

Consumer Privacy Rights and Online Behavioral Advertising

Tony Frost

As Federal Trade Commission Chairman William Kovacic

I. EXECUTIVE SUMMARY

Online behavioral marketing offers both great promise and considerable concern. The amount of data that is collected about consumers' internet browsing practices in order to specifically target advertisements towards them allows for much of the free content that consumers desire, but is also a source of concern because much of that information may be considered private by consumers.

The Federal Trade Commission is in an advantageous position to protect consumer privacy rights in the area of online behavioral advertising, notably because the location of its jurisdiction is so large. As such, the FTC is proposing three areas in which industry should move forward with the help of the FTC in order to help protect consumer privacy rights. (1) In accordance with the FTC proposed guidelines for self-regulation of online behavioral advertising, there are certain industry practices that need to be curbed and others that need to be clarified to the consumer public. (2) Industry participants must join with the FTC in educating the consumer public and businesses about the risks of gathering data on consumer behavior and as to the limits to which gathering consumer data is permissible. (3) The FTC must remain flexible in its approach to online behavioral advertising; specifically targeted regulations must not quickly become obsolete and the FTC must remain vigilant in assessing new risks to consumer privacy. This paper seeks to address these three major topics.

II. INTRODUCTION

The past decade and a half have witnessed explosive growth in consumers' ability to

easily access large amounts of information over the internet. The benefits provided to consumers are manifest. Consumers may search for, exchange, and create information faster and easier every day. This is a good thing. Inherent in this new medium, however, are risks to consumer privacy. This paper will explore both these issues and a path towards solutions for these risks.

The vehicle that allows consumers to freely surf the web and provides the infrastructure for the web's massive growth is online advertising. Much online advertising is similar to traditional advertising and is called contextual advertising.¹ Advertisements of this sort are the kinds we would find in newspapers or in magazines. These advertisements have been targeted towards end-users through the context of their surfing experience – what the users have typed into a search engine, or the content of specific web pages that they have visited. The content of a visited web-page or text of a search query suggests to advertisers that potential consumers may be interested in certain advertisement.

Behavioral advertising is a newer form of internet advertising that has proved better at targeting advertisements to consumers and thus more lucrative. Online behavioral advertising is the tracking of a consumer's activities online – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests.² Particular practices in this area that are concerning to the consumer privacy advocate are the gathering of data without consent, the transparency of data gathering techniques, the use and security of data that is logged by advertisers, and the probability that changing business models will lead industry to use

1 PC MAGAZINE, *Contextual Marketing*,

http://www.pcmag.com/encyclopedia_term/0,2542,t=contextual+marketing&i=56351,00.asp.

2 FTC, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, (2007), <http://www.ftc.gov/os/2007/12/P859900stmt.pdf>.

information in a different way than users had originally anticipated.³ The FTC must further be aware that technological growth means that there will undoubtedly be newer and more invasive privacy concerns in the future.

There are two broad categories of approaches that can be used in response to the consumer privacy concerns swirling around the collection and use of data in the internet age. First, companies that deal with sensitive consumer data may be able to police themselves to a certain extent. This is called self-regulation and is conducted by coalitions of companies that are invested in online advertisement, such as the Network Advertising Initiative (NAI).⁴ Second, specifically targeted regulations could be passed to ensure that certain minimum standards are being met and that advertisers are accountable for misusing or mistreating consumers' private data.⁵

The FTC, at this time, wishes to propose a three pronged approach for protecting consumer privacy rights in the area of online advertising. This approach seeks to retain the benefits of the technological improvements of the internet while properly safeguarding the privacies of consumers. (1) The FTC is currently concerned with several specific areas of behavioral advertising techniques, which are best exemplified by the FTC's proposed principles for self-regulation.(2) At the forefront of combating privacy risks that consumers face while using the internet is educating consumers as to the risks that they face while browsing. It is also important to educate the behavioral advertising industry as to what they are permitted to do within the scope of behavioral advertising. (3) The FTC must maintain flexibility in order to

3 *Id.*

4 NETWORK ADVERTISING INITIATIVE, *Written Comments for the FTC's Behavioral Advertising Town Hall Forum* (2008), www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf.

