Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives

Melissa Jane Dark
Purdue University, USA
Chapter 8
Behavioral Advertising Ethics

Aaron K. Massey
North Carolina State University, USA

Annie I. Antón
North Carolina State University, USA

ABSTRACT
Behavioral advertising is a method for targeting advertisements to individuals based on behavior profiles, which are created by tracking user behavior over a period of time. Individually targeted advertising can significantly improve the effectiveness of advertising. However, behavioral advertising may have serious implications for civil liberties such as privacy. In this chapter, we describe behavioral advertising ethics within the context of technological development, political and legal concerns, and traditional advertising practices. First, we discuss the developmental background of behavioral advertising technologies, focusing on web-based technologies and deep packet inspection. Then, we consider the ethical implications with a primary focus on privacy of behavioral advertising technologies. Next, we overview traditional market research approaches taken to advertising ethics. Following that, we discuss the legal ethics of behavioral advertising. Finally, we summarize these cross-disciplinary concerns and provide some discussion on points of interest for future research.

INTRODUCTION
Behavioral advertising is a method for targeting advertisements to individuals based on their actions. Market researchers construct behavior profiles by tracking user actions, such as purchases, recommendations, or reviews. Advertisers use an individual’s behavior profile to tailor advertisements to that individual. An online behavior profile can be built by tracking the websites people visit on the Internet. The development of new behavioral advertising technologies, such as Deep Packet Inspection (DPI), makes the construction of behavior profiles possible in contexts where it was previously impractical. Behavioral advertising is currently a challenging public policy concern with interdisciplinary ethical implications as evidenced
Behavioral Advertising Ethics

by recent efforts by the U.S. Federal Trade Commission (FTC) to encourage best practices.

New behavioral advertising technologies raise challenging ethical questions that this chapter seeks to address. How should consumers and advertisers approach the tradeoff of privacy for improved advertising effectiveness? What level of control over behavioral tracking should consumers have? Is first-party behavioral advertising more ethical than third-party behavioral advertising? Are there important ethical differences between web-based and network-based behavioral advertising? Is an opt-in default more ethical than an opt-out default? More specifically, who owns data regarding online behavior? How should traditional market research ethics affect behavioral advertising? Do current behavioral advertising technologies violate legislation or are they in some other way ethically dubious? We aim to clarify the scope and ethical implications of these questions.

Many of these ethical questions are civil liberty concerns. Civil liberties are rights in freedom. For example, the freedom of religion, freedom of speech, the right to keep and bear arms, the right to not be discriminated against, the right to a fair trial, and the right to privacy are all civil liberties. These freedoms limit government power and prevent governments from unduly intervening in the lives of citizens. Because many of the ethical issues regarding behavioral advertising ethics are fundamentally consumer privacy concerns, we have chosen this as a focus for this chapter.

Privacy is a particularly challenging ethical concern because it is inherently difficult to define. George Washington University Law Professor Dan Solove (2008) describes privacy as a “concept in disarray” (p. 1) that “[n]obody can articulate” (p. 1). Possibly the best-known definition of privacy comes from an 1890 law review article by Warren and Brandeis wherein they stated that privacy is “the right to be let alone” (Warren & Brandeis, p. 193, 1890). As data processing became more important Alan Westin (1967) recognized that being left alone was insufficient; he describes privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (p. 7). This recognizes that providing control to individuals is an important aspect of privacy. A more recent control-based definition by Jim Harper (2004) emphasizes even further the importance of the individual consumer. Harper (2004) calls privacy “the subjective condition that people experience when they have the power to control information about themselves” (p. 2). For the purposes of this chapter, we will assume Harper’s control-based definition of privacy because it acknowledges both that privacy means different things to different people (i.e. that it is subjective) and that privacy involves an element of consumer control.

The FTC (2000a, 2000b) has voiced concerns that behavioral advertising violates consumer expectations of privacy. However, the difficulty of defining and valuing privacy hampers efforts to compare the economic benefits of behavioral advertising to the cost of constraining civil liberties (Solove, 2008; Szoka & Thierer, 2008). In an empirical study on the effectiveness of behavioral advertising, Yan, Liu, Wang, Zhang, Jiang, and Chen (2009) reported that the information collected to construct a behavior profile can be used to improve advertising effectiveness by at least 670% (Yan et al., 2009). This tension between powerful economic incentives and important civil liberties has resulted in scrutiny from the FTC (2000a, 2000b, 2007, 2009), U.S. Senate (Privacy Implications, 2008), and the U.S. House of Representatives (What Your Broadband Provider, 2008, Communications Networks, 2009).

Advertising-based business models are common on the Internet. The FTC (2000a) reported to Congress that Internet advertising revenues for 1996 totaled $301 million. By 2001, Internet advertising produced $7.2 billion in revenues (Internet Advertising Bureau [IAB], 2002). In 2007,
Internet advertising revenues had grown to $21.2 billion a year, with search-based advertising from companies like Google and Yahoo comprising 41% of that total (Internet Advertising Bureau, 2008). eMarketer (2007), a company that provides statistical research on e-business and online advertising, estimated that industry-wide spending on behavioral advertising techniques would grow from $220 million in 2005 to $3.8 billion in 2011, a 17-fold increase.

Developments in behavioral advertising technologies are driving the potentially explosive increase in its use. Behavioral advertising is a relatively new technique in the Internet advertising industry. Online advertisements were first targeted to consumers though advertisements that did not change based on the individual viewing the website. We refer to this practice as ‘static advertising.’ In static advertising, targeting was done based on the content of the website. If the website was about skiing, then the ads would be for products like ski jackets and particular ski lodges. However, some websites delivered primarily dynamic content, and for those sites static advertising is less effective.

Advertisers developed a new mechanism for targeting advertisements, called contextual advertising, based on the dynamic content of the website. In contextual advertising, information used to generate advertisements typically is not stored or linked to an individual. As a result, it is not necessary to generate or store individual behavioral profiles. Consider Google’s Gmail service, which automatically scans the content of an email, determines the context of that email by identifying key words and phrases, and displays advertising previously determined to be related to that context. Although there was a firestorm of discussion amongst privacy advocates at the time (Electronic Privacy Information Center, 2004; World Privacy Forum, 2004), the debate has calmed down significantly since the details of the service became better understood. A computer algorithm determines the context of each message by scanning email contents and selects an ad to display. Google employees do not read email delivered to Gmail to generate these ads. Also, Google’s Gmail service is voluntary. If someone remained concerned about their privacy after hearing how the service worked, they could avoid the potential privacy violation by simply using a different email service provider.

