those required by the traditional fair information practices. For example, NAI companies will not use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, or social security numbers for profiling.²⁸ In addition, NAI companies have committed to ensure that they obtain data for profiling from reliable sources.²⁹

III. RECOMMENDATIONS

The Commission commends the NAI companies for the innovative aspects of their proposal and for their willingness to adopt and follow these self-regulatory principles. Their principles address the privacy concerns consumers have about online profiling and are consistent with fair information practices. As the Commission has previously recognized, self-regulation is an important and powerful mechanism for protecting consumers, and the NAI principles present a solid self-regulatory scheme.

²⁶ On March 7, 2000, TRUSTe announced the formation of an Advisory Committee on Third Party Ad Servers and Licensee Practices. The mission of the Advisory Committee was to provide TRUSTe with options for “how its licensees can effectively implement fair information practices of notice and choice while addressing the consumer’s need for full and understandable disclosure, technological capabilities and constraints, and the nature of contractual relationships between third party ad servers and TRUSTe licensees.” The term of the Advisory Committee ended June 1, 2000, and its final product was proposed options for inclusion in the next version of TRUSTe’s license agreement. *TRUSTe Forms Advisory Committee on Third Party Ad Servers and Licensee Practices* (available at <http://www.truste.org/about/about_tpas.html>).

²⁷ See NAI Principles at 12.

²⁸ See NAI Principles at 3.

²⁹ See NAI Principles at 3.

Moreover, NAI members have agreed to begin to put their principles into effect immediately while Congress considers the Commission's recommendations concerning online profiling.

Nonetheless, backstop legislation addressing online profiling is still required to fully ensure that consumers' privacy is protected online. For while NAI's current membership constitutes over 90% of the network advertising industry in terms of revenue and ads served, only legislation can compel the remaining 10% of the industry to comply with fair information practice principles. Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program. In addition, there are unavoidable gaps in the network advertising companies' ability to require host Web sites to post notices about profiling, namely Web sites that do not directly contract with the network advertisers; only legislation can guarantee that notice and choice are always provided in the place and at the time consumers need them.³⁰

Accordingly, the Commission recommends legislation that would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites with respect to profiling. Such legislation would set out the basic standards of practice governing the collection and use of information online for profiling, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act,³¹ including authority to enforce those standards. In the context of profiling, determining the contours of the fair information practice of "choice," in particular, presents special challenges in framing a legislative mandate and in promulgating the required standards, which would require close attention.

The proposed legislation would also provide the implementing agency with the authority to grant safe harbors to self-regulatory principles which effectively implement the standards of fair

³⁰ The Direct Marketing Association (DMA) has indicated that, even in the absence of a contractual requirement, host Web sites that are members of DMA will commit to posting the notices required by the NAI Principles. The Commission commends DMA and its members for their commitment, but nonetheless believes that legislation is necessary to ensure that such notice is provided at all Web sites, not merely at DMA member sites.

³¹ 5 U.S.C. § 553. Rulemaking authority also would enable the implementing agency to take into account relevant technological advances that address online profiling issues.

information practices articulated in the legislation and subsequent rulemaking. The Commission presently believes that there is a good case the NAI Principles would qualify for such a safe harbor, but other industry groups or individual firms would be free to apply for safe harbor approval as well.³² Under the proposed legislation, all network advertising companies and all consumer-oriented commercial Web sites that permit the collection of information from or about consumers by network advertising companies would be required to comply with the four widely-accepted fair information practices.³³

The Commission recognizes that the implementation of these practices may vary with the nature of the information collected and the uses to which it is put, as well as with technological developments. For this reason, the Commission recommends that any legislation be phrased in general terms and be technologically neutral. Thus, the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules or regulations.

V. CONCLUSION

The Commission is committed to the goal of ensuring privacy online for consumers and will continue working to address the unique issues presented by online profiling.

³² Under the legislative framework recommended by the Commission, the final decision as to whether any self-regulatory guidelines qualify for safe harbor status will be made by the implementing agency, following any rulemaking, and after it has the opportunity to consider the guidelines and their effectiveness at the time the application for safe harbor treatment is made, and consider any relevant experience with comparable self-regulatory schemes.