5 Edward Markey, *Consumers Have Right to Know What Broadband Providers Know About Web Use* (2008), http://markey.house.gov/index.php?option=com_content&task=view&id=3411&Itemid=141.

react to the inevitable consumer privacy concerns that tomorrow's cyberspace will bring.

Important in this area are the need to enact regulations that are specific while up-to-date, and the need to remain perceptive to new threats to consumer privacy.

III. CURRENT CONCERNS AND PLANNING FOR THE FUTURE OF CONSUMER PRIVACY

A. The FTC is an Appropriate Enforcer of Consumer Privacy Rights

The Federal Trade Commission (FTC) is in a particularly advantageous position to guard against harms to consumer privacy on the internet. The internet is a problematic area for enforcement of rules regarding privacy (or anything else for that matter), at least in part, because it is not tied to any particular geographic area.⁶ The victims and perpetrators of privacy harms are geographically scattered. Local enforcers do not wish to spend precious capital protecting consumers from other geographical areas. In the same way, local enforcers are hard pressed to enforce against perpetrators of harms from geographically distant areas. Furthermore, local enforcers simply do not have the resources to combat the privacy ills that plague their consumers' internet activity.⁷

The FTC is in a much better position than local enforcers to remedy privacy harms against consumers. The FTC is an agency with broad powers of enforcement, including the ability to cooperate effectively with foreign governmental agencies. Because of this it is well-equipped to safeguard consumer privacy in an area where bad-actors are difficult to hold accountable due to geographical proximity.⁸

The SAFE WEB act of 2006 is an example of the broadening of the FTC's powers to deal with geographically remote bad actors in the area of online crime.⁹ SAFE WEB has given the

⁶ See Peter Swire, *No Cop on the Beat 3*, accessible at <http://ssrn.com/abstract=1135704>.

⁷ *Id.*

⁸ Peter Swire, *Letter to the FTC*, <http://ftc.gov/os/comments/behavioraladprinciples/index.shtm>.

⁹ SAFE WEB Act, Pub. L. No. 109-455, §§ 4, 6 2006.

FTC the ability to redress harm in both the United States for harm done by foreign actors and in foreign countries by wrongdoers located in the United States. In using tools like SAFE WEB the FTC can find consumer privacy breaches and enforce privacy rights against wrongdoers.

B. Specific, Targetable Harms and the FTC's Proposed Principles Regarding Self-Regulation

The United States can now boast that 75% of its adults and 90% of its teenagers are accessing the internet.¹⁰ Because of this, it is time to take seriously the privacy concerns that accompany the many benefits of the internet.¹¹ However, proposing solutions to the problems that accompany internet consumption is difficult, in large part because of the difficulty in determining just what privacies consumers are concerned with. Different consumers hold different privacies dear. This implies an overarching consumer privacy protection theme: users must be equipped to make privacy choices for themselves when accessing the internet.

The internet has largely sprung to life in a legislative vacuum. The early years of the internet seemed more of a frontier world, where the web seemed a place of anonymity and enforcers were slow to realize its inherent privacy risks.¹² This assumption, however misguided, is one that is held by much of the consumer populace. The relatively recent introduction of more invasive advertising techniques such as behavioral advertising through the use of cookies, flash cookies, and deep packet inspection, for example, have become of greater concern to consumer privacy.

A primary concern is that, while online behavioral advertising is, at least in part, the vehicle through which consumers are able to travel the web for free, it is largely an invisible,

10 Susannah Fox , *Privacy Implications of Fast, Mobile Internet Access* (2008)
www.pewinternet.org/pdfs/Privacy_Fast_Mobile_Access.pdf.