The remainder of this chapter is organized as follows. First, we provide some background on the developmental history and operation of behavioral advertising technologies with a specific focus on DPI. Following that, we discuss the impact of technology ethics on behavioral advertising practices. Next, we describe the traditional market research approaches to advertising ethics because market research ethics has a long and rich history that provides interesting insights into the challenge of behavioral advertising (Blankenship, 1964; Tybout & Zaltman, 1974). Then, we discuss the legal implications of using DPI for behavioral advertising. Finally, we summarize the discussion and provide some thoughts on future research.

BACKGROUND

In this section, we describe the technical differences between first-party and third-party behavioral advertising, and detail specific web- and network-based technologies used to construct behavioral profiles online.

First-Party Behavioral Advertising

To start our discussion, consider the simplest form of behavioral advertising: an offline loyalty card program. Many businesses, such as supermarkets and bookstores, offer loyalty card programs to their customers. A loyalty card program allows a customer to trade personal information, such as their name, address, and shopping history, in exchange
for discounts on products sold. The business can use the shopping history to produce individually targeted advertisements. For example, if a customer in a loyalty card program at a bookstore purchases three books on the American Revolution, then the bookstore could use this information to send coupons or other advertisements on U.S. history books to that customer. Most loyalty card programs are examples of first-party behavioral advertising.

In first-party behavioral advertising, the party displaying the advertising is also the party collecting the behavioral profile. First-party behavioral advertising can be accomplished through a multitude of techniques, including web-based techniques that could also be used by third-party advertisers. Amazon.com’s recommendation service is a well-known example of first-party behavioral advertising. Amazon.com can collect the entire set of page links clicked on by registered, logged-in Amazon.com shoppers without being limited to the technologies on which a third-party advertiser would be forced to rely. The raw data is known as clickstream data, and it can be coalesced into a more concise behavioral profile through analysis and data mining. Amazon.com has patented their product recommendation analysis and data mining techniques (Wolverton, 2000). Amazon.com can use their behavior profiles to recommend other products to users. In addition to clickstream data, Amazon.com has access to customer wish lists, reviews, and ratings. This full access to customer data is only possible in first-party behavioral advertising systems. It is important to note that access to more data does not necessarily result in more effective advertising results. In fact, data analysis becomes harder as data sets change or grow in size and complexity.

**Third-Party Behavioral Advertising**

In third-party behavioral advertising, the party displaying the advertisement is different from the party collecting the behavior data and selecting which ad to display. Third-party behavioral advertising occurs when a web-based company partners with a dedicated advertising company that uses behavioral advertising techniques. The web-based company is the first party, the consumer is the second party, and the advertising company is the third party. In these partnerships, the third-party advertising company collects individuals’ information to improve their targeting. Third-party advertisers use two broad techniques to construct behavior profiles: web-based or network-based. Each technique can be implemented with different underlying technologies. For example, cookies, web bugs, and local shared objects (LSO), also known as flash cookies, are technologies that can support web-based behavioral advertising. Advertising companies serving ads to many websites with these technologies can construct behavior profiles by tracking individuals as they surf from one website to another.

Currently, advertisers use two third-party behavioral advertising techniques to construct behavior profiles: web-based profiling and network-based profiling. Web-based techniques involve tracking behavior as users surf the Internet, but they are limited because advertisers can only collect information on websites to which they have access, such as those sites on which they advertise. More recently, Internet Service Providers (ISPs) have adapted network management techniques, like DPI, to do network-based profiling of their customers’ behavior on the Internet. Network-based techniques are capable of building more detailed behavior profiles than web-based techniques because they have access to all online behavior rather than being limited to just web traffic. If this technology is widely adopted, then ISPs could operate as third-party advertising agencies. This would provide ISPs with an additional revenue source and improve the quality of broadband infrastructure, but it would also raise ethical concerns about pervasive surveillance of online activities affecting consumer privacy and free speech.
Web-Based Techniques

Web-based techniques for behavioral advertising involve tracking behavior as users surf the Internet. These techniques are limited because advertisers can only collect information on websites to which they have access, such as those sites where they advertise. The first web-based behavioral advertising technologies came in the form of browser cookies and web bugs (Federal Trade Commission [FTC], 2000a; FTC, 2000b).

A browser cookie is a small file that contains information about the user and the user’s session with a particular domain name and is stored on an Internet user’s computer. Cookies are built into the Hypertext Transfer Protocol (HTTP), which is an application level protocol that runs on the Internet. Netscape began supporting cookies in 1994, and Microsoft’s Internet Explorer began supporting cookies in 1995. Cookies can be used to identify or authenticate the user to the website, and can store session information such as the items currently in a user’s electronic shopping cart for a particular domain.

Cookies loaded from the same domain as the website visited are called first-party cookies. When an advertisement on a webpage is hosted on a third-party server, cookies may be transferred by the HTTP request that loads the advertisement. These cookies are called third-party cookies. Domains can access only those cookies that they have previously set. For example, a cookie set by the domain www.example.com is only accessible to www.example.com. Most browsers allow users to set separate preferences for first-party and third-party cookies. Typical preferences include allowing cookies automatically, blocking cookies automatically, or prompting the user to choose whether to allow or block cookies as the user browses the web. In addition, users can install browser extensions for Firefox like Adblock Plus or NoScript to prevent loading advertisements or the associated cookies.

Since cookies are the primary mechanism for identifying returning users, they can be used to differentiate between users desiring behaviorally targeted advertising and users desiring no targeted advertising. The former are called “opt-in” cookies, which indicate a desire to participate in information collection, and the latter are called “opt-out” cookies, which indicate a desire to avoid participation in information collection. There is no standard or industry-wide preference between opt-in and opt-out cookies. As a result, users may have both opt-in and opt-out cookies on their system at the same time. This can lead to challenges for individuals seeking to control their information collection because browsers only offer the ability to delete all cookies and anti-spyware programs often delete cookies (Swire & Antón, 2008). Individuals concerned about their privacy may prefer to keep opt-out cookies and delete opt-in cookies (Swire & Antón, 2008).