³³ This legislative proposal supplements the legislation previously recommended by a majority of the Commission on online privacy generally. Among other things, it expands upon the “notice” element to require host Web sites to provide clear and conspicuous notice about the use of cookies or other technology by the network advertising companies to collect non-personally identifiable information.

Statement of Commissioner Mozelle W. Thompson

Online Profiling: A Report to Congress (Part 2) Recommendations

The Internet is generally recognized as an empowering technology that makes vast quantities of information readily available to consumers and businesses alike. The Internet's growth, as well as the concurrent emergence of related technologies, has led to the creation of a vigorous new electronic marketplace based upon direct personal connections between merchants and consumers. Benefits from this new marketplace include increased choices, efficiencies and other advantages for both business and consumers.

Information accessibility does, however, raise important concerns about personal privacy and the information that is collected from consumers by online businesses. Nowhere is this more clear than in the case of online "profilers" - a new industry that uses technology to gather information from Internet consumers. In connection with our work in the area of electronic commerce and the protection of consumers' personal data, the FTC has reviewed the actions of these online profilers.

The self regulatory program presented here provides the profiling industry with an opportunity to come out from the shadows and include consumers in its value proposition. More specifically, the program will require the Network Advertising Initiative ("NAI") companies to tell consumers what they are doing with consumers' personal information and give consumers a choice about whether to participate. But this program alone will not provide all that consumers need and want in this area.

Members of the profiling industry need to do more than derive self-benefit from gathering information from consumers that they follow around the World Wide Web. They must incorporate their self-regulatory program into a plan to demonstrate how consumers will benefit from information gathering and profiling. This undertaking is important both to consumers and to the future of the industry.

In addition, the Commission's work with the NAI and consumers shows that although the principles behind the NAI's self-regulatory program are sound, legislation is needed to address certain gaps in the program's reach. Accordingly, our report is also making legislative recommendations that I support because they are fully consistent with our view that well-drafted legislation in this area will bolster consumer confidence by allowing us to address areas that industry is unwilling or unable to address itself.

STATEMENT OF COMMISSIONER THOMAS B. LEARY
CONCURRING IN PART AND DISSENTING IN PART
Online Profiling: A Report to Congress (Part 2): Recommendations

I agree with the Report's recommendations relating to Online Profiling insofar as they endorse the NAI self-regulatory principles, advocate safe-harbor protections for these principles and others of a similar kind, and recommend some "backstop legislation." However, for the reasons expressed in my separate statement relating to online privacy generally,¹ I believe that legislation should focus on adequate "Notice" and not mandate across-the-board standards for other elements of the so-called "fair information practices."

There is a need for clear and concise disclosure of individual privacy policies in both the online and offline worlds, and this need is particularly compelling in the area of online profiling.² The technological capabilities for profiling are unfamiliar to many people and the practice may be perceived as particularly intrusive. However, if people are adequately informed about profiling, as well as other practices that raise privacy concerns, the marketplace should provide the appropriate mix of substantive privacy protections.

An appropriate marketplace response obviously depends on communication of consumer choices, which might initially suggest that some legislative attention to the element of "Choice" is

¹ Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress" (Statement of Commissioner Thomas B. Leary, Concurring in Part and Dissenting in Part) (May 2000).

² My previous Statement emphasized that the practice was "uniquely invasive" and that it is necessary to "ensure that consumers are adequately informed about these Internet capabilities." *Id.* at 8.

also appropriate. However, I have been reluctant to endorse this legislative option because, up to now, there has not been sufficient attention to what “Choice” means.

If mandated “Choice” simply refers to some mechanism whereby a consumer can either grant or refuse permission for online profiling, I would have no problem with it. A consumer should have the ability to exit the site before the fact of the visit becomes part of a profile. If, however, “Choice” means that a consumer can exercise this choice (either by opting out or failing to opt in) and still obtain the same benefits as a consumer less solicitous of privacy, it could be unfair. Consumers who object should not have a legally guaranteed right to “free-ride” on possible value and corresponding benefits made possible by the cooperation of those who do not object. Put another way, it should not be illegal to reward consumers who are willing to be profiled. The question of appropriate rewards or penalties attendant upon the exercise of various options can be extremely complicated.