11 *Id.*

12 Glenn Fleishman, *On the internet no one knows you're a dog* ,
<http://www.nytimes.com/2000/12/14/technology/14DOGG.html?>.

unknown commodity.¹³ Consumers often have a nominal understanding of web advertising (*i.e.* they understand that advertising, in some form powers their internet experience), but it is less clear that they have an understanding of the mechanics of that advertising.¹⁴ This is true with regard to many forms of behavioral advertising (especially pronounced are the more invasive techniques such as deep packet inspection (DPI)). Candidly, regardless of which privacies consumers wish to be protected, they will be unable to take precautions to stop threats of which they are unaware.

Recently, industry participants have shown an interest in participating in the protection of consumer privacy rights discussion through self-regulatory practices. Organizations such as the Network Advertising Initiative (NAI) have been instrumental in grouping together behavioral advertisers and suggesting minimum standards with which all participants must comply.¹⁵ Developing minimum standards of compliance to which industry participants can adhere in different areas is important for the protection of consumer privacy rights. It is currently unclear, however, whether the NAI or any self-regulatory body will be able to completely police the industry.

Legislation targeted towards these specific harms may, in fact, be necessary in order to ensure that consumer privacies are protected. This legislation would have to be as minimally obtrusive as possible in order to address specific privacy concerns that arise in the area of behavioral advertising. An example of a piece of legislation targeted toward specific privacy

13 FTC, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, (2007), <http://www.ftc.gov/os/2007/12/P859900stmt.pdf>.

14 TRUSTe, *Consumer Awareness and Attitudes about Behavioral Targeting*, http://www.truste.org/about/press_release/03_26_08.php (last visited Nov. 25, 2008).

15 NETWORK ADVERTISING INITIATIVE, *Written Comments for the FTC's Behavioral Advertising Town Hall Forum* (2008), www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf.

harms is the Children's Online Privacy Protection Act (COPPA).¹⁶ This law, passed in 1998, concerns the collection of data from children under the age of 13. The FTC has the authority to enforce COPPA against online advertisers.

In an area where technology is evolving as rapidly as this, it is important for the FTC to work quickly with industry and the Congress to determine solutions to specific privacy risks and harms that consumers face. Because of this, the FTC would like to call attention to the more pressing of these specific areas, which are best illustrated by the FTC's proposed principles for self-regulation.

The FTC's proposed guidelines were intended to outline the scope of consumer privacy protection in the area of behavioral advertising.¹⁷ While these principles articulate the broad scope of consumer privacy protection, they also help illustrate narrow instances of consumer privacy harm that must be dealt with. The proposed principles are: (1) Companies that gather data must be transparent regarding their data gathering practices and those practices must be within the consumers' control. (2) There must be reasonable security and limited data retention for all gathered consumer data. (3) Consumers must give affirmative express consent for material changes to existing privacy promises made by data gatherers. (4) Consumers must give affirmative consent for any sensitive data gathered.

i. Transparency and consumer control

Industry leaders must strive to be transparent to consumers with their data gathering practices. There is evidence to suggest that consumers simply do not know the extent to which their data is being gathered. The proposed principle reads:

¹⁶ Children's Online Privacy Protection Act, 15 U.S.C. § 6501–6506 (Pub.L. 105-277, 112 Stat. 2581-728, enacted October 21, 1998).

¹⁷ FTC, *supra*, note 13.

Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.¹⁸

Unfortunately, current data gathering practices do not uniformly adhere to this proposed guideline. Industry's data gathering behavior that have, at least in some cases, flouted this principle.

One area where industry is not being completely transparent and where consumers are not being given enough choice is in the practice of deep packet inspection (DPI). DPI is a surreptitious practice whereby a third party, in conjunction with a broad band internet service provider (ISP), scans "packets" of information as they are transferred from the ISP to the consumer.¹⁹ This practice is currently often practiced without express consent of the consumer and, ostensibly, without the consumer being aware of the practice's existence. This type of invasive cataloging of individual consumers behaviors without their consent or knowledge is at odds with the spirit of the proposed principal.