A web bug is fundamentally different from a cookie because it does not store data on the user’s computer. Web bugs are typically tiny web graphics that are a single pixel in both height and width. They are included in the HTML for a website, but may be hosted on an advertising server. Web bugs usually match the background color of the website and, as a result, appear invisible to the Internet user. When the website is loaded, the advertising server can track all the sites for which a particular IP address requests a web bug image by logging the IP address of the Internet user’s HTTP request for the web bug.

Web bugs may be used in tandem with cookies to increase the chances of collecting behavior information. Although web bugs cannot collect as much information as cookies, they are more difficult to block than cookies because browsers currently do not allow users to set preferences for blocking web bugs. Web bugs are third party images and do not need to use Javascript, and Javascript-blocking browser extensions, such as NoScript, may not be able to block web bugs.
Browser extensions attempting to block all advertising from third-party servers, such as Adblock Plus, may perform better.

Another important difference between cookies and web bugs is that web bugs can be used more easily to track users in HTML-formatted emails. An advertiser or spammer can verify that an email address is valid and active using a web bug. Consider the email address bob@example.com. To verify this email address, an advertiser could set up a web bug with an identifying filename, such as bob-at-example-dot-com.jpg, on a third-party server and include that image in an HTML-formatted email sent to the email address. Assuming that bob@example.com is a valid, active email address and that the owner of that email address allows HTML-formatted email, then an HTTP request for the image will be made when the owner opens this email. The advertiser merely needs to record this request in his log files to determine whether both the timestamp and the email account are valid. It is important to note that web bugs do not work with email if the email client has been configured not to accept HTML-formatted email.

LSOs, also called flash cookies, are another technology for web-based behavioral advertising. LSOs are built into all versions of Adobe Flash Player—a common browser extension that supports audio, video, and online games. YouTube videos make use of Adobe Flash Player. Essentially, LSOs serve the same role in a flash-based setting as cookies in an HTTP-based setting, which is why they are sometimes called flash cookies. They are used to store settings, such as a volume preference, or keep track of session information, such as a score in a game, and they are only accessible to the same domain that created them. Although LSOs perform similar functions as cookies, user preferences for LSOs are set differently. Settings for LSOs are stored in the Adobe Flash Player Settings Manager and not in the standard browser preferences. Adobe has published documentation on their Settings Manager\(^6\) and a walkthrough on how to manage and disable LSOs\(^7\). A browser extension that deletes LSOs, called Objection\(^8\), is available for Firefox.

Through cookies, web bugs, and LSOs, third-party advertisers are able to compile behavioral profiles of Internet users. These profiles can include the content of the pages visited in a particular website, the amount of time the user spends on a particular page, any search terms the user enters for that site, and any purchases the user makes while on the site. This information can be tracked regardless of whether or not the user clicks on an advertisement.

**Network-Based Techniques**

Network-based techniques for behavioral advertising build behavior profiles from all network traffic rather than just web-based traffic. Network traffic is composed of discrete data packets sent through a layered set of protocols collectively known as the Internet Protocol suite. Layered protocols operate by abstracting away details to simplify the construction of a communications network. The Internet’s layered network architecture enables encapsulated services starting with the hardware layer through the network layer up to the application layer. Each layer provides just enough information, in the form of a packet header, to complete the delivery of a packet. Packet headers are critical elements of network layering. They identify the source and destination for a particular packet at a particular layer. This identification is roughly similar to the routing information of an envelope sent through the postal system, which identifies the recipient’s address and the sender’s (return) address.

The concept of an envelope for real world postal mail is a common analogy for packet headers, but there are several inaccuracies with this analogy. First, packets may be wrapped in many packet headers with the outermost packet header being the one that represents the current layer. Second, as the packets are delivered, the packet headers are updated, removed, or altered as a part of the
normal course of delivery. Finally, and perhaps most importantly, the contents of a packet are not invisible or hidden by a packet header. In regular mail, the envelope protects the contents of a message.

The delivery of packets according to their packet headers alone is the intended design of the Internet’s layered protocols. Deep Packet Inspection is a label for a broad classification of technologies that inspect beyond the packet header to view the actual data being delivered. DPI techniques are called “deep” packet inspection because they look “deeper” into each packet to see past the header, glimpsing the actual data contained in the packet. By inspecting the packet’s payload contents for all packets that an Internet user sends or receives, ISPs are able to generate a detailed behavioral profile from which targeted advertising can be constructed. In contrast to web cookie-based approaches, customers have no way to control DPI-based behavioral advertising with their browser preferences.

DPI ignores abstraction, which is a convenience of network protocol design. Looking at the data itself has been possible since the original design of the Internet, but the culture of the early Internet opposed violating abstraction in network design. Saltzer, Reed, and Clark (1984) describe the engineering efficiency gained by maintaining abstraction layers. This concept is called the end-to-end design principle (Salzer, Reed, & Clark, 1984). Essentially, the end-to-end design principle states that application design should be done at the endpoints in a communication system (Salzer, Reed, & Clark, 1984). For example, since all information transferred over the network is broken up into packets, it is possible that the packets will arrive out of order. It is easier to let the endpoints correct the order of the packets than to construct the core of the network so that it ensures that packets arrive in the correct order. A single error in delivering a packet could cause delays due to the need to retransmit the packet.

As a consequence, all subsequent packets would also be delayed.

The end-to-end principle links DPI to network neutrality, which is another highly debated ethical concern in network management. Network neutrality is difficult to define and actually comprises three separate ethical debates. First, network neutrality can describe an argument about tiered pricing schemes for end-users or for content providers. Second, network neutrality can describe a free speech argument about filtering content in the core of the network by blocking sensitive political, religious, racial, or sexual content. Finally, network neutrality can describe the argument about maintaining the culture of the end-to-end principle in networking. It is in this final argument that DPI and network neutrality are linked. If the culture of the end-to-end principle is not maintained, then end-users lose a measure of autonomy in their communications. As a result, the use of DPI involves a narrower set of ethical decisions than network neutrality.