Because there does not seem to be adequate discussion of this issue in the Report’s recommendations or in any of the numerous privacy bills thus far introduced, - - and because the “free-riding” issue may or may not be significant, depending on the individual business - - I am reluctant to endorse a legislative mandate for “Choice,” at this time. Similar concerns about unaddressed complexities apply to proposals for mandated “Access” and “Security.” It is not appropriate to defer all the tough issues for future rule-making.

Notwithstanding these reservations, I have voted for this Report. Unlike the earlier, more general Commission Report on Privacy Online, this Report contains more points with which I concur than points from which I dissent. This Report focuses on a particularly serious issue that

applies uniquely to the online world and it gives appropriate recognition to a comprehensive self-regulatory scheme. In these circumstances, the particular legislative proposals that I consider overbroad have a relatively limited impact. I am optimistic that further dialogue will continue to narrow our remaining points of disagreement.

DISSENTING STATEMENT OF COMMISSIONER SWINDLE

in *Online Profiling Project*, File No. P994809

I applaud the member companies of the National Advertising Initiative (NAI) for their agreement on self-regulatory principles concerning online profiling, *Self-Regulatory Principles For Online Preference Marketing By Network Advertisers*. The agreement provides transparency to consumers by furnishing notice of network advertisers' profiling on host Web sites and enabling consumers to choose not to participate in profiling.

I wholeheartedly endorse the language in the Commission's report commending NAI for the innovative aspects of its proposal and for its willingness to adopt and follow these self-regulatory principles. I recognize that there may well have been instances of unacceptable practices related to profiling, which has unique attributes. The NAI has recognized this concern and has put forward a commendable scheme of self-regulation. As the Commission has generally recognized,¹ self-regulation is an important and powerful mechanism for protecting consumers, and the NAI principles present a solid self-regulatory scheme.

My dissent here is not directed to the NAI principles. Rather, it is directed to the majority's recommendation that, despite NAI's laudable self-regulatory efforts, legislation is

¹ Federal Trade Commission, *Online Profiling: A Report to Congress (Part 2), Recommendations* at 9 (July 2000).

needed as a “backstop.”² Such legislation would have the same characteristics as the legislation recommended by a majority of the Commission in its 2000 Privacy Report, which I strenuously opposed.³ Again, the devil is in the details. I consider legislation that mandates the four fair information practice principles to be overly burdensome and unwarranted, for the reasons discussed at length in my dissent from the 2000 Privacy Report.⁴ Simply stated, we do not have a market failure here that requires legislative solution.

I oppose imposing burdensome regulation on an entire industry to address the 10% of advertisers who are not members of NAI – that is, those engaged in profiling to which the NAI self-regulatory principles would not apply. The majority can neither define nor identify who these advertisers are. We should not recommend legislation and regulation if we cannot demonstrate that the problems they are intended to resolve are real and significant. My colleagues, unwilling to accept a self-regulatory approach, find it necessary to support a highly regulatory scheme for an entire industry. I fear that the legislative recommendation will create an incentive for industry to discontinue seeking self-regulatory solutions.

² *Id.* at 10.

³ Federal Trade Commission, *Report to Congress on Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000) (Dissenting Statement of Commissioner Orson Swindle).

⁴ *See generally id.*

The majority has been hasty in calling for legislation and regulation governing online profiling. NAI just announced its self-regulatory principles to address concerns that have been raised about online profiling, including a notice requirement that we all agree is paramount. Technology also has just been introduced into the marketplace that will empower consumers to address online profiling without the need for government action.⁵ With each passing week, we learn more about industry initiatives and technological changes that can alleviate concerns about online profiling. Why not give these promising developments a chance before resorting to the heavy hand of government intervention?

I dissent.

⁵ *Microsoft Announces New Cookie Management Features for Internet Explorer 5.5* (July 20, 2000) (company press release).

Appendix: NAI Principles