Even with the use of more innocuous techniques such as flash cookies, or local shared objects, industry has not made it clear to consumers that their behavior is being tracked.²⁰ While these techniques are not *per se* bad, their use without transparent notice to consumers is concerning. This is an area where specific regulations may be necessary if self-regulation cannot determine an adequate path to enable industry to become transparent about its actions to.

18 *Id.*

19 CDT, *Online Behavioral Advertising: Discussing the ISP-Ad Network Model* (2008), <http://www.cdt.org/publications/policyposts/2008/15>.

20 I'm a Super, *Flash Cookies: the Silent Privacy Killer*, <http://www.imasuper.com/66/technology/flash-cookies-the-silent-privacy-killer/> (last visited Nov. 25, 2008).

consumers

ii. Data retention and security

An issue of exceeding importance that the behavioral advertising industry must deal with is that consumer data must be kept safely. The FTC's proposed principle regarding such matter is as follows:

Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with the data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company ... Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.²¹

Most commonly, websites that wish to make use of behavioral data use devices called “cookies” to track the behavior of consumers on the internet.²² Through the use of cookies, businesses may keep, among other things, information on sites a user has visited, time a consumer has spent on each site, and the IP address of your computer. It is not unforeseeable that information could be tailored together to match personal users with their browsing habits. The amount of information gathered is staggering and it must be kept secure, both physically and virtually.

There is also considerable concern as to how long it is necessary for companies to retain data that they have accrued on consumers' browsing history. There is currently much worldwide discussion about what length of retention is appropriate.²³

the development of industry-wide standards may be advantageous in order to ensure that

21 FTC, *supra* note 13.

22 CDT, *Simple Behavioral Advertising*, <http://www.cdt.org/privacy/targeting/simple.php> (last visited Nov. 25, 2008).

23 Google reduces search data retention time to 9 months, but not enough, <http://www.edri.org/edrigram/number6.18/google-search-retention> (last visited Nov. 25, 2008).

privacy norms are properly developed and adhered to. A consistent manner of treatment of this data is an important goal so that consumers can be assured that their data is safe and so that industry participants can set appropriate expectations for their business models.

iii. Affirmative express consent for material changes to existing privacy promises

As companies seek to change their business models when developing behavioral advertising techniques, it is important for them to allow consumers to be aware of the changing practices that these companies are employing. The FTC proposed policy is:

As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers.²⁴

The rationale for this proposal is simple: consumers have a right to determine in what way their private data is used. If consumers have signed up for a service with the knowledge that data about their online behavior is going to be used in a specific way, then those consumers have a right to ensure that data is used only in the manner to which they agreed.

iv. Affirmative express consent for the collection and use of sensitive data

There may be legitimate business reasons for companies to collect sensitive data about consumers. It is imperative, however, that companies receive express consent from individuals whom they collect this data from. As such, the FTC proposed principle is: “Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising.”²⁵

The collection of sensitive data may be an area where a bright line rule could be

²⁴ FTC, *supra* note 13.

²⁵ *Id.*

developed, either by industry or in regulatory fashion, in order to establish minimum business practice standards. It would seem in the best interest of both consumers and of industry participants to have knowledge of what constitutes sensitive data. Some examples of sensitive data may include data on: sexual orientation, health records, social security numbers, or financial information.

This problem is compounded, and express consent of the individuals is extremely important, when companies who collect this data also collect what could be personally identifiable information (PII). In this case consumers may well be concerned that PII is being married to sensitive information. Express consent of the consumers must be required in order for this to happen.

The NAI, among other self-regulatory bodies, has commendably agreed not to use PII in conjunction with sensitive data.²⁶ However, it is unclear that what constitutes PII to the NAI or other self-regulatory bodies is a sufficiently strict standard such that data is actually not personally identifiable.