The link between DPI and network neutrality exists because DPI technologies violate the end-to-end principle in two ways. First, DPI inspects beyond the packet header as packets are in transit for content analysis, classification, and collection. This type of application development in the core of the network violates the end-to-end principle. Second, in order to serve behaviorally targeted advertising, DPI inserts a fake web cookie into the packet streams of Internet users surfing the web. In non-DPI networks, the only way that a cookie can be placed on a user’s browser is if the server at the other end of the communication placed it. However, in DPI networks, fake web cookies, which can be used as identifiers for third-party advertising services seeking to serve behaviorally targeted advertisements, must be placed on the user’s browser by the ISP. This is a violation of the end-to-end principle as well because the cookie was generated in the core of the network by the end user’s ISP rather than at the endpoint.
Since DPI refers to any technology that inspects the payload content of the packet rather than just the packet header, DPI techniques can be used for purposes other than advertising. For example, DPI can be used to filter spam, viruses, or malware out of the network by inspecting packets for identifying signatures. In addition, DPI can be used to improve quality of service by prioritizing packets for real-time media applications like streaming audio, streaming video, or VOIP (Voice Over Internet Protocol) telephony. These other uses of DPI could provide ISPs with an additional revenue stream without the need to collect personal information. For example, an ISP using DPI to improve the quality of streaming video from a particular domain, such as YouTube or ESPN, could charge customers an additional monthly fee to receive prioritized quality of service on these domains. Because these services are not advertising-based, we will not discuss their ethical implications other than to say that this use of DPI could be considered an unethical violation of network neutrality.

**BEHAVIORAL ADVERTISING ETHICS**

Ethics is the study of moral values. It is the authors’ view that technology exists in an inherently value-free state. For example, consider a hammer—if used to build a home, then the hammer serves an ethically valuable, or “good,” purpose. If used as a weapon to attack an innocent person, then the hammer serves an ethically questionable, or “bad,” purpose. The value-free nature holds for all forms of technology, and it has been recognized by several important computer technology organizations. For example, the Association for Computing Machinery (ACM), which the world’s oldest scientific and educational computing society, states in their Code of Ethics (Association for Computing Machinery, 2009) that, “Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources” (Section 3.3, para. 1). Similarly, the IEEE Code of Ethics (Institute of Electrical and Electronics Engineers, 2006) seeks “to improve the understanding of technology, its appropriate application, and potential consequences” (Point 5) because the ethical values resulting from inherently value-free technologies are a result of human understanding and value-laden use of technology. In this section, we seek to comment on the value-based ethical concerns involved in the development and use of behavioral advertising technologies.

**Value-Based Ethical Concerns in First-Party Behavioral Advertising**

In first-party behavioral advertising, the party doing the advertising and collecting the profile is also the party being visited by the end user. Because the party collecting the information is also interested in selling products to that individual, the company has a vested interested in ensuring that the behavioral profile is secure, and that the end user has the ability to update or correct it. In short, first-party advertisers must be concerned about losing customers if their information practices do not satisfy the individuals to whom that information refers.

Third-party advertisers do not necessarily have the same level of economic interest because they operate as middlemen. They are concerned with improving their advertising effectiveness with accurate customer information, and they have an interest in keeping the information they collect secure to ensure that their competitors do not have access to it. However, third-party advertisers do not have the same level of concern about losing individual customers based on their information practices because their customers are other businesses rather than individuals.

First-party behavioral advertising is regarded by the FTC (2009) as “more likely to be consistent
with consumer expectations, and less likely to lead to consumer harm than other forms of behavioral advertising” (p.26). Consumers can be made aware of a given site’s data collection practices via a website’s privacy policy. When data collection is conducted through cookies, consumers can control whether or not they wish to participate by directing their browser to accept or reject cookies from a given domain. This feature is common to all major browsers and can be configured without extensive technical knowledge.

Value-Based Ethical Concerns in Third-Party Behavioral Advertising

In third-party behavioral advertising, the party being visited by the end user is not the same as the party collecting behavior information or serving advertisements. While first-party behavioral advertising tracks an individual’s behavior in a single domain, third-party behavioral advertising can track an individual’s behavior across multiple websites. This could entail a third-party, generally an advertising company, setting a single cookie on the users’ browser and accessing it as the user browses from website to website.

For example, if a ski lodge website were to support third-party behavioral advertising, then the site may attempt to set a cookie for a third-party advertising company. If the user subsequently visits a different domain to book a travel package and that travel website hosted ads through the same advertising company, the advertising company would recognize the user and serve advertisements related to ski trips and ski lodges even if it was the user’s first time visiting the subsequent travel site.

Both first- and third-party behavioral advertising allow Internet users some level of control over tracking if they depend on stored cookies for user identification. Modern browsers allow users to tailor how they want to manage cookies. As mentioned in the background section, individuals concerned about privacy often delete or actively manage the cookies stored on their browsers. However, this level of control is not afforded to individuals tracked through newer, non-cookie based technologies. For example, web bugs are often transparent and designed to be invisible from the end user’s perspective. In addition, browsers and email clients do not commonly offer the ability to block web bugs.

The Ethics of Deep Packet Inspection Technology

Preserving the privacy of ISP customers is the primary ethical concern surrounding Deep Packet Inspection (DPI) technologies. DPI-based third-party behavioral advertising can be implemented in an undetectable fashion from the end user’s perspective. If privacy is a desirable control-based right for end users of an ISP’s services, then the ethical questions regarding behavioral advertising can be simply stated as follows, “Does the user have control over when their Internet usage is monitored by their ISP?” The answer to this, at least in part, is that customers have two clear technologies that provide them with control over their privacy: encryption and onion routing.

Strong encryption protocols like Secure Socket Layer (SSL), Transport Layer Security (TLS), and Pretty Good Privacy (PGP) can be used to prevent DPI technologies from being able to decipher the contents of the packet payload data. There are two problems with encryption as a means to protect end user privacy. First, encryption technologies require more processing power for servers. Providing encryption on a popular web server could prove to be prohibitively expensive or impractical, even for larger web-based organizations. Second, many websites simply do not support encryption at all. For these sites, the end user is still caught between using the service, being monitored by DPI technologies, or not using the service at all.
Onion routing is another means to protect privacy when using ISPs that employ DPI. Onion routing provides a bi-directional, private, encrypted tunnel for all Internet traffic (Reed, Syverson, & Goldschlag, 1998). Because of this tunnel, the web server cannot accurately identify the end user; it can only identify the end of the tunnel, called an exit node. The tunnel also prevents ISPs from determining the content of the traffic being delivered because the information is encrypted until it reaches the exit node. The name “onion routing” comes from the protocol’s design, which calls for layers of encryption to hide user details.

In theory, onion routing seems to be the answer to the ethical concerns raised by DPI. In practice, onion routing introduces two important problems. First, servers that provide onion routing services cannot support the demand. The extra processing and bandwidth needed often painfully slow the available servers. A single onion router must support and encrypt all of an Internet end user’s traffic to be effective. Such a design does not scale well to many thousands of users. Second, onion routers eventually have to decrypt the traffic that they are protecting. Onion routing is not end-to-end encryption; it merely provides source address anonymization in the segment of the route that deploys onion routing. For example, consider Bob, who is a New England Patriots fan living in Indianapolis, which hosts a rival team: the Indianapolis Colts. One day Bob decides to shop for Patriots apparel online. If Bob is using an onion router to protect his communication, then the onion router has to decrypt his Internet traffic at the exit node and pass it along to Bob’s online store of choice. If Bob’s browsing includes any unencrypted personal information, such as a username or credit card, then any router or server between the exit node and the online store at which Bob is shopping has a chance to identify Bob as a New England Patriots fan. Individuals desire better results from technology when seeking to control their privacy.

Market Research Ethics

Market research has a long history of addressing the ethical implications of advertising and should be a part of the behavioral advertising ethics discussion. Advertisers recognize that ethics has important relationships with the quality of market research data and ethical consumer protection concerns (Blankenship, 1964; Tybout & Zaltman, 1974; Warne, 1962). Tybout and Zaltman (1974) state, “an understanding of ethical issues involved in marketing research is essential for producing quality research” (p. 357). Many professional marketing organizations, including the American Marketing Association and the Market Research Society, maintain Codes of Ethics that should also impact any discussion of behavioral advertising. These Codes of Ethics discuss ethical practices for generating profiles of specific consumer groups through focus groups, interviews, and other traditional market research techniques. However, market researchers also recognize that a Code of Ethics is not enough. Blankenship (1964, p. 26) writes, “Codes alone cannot provide the answer. They can merely provide a few guideposts.”

Market researchers seek to understand what people need, want, or believe for various purposes, including designing products, pricing products, improving product placement, and advertising. Marketers are tasked with determining what people want to buy despite the fact that many consumers do not know what they want. In an attempt to improve advertising results, the scope of advertising has expanded over time to include many sensitive areas of a person’s life, such as education, family planning, and government (Tybout & Zaltman, 1974; Warne, 1962). Market research must be done carefully to ensure the quality and accuracy of the data while not violating individuals’ rights.
Researchers use standard customer’s rights as a guide to ensure ethical market research practices through surveys and interviews (Tybout & Zaltman, 1974). These rights are four-fold: the right to choose, the right to safety, the right to be informed, and the right to provide feedback and be heard. A consumer’s right to choose is traditionally embodied as the choice to take a survey or participate in an interview (Tybout & Zaltman, 1974). Marketers have a strong incentive to allow the consumer to freely choose to participate in market research because they are concerned about the quality of the data obtained from a ‘forced’ interview or survey (Tybout & Zaltman, 1974). Although this seems straightforward, marketers could subtly trick consumers into participating in market research that they may otherwise decline. Tricks could include outright deception or more subtle psychological pressure to participate. Consumers who are ‘forced’ or otherwise pressured to provide information may be self-conscious or behave differently than they would otherwise.

In addition to the various methods to pressure participation, so-called unobtrusive measures could be used to collect data about consumers without informing them of the collection (Tybout & Zaltman, 1974). Imagine a door-to-door market researcher using the pretext of trying to determine a homeowner’s opinion of vacuum cleaners. Once the researcher is allowed into the customer’s home, he can learn all sorts of additional information about that homeowner, such as their taste in furniture, art, and lifestyle. If this information is recorded for marketing purposes without informing the customer, then that customer’s right to choose has been violated.

In the case of DPI, there are at least two clear ways that an individual’s right to choose may be violated. First, if an ISP has a monopoly in a particular market, the individual’s right to choose is tied to their use of the Internet. Although the individual may wish to keep their web browsing habits to themselves, their wish to browse the web may be stronger. Second, in the initial pilot studies conducted by Comcast and NebuAd consumers were informed of the opportunity to opt-out of the pilot study through an obscure and easily disregarded notice (Anderson, 2008). The obscure nature of the notice itself may have violated the individual’s right to be informed, and the policy may have violated the individual’s right to choose by not ensuring that Comcast customers were freely choosing to take part. More importantly, the incentives are significantly different for DPI than for market research. Many consumers are completely unaware of the technology behind DPI or the types of information collected. In addition, individuals feel comfortable doing things online that they would not do in a traditional, real-world store. As a result, marketers may be more confident about the quality of the data and more inclined to use unobtrusive measures to obtain the data they need. After all, since individuals are unaware and intrinsically comfortable at their keyboards, the behavioral data they produce is likely to be high quality.

Tybout and Zaltman (1974) show the consumer right to safety in market research has at least three components: protection of anonymity, protection from undue stress, and protection from deception. Protection of anonymity safeguards the confidentiality of individuals’ answers to sensitive questions, such as those regarding income, age, religion, or politics. Protection from undue stress is traditionally meant to protect individuals from potential psychological burdens. For example, if an individual with little knowledge of baking is asked a variety of questions about cake pans, then they may become distressed about their lack of cooking ability. Protection from deception ensures the consumers’ ability to make informed choices regarding market research. It is particularly important given that DPI technologies can be used without alerting or informing consumers.

During the Senate Committee on Commerce, Science, and Transportation’s hearings on behavioral advertising in 2008, one senator raised the question of how profiles were created in the
Behavioral Advertising Ethics

days before Deep Packet Inspection (Privacy Implications, 2008). It is important to recognize that advertising firms made ethical decisions about the collection of customer profiles and purchasing habits for the purposes of targeting advertisements. Directed marketing companies have been collecting profiles for this purpose decades prior to the advent of DPI technologies. These profiles were combined into comprehensive lists that included the names, addresses, phone numbers, and other contact information for people with similar profiles. The fact that consumer mailing lists were created, bought, sold, and used for marketing purposes prior to the Internet does not directly justify the development or use of DPI, but it may provide insight that helps answer the ethical concerns raised by behavioral advertising.