C. The need for comprehensive education of the consumer population and of business participants

Education, of both consumers and of businesses is an extremely important tool in allowing the FTC to stay ahead of the curve with regard to privacy rights of consumers in the context of behavioral advertising.²⁷ If the FTC and industry participants can better educate consumers as to the risks to their privacy that online behavioral advertising can pose (including protection mechanisms such as opt-out consent) then they will be more able to guard against the

²⁶ NETWORK ADVERTISING INITIATIVE, *Written Comments for the FTC's Behavioral Advertising Town Hall Forum* (2008), www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf.

²⁷ C-SPAN, *William Kovacic, Federal Trade Commission, Chairman*, <http://www.c-span.org/Watch/watch.aspx?MediaId=HP-A-10562> (last viewed, Nov. 25, 2008).

invasions of their privacy that are most concerning to them. Similarly, if the FTC can educate businesses as to exactly what they are permitted to do within the world of online behavioral advertising, then it is more likely that industry participants will be able to develop the best practices that they can while respecting consumers' basic privacy rights.

In order to properly educate consumers as to the data gather techniques that go along with behavioral advertising, it is important for the FTC to join with industry participants involved in the gathering of data for behavioral advertising. The best interest of the public and, ultimately, of businesses seeking to profit from online advertising is better served by a well-educated consumer base.

An illustrative poll recently taken by TRUSTe, a nonprofit organization designed to self-regulate privacy concerns on the internet, suggested that 71 percent of online consumers are aware that their browsing information may be collected by a third party for advertising purposes, but only 40 percent are familiar with the term “behavioral targeting.”²⁸ To the contrary however, it seems that consumers do, as a whole, wish for advertisements more specifically targeted towards their tastes.²⁹ This apparent contradiction implies the need for better education of the practices of data gathering and transparency with regard to how specifically targeted advertisements are created (through the use of behavioral data gathering techniques).

D. The need for the FTC to remain flexible when approaching the issue of behavioral advertising and consumer privacy

The nature of advertising on the internet and the relative immaturity of this type of advertising as a business practice suggest that there will be continued development and

²⁸ TRUSTe, *Consumer Awareness and Attitudes about Behavioral Targeting*, http://www.truste.org/about/press_release/03_26_08.php (last visited Nov. 25, 2008).

²⁹ *Id.*

refinement of it in the years to come. Circumstances surrounding how data is captured and to what end it is used are likely to change. Because of this, the FTC must remain particularly flexible with regard to behavioral advertising. This is particularly true in two ways: (1) The FTC must develop methods of regulating, or allowing for the self-regulation, of specific harms while making sure that the manner of regulation or self-regulation does not quickly become obsolete. (2) The FTC must remain open and flexible to possible legislation or cooperation with industry participants in order to remedy the consumer privacy risks of the future.

Statutes or promises made to consumers through self-regulatory bodies could be made broadly enough such that they cover all future privacy invasions due to behavioral advertising. This approach, however, is the proverbial sledge hammer when a scalpel is needed. What regulators sacrifice in terms of breadth of statutes or promises to consumers, they gain in more specifically tailored regulatory or self-regulatory solutions to problems. This dichotomy is at the heart of the balance between allowing for robust growth of the internet and protecting consumer privacies. Because of this it will be better for regulations or self-regulatory promises to be directed precisely at specific harms, but to be vigilant that these regulations or promises can become obsolete quickly and may therefore need to be amended.

IV. CONCLUSION

In conclusion, the FTC would like to stress three points with regard to behavioral advertisements and consumer privacy rights. (1) There are currently practices that concern privacy rights of consumers that are untenable and must be remedied. (2) The FTC must continue to educate the behavioral advertising industry participants and work with those participants in order to educate consumers at large in order to help minimize the privacy risks to consumers. (3)

Finally, in order to adequately approach the problem of consumer privacy rights in the ever evolving world of behavioral advertisements on the internet, the FTC must retain flexibility in both passing regulations and in being vigilant for new abuses of consumer privacy. The FTC looks forward to working with consumers and industry participants in the ongoing challenge of assuring consumer privacy rights and in fostering an environment that produces the broadest benefits possible to consumers.