Earlier directed marketing technology consisted of mailing lists and databases with contact information that did not contain enough information about individuals’ preferences to target advertising behaviorally. Instead, directed marketing entailed classifying consumers into groups, such as “suburban middle class family” or “urban 20-somethings.” Marketers sent specially designed marketing materials directly to the homes of individuals within these consumer groups. For example, an ad for a new bedroom set could be sent only to “suburban mothers” while an ad for football tickets could be sent specifically to “urban 20-something males.”

Although this was more efficient than mailing advertisements to every household, directed marketing had relatively low response rates. It was driven by the 2% rule, which states that any of these marketing materials with a response rate of 2% or greater were worth the investment (Hughes, 1996). Most directed marketing campaigns resulted in 3-4% response rates, which meant that even a small change in effectiveness could result in relatively large economic benefits to the company (Department of Health Education and Welfare, 1973). Given these response rates, direct marketers were eager for any technology that might improve advertising effectiveness. In 1973, the Department of Health, Education, and Welfare voiced concerns that directed marketing needed “constructive publicity toward emphasizing the rights of the individual” to address citizens’ civil liberties concerns (Department of Health Education and Welfare, Section IV, A Note on Mailing Lists, para. 9, 1973). In particular, the HEW report (Department of Health Education and Welfare, 1973) was concerned that citizens had little control over their private information was being used.

In many ways, the current discussion surrounding ethical principles for behavioral advertising mirrors the previous discussion regarding directed marketing. Just as directed marketing was more effective than random mass mailings, behavioral advertising is more effective than contextual or static online advertising. Randall Rothenberg, President and CEO of the Interactive Advertising Bureau, testified before the U.S. House Small Business Committee’s Subcommittee on Regulations, Healthcare, and Trade that web-based advertising provides a significant improvement in effectiveness over traditional directed marketing because the interactive environment promotes an “ongoing, two-way engagement among consumers, their media, and the advertising” and “generates data on consumer interests, needs, and consumption patterns that makes advertising effectiveness far easier to measure” (Rothenberg, 2008). Although the technology has changed, the ethical questions remain strikingly similar: What consumer information should advertisers be allowed to collect and how should they collect it? What levels of notice, control, and access should consumers have? This history of market research ethics should not be ignored.
Legal Ethics

Whereas ethics is the study of moral values, the law is a codification of rules describing the particular values society desires to uphold and enforce. In the United States, the FTC is an independent government organization tasked with consumer protection. To protect consumer privacy, the FTC supports five principles, called the Fair Information Practice Principles. These principles are as follows: (1) Notice / Awareness, (2) Choice / Consent, (3) Access / Participation, (4) Integrity / Security, and (5) Enforcement / Redress. The first principle, Notice / Awareness, matches well with Tybout and Zaltman’s (1974) “Right to be Informed” for market research subjects. The second principle, Choice / Consent, matches well with Tybout and Zaltman’s (1974) “Right to Choose” for market research subjects. The fourth principle, Integrity / Security, matches well with Tybout and Zaltman’s (1974) “Right to Safety” for market research subjects. The similarities between the Fair Information Practice Principles and consumer rights described by Tybout and Zaltman are examples of the FTC codifying ethical values.

The Federal Trade Commission (2000a, 2000b) first examined online profiling by holding a November 1999 workshop with network advertising companies. The Network Advertising Initiative (NAI), which was formed by several of these advertising companies, created self-regulatory principles for online profiling which the FTC (2000a, 2000b) supported. Continued public concern over behavioral advertising led the FTC (2007) to hold a November 2007 Town Hall workshop on behavioral advertising technologies. This workshop sought to develop guidelines for self-regulation of the industry (Federal Trade Commission, 2007).

In December of 2007, the FTC released its proposed self-regulatory principles for behavioral advertising, and requested additional comments to be submitted by following April. The next year the NAI (2008) revised their self-regulatory principles to ensure that “notice, choice, use limitation, access, reliability and security” (p. 3) were maintained. The FTC’s four final self-regulatory principles were released in February 2009 and focus on (1) transparency and consumer control, (2) reasonable security and limited data retention for consumer data, (3) affirmative express consumer consent to material changes in existing policy, and (4) affirmative express consumer consent to the use of sensitive data for behavioral advertising (Federal Trade Commission, 2009). Key industry advertising and consumer protection groups, including the Internet Advertising Bureau, the Direct Marketing Association, and the Council of Better Business Bureaus, expanded on the FTC’s principles to seven “Self-Regulatory Principles for Online Behavioral Advertising” (2009): consumer education, consumer control, transparency in the collection and use of data, security, consumer consent for material changes in policy, sensitive data handling, and accountability.

Despite the history of active participation from the government and many advertising companies, many scholars believe that self-regulation is not the answer. Chris Hoofnagle (2005), writing on behalf of the Electronic Privacy Information Center (EPIC), believes that privacy self-regulation principles still leave consumer privacy vulnerable and fail to educate consumers of the potential threats to their privacy. For example, Hoofnagle (2005) points out that opt-out policies are burdensome for consumers. Hoofnagle (2005) states that market forces have been “eroding both practices and expectations” (p. 15) regarding privacy and recommends that the FTC “abandon its faith in self-regulation” (p. 15). Other public interest organizations have taken a more moderate approach. For example, in 2008 the Center for Democracy and Technology (CDT) supported progress in self-regulation of privacy when responding to the NAI’s 2008 principles, but also noted seven areas needing improvement. For example, the
Behavioral Advertising Ethics

CDT (2008) also takes issue with the use of opt-out choice mechanisms. More broadly, the CDT (2008) recommends independent third-party audits to ensure compliance to self-regulatory principles and foster accountability.

By May 2008, Charter Communications had partnered with a behavioral advertising company called NebuAd to run a pilot program using a new technology called DPI. Representatives Barton (R-TX) and Markey (D-MA) sent a letter to Charter Communications asking them to put the behavioral advertising pilot program on hold until the privacy concerns could be discussed (Barton and Markey, 2008). In July 2008, Representatives Dingell (D-MI), Barton, and Markey sent a letter to Embark CEO Tom Gerke seeking further information about a behavioral advertising technology test conducted in conjunction with NebuAd (Barton, Dingell, and Markey, 2008). Charter Communications is the third-largest cable operator in the U.S., and Embarq is the fourth-largest telephone carrier.

Eventually, both the U.S. Senate and House of Representatives decided to hold hearings to discuss the ownership of online behavior information, the legality of DPI itself, and Internet users’ privacy concerns with comprehensive behavioral tracking. These hearings included testimony from Microsoft, Google, Facebook, the FTC, the Center for Democracy and Technology, and the Competitive Enterprise Institute (Privacy Implications, 2008; What Your Broadband Providers, 2008). Neither the Senate Committee hearings nor the House Committee hearings provided conclusive solutions to these concerns, but both committees promised to investigate the issue further.

Although neither the Senate Committee hearings nor the House Committee hearings provided conclusive answers to the questions raised, the advertising industry responded with significant changes. The CEOs of NebuAd and Adzilla, the two largest behavioral advertising companies in the United States, resigned from their positions under this extreme level of scrutiny (Hansell, 2008; Keane, 2008). Both NebuAd and Adzilla eventually closed their doors entirely leaving the U.S. without a DPI-based behavioral advertising business (Austin, 2009; Hansell, 2008; Keane, 2008). The largest remaining network-based behavioral advertising company in the world is Phorm, which operates in conjunction with British Telecom in the United Kingdom, but the European Commission is suing them for violations of European Union data protection laws (Wray, 2009). Google recently announced a web-based behavioral advertising service, but its impact remains to be seen (Helft, 2009).

Internet service providers are the only companies that are positioned to implement ISP-based behavioral advertising. As Paul Ohm points out, “Everything we say, hear, read, and do on the Internet passes first through their computers. If ISPs wanted, they could store it all, compiling a perfect transcript of our online lives” (Ohm, p. 1, 2009). Their position in the network puts ISPs in a unique and powerful position, but it does not put them beyond legislation and regulation.

Although Ohm’s statement is theoretically true, Ohm also points out one practical problem that is important to the technology behind DPI. Compiling a perfect transcript of an individual’s Internet use might be possible, but given the sheer amount of data that passes through an ISP’s customer-facing routers, it would be technically infeasible to record all of this data in an easily accessible format. Normal routing of Internet traffic involves viewing the packet header to get routing information and not at the payload. No recording of information is necessary to deliver the packet. The construction of a complete profile of an individual’s online behavior would require viewing and recording much larger amounts of data than contained in the packet header.

Ohm points out that Federal and State wiretapping laws, such as the federal Electronic Communications Privacy Act (ECPA), regulate packet-level surveillance, and it is possible that network-based behavioral advertising violates these laws (Ohm, 2009). The ECPA amended the
Behavioral Advertising Ethics

federal law protecting the privacy of telephone conversations. Although the ECPA is perhaps better known for its protections of stored electronic communications, like emails stored by an ISP, these stored protections are much weaker than the protections provided to active communications, like packets sent while web surfing. Because DPI techniques inspect active communications, Ohm (2009) believes a strong case could be made that these techniques are already illegal.

The construction of complete end user profiles has been defended in some contexts as ‘reasonable network management.’ In particular, the United States Federal Trade Commission, which regulates ISPs’ business practices, justified the use of DPI techniques as ‘reasonable network management’ because many ISPs use DPI to drop spam, viruses, and other malware. The legal ethics of this situation can be understood by the context of the situation. If a value-free technology can be used in one context (e.g. network security) as justifiably reasonable, nothing prevents the use of that same technology from being unethical in another context (e.g. marketing).

Nissenbaum (2004) discussed the importance of context to privacy law as an attempt to justify privacy as independent of property law. Privacy law and property law are historically intertwined because each is tied to the societal understanding of public and private contexts. Nissenbaum (2004) describes information as another context in which privacy laws apply. She outlines a framework, called “contextual integrity,” that can be used to understand information privacy in spaces that would traditionally be considered public (Nissenbaum, 2004). In this framework, the distinction between public and private is made based on the context in which it is used rather than whether it is public or private, or even if it is gathered publically or privately (Nissenbaum, 2004). Using contextual integrity, Nissenbaum (2004, pp. 152-153) examines the privacy concerns involved in consumer profiling:

In the past, it was integral to the transaction between a merchant and a customer that the merchant would get to know what a customer purchased. Good—that is to say, competent—merchants, paying attention to what customers wanted, would provide stock accordingly. Although the online bookseller Amazon.com maintains and analyzes customer records electronically, using this information as a basis for marketing to those same customers seems not to be a significant departure from entrenched norms of appropriateness and flow. By contrast, the grocer who bombards shoppers with questions about other lifestyle choices—e.g., where they vacationed, what movies they recently viewed, what books they read, where their children attend school or college, and so on—does breach norms of appropriateness. The grocer who provides information about grocery purchases to vendors of magazine subscriptions or information brokers like Seisint and Axciom is responsible not only for breaches of norms of appropriateness but also norms of flow.

Nissenbaum’s concept (2004) has already impacted the development of information systems. Barth, Datta, and Mitchell (2006) examined the use of contextual integrity to construct a framework for reasoning about access control and privacy policy frameworks. They validated their contextual integrity framework against information systems that must comply with laws and regulations (Barth, Datta, & Mitchell, 2006). Specifically, they evaluate information systems for compliance with the Health Insurance Portability and Accountability Act, the Children’s Online Privacy Protection Act, and the Gramm-Leach-Bliley Act (Barth, Datta, & Mitchell, 2006). Although the contextual integrity framework may be limited to information systems, it certainly appears promising for use in analyzing the legal aspects of DPI.

Many unanswered legal questions about behavioral advertising remain. Congressional hearings have not yet conclusively determined whether behavioral advertising is in the public’s
best interest. The recent FTC self-regulatory rules have not yet impacted the industry, and scholars such as Hoofnagle do not believe they will. No conclusive case law exists that would clarify if DPI is a violation of existing wiretapping laws. Lawyers and lawmakers have not yet clearly defined the contexts for online privacy.

**FUTURE RESEARCH DIRECTIONS**

Behavioral advertising has the potential to improve sales and the consumer experience significantly, but it is still an under-researched area (Yan et al., 2009). Web-based behavioral advertising requires better control mechanisms for web bugs and LSOs. In particular, researchers should determine how to design a browser such that could provide end users the ability to set preference options to block web bugs and LSOs. Researchers also need to address the conflicts between opt-in and opt-out cookies. One promising solution may be recent browser extensions, such as the Targeted Advertising Cookie Opt-out (TACO) extension\(^\text{10}\), that automatically restore opt-out cookies.

The most important area for future research in network-based behavioral advertising is the question of end user control over whether their Internet traffic is being monitored through DPI. Perhaps it is possible to provide users a technological solution that would allow them to control DPI. Finally, users could pursue a legal solution by pushing for new state or federal laws banning the use of DPI technologies by ISPs.

Focus is also needed on ways to provide end users choice regarding subjects that can be tracked. Providing a finer granularity of control would enable end users the ability to allow their ISP to build behavioral profiles regarding only certain types of marketing (e.g. furniture) while preventing more sensitive types of marketing (e.g. healthcare prescriptions). Although this level of control is more complex, if implemented on a per individual basis, it may provide a generic solution for communities that share relatively uniform norms of privacy. For example, this is the approach taken by Phorm to comply with the privacy norms of the United Kingdom.

Consumer notice and consumer education are a critical areas of future research needed to solve some of the ethical concerns of DPI technologies. If an ISP is profiling their customers, a control-based definition of privacy as the ethical standard calls for clear notification regarding what is being collected about them, how it is being collected, and what mechanisms they can use to control this process. Furthermore, consumers should be able to view, amend, or correct errors in these profiles. Providing these controls and assisting users in exercising them preserves end user privacy while allowing ISPs to make use of their valuable position in the Internet topography.

The effects of third party doctrine are another important area for future research. Third party doctrine is a legal interpretation of the Fourth Amendment of the U.S. Constitution, which protects citizens against unreasonable searches and seizures by the government. Third party doctrine states that individuals sharing information with third parties cannot make a Fourth Amendment claim of protection on that information. The ethics of third party doctrine extend beyond behavioral advertising, but under third party doctrine citizens could not use the Fourth Amendment to protect information shared with advertising companies using behavioral advertising technologies.

Finally, future research should also consider the effects of behavioral advertising on other civil liberties. For example, behavioral advertising technologies could be used as tools of discrimination because they can profile based on cultural or racial subjects. Similarly, if these technologies are used to profile religious subject matter, then there may be effects on freedom of religion. Behavioral advertising may also have a chilling effect on free speech because consumers may change the way they communicate when they know they are being profiled.
CONCLUSION

In this chapter we have discussed the ethics of behavioral advertising as they relate to consumer expectations of civil liberties, especially privacy. We began by describing behavioral advertising technologies and comparing them with earlier forms of advertising. Next, we then discussed previous market research ethics that provide insights into this ethical debate. Finally, we discussed the role of laws and regulations as a societal expression of ethically acceptable practices.

Although there are many difficult ethical questions about behavioral advertising, the role that advertising plays is incredibly important both in the economics of the Internet and more broadly in capitalist society. Advertising fueled the explosive growth of the Internet. Many products and services are offered free of charge to the end user. The company that provides the service makes money through advertisements included in these products and services. In addition, the cost of advertising is the overhead of matching consumers with producers in a capitalist economy. The lower this cost is, the more efficiently a capitalist economy performs. When consumers are able to find new and interesting products more easily while feeling confident about their privacy and producers are able to sell to everyone that truly wants their products, all players in the market win. There are real benefits to effective targeted online advertisements, but we must adequately address the ethical issues surrounding behavioral advertising.

REFERENCES


Behavioral Advertising Ethics


KEY TERMS AND DEFINITIONS

Behavioral Advertising: A method for targeting advertising to individuals based on their actions.

Behavioral Profile: A profile of an individual’s actions, interests, and demographics that can be used to tailor advertisements.

Cookie: A small file stored on a computer, or other web-browsing device, that can be used to identify returning users or store web browsing session information such as items stored in an online shopping cart.

Deep Packet Inspection (DPI): Any method of Internet routing or network management that involves using information in the packet payload instead of or in addition to the information in the packet header.

Local Shared Object (LSO): A small piece of information stored on a machine through Adobe Flash Player that can be used to identify a returning user or store web browsing session information such as the score on a flash-based game.

Web Bug: An image file loaded included on a web page or in an email for the sole purpose of tracking who loaded it and when it was loaded.

Typically, web bugs are 1 pixel by 1 pixel transparent images.

ENDNOTES

1 Yan et al. refer to behavioral advertising as behavioral targeting.
2 The Click-Through Rate (CTR) commonly measures Internet advertising effectiveness; it is calculated as the number of times an ad is clicked compared to the number of times it is shown.
4 http://adblockplus.org/
5 http://noscript.net/
7 http://kb2.adobe.com/cps/526/52697ee8.html
8 http://objection.mozdev.org/
9 It is worth noting that some scholars would disagree with this statement and claim that ethical value is embedded during the design
APPENDIX: DISCUSSION QUESTIONS

1. Is opt-in or opt-out a more ethical default for cookies?
2. How can browsers support both opt-in and opt-out defaults when deleting cookies?
3. Should third-party cookies be treated differently than first-party cookies?
4. What is an ethical duration for the validity of cookies?
5. Would a more transparent standard for cookies improve user privacy? If so, how?
6. Do transparent web bugs violate notice/awareness?
7. Is the use of an image as a web bug a violation of the original purpose for which it was designed?
8. Web bugs are difficult to block, but they can only provide limited information. Does this make web bugs more or less fair than cookies?
9. Does the use of web bugs by spammers de-legitimize the use of web bugs by traditional advertisers?
10. How can an ISP provide customers notice regarding the use of DPI?
11. How can an ISP provide customers a choice regarding the use of DPI?
12. What types of information should be collected and used to generate profiles? How long should organizations keep this information?
13. Is it ethical to use DPI to detect and drop packets that contain viruses? In what ways is this different than advertising?
14. Cookies and DPI were originally developed for non-advertising purposes, but they have been found to be useful for advertising. Is it ethical to use technologies for a secondary purpose (i.e. for something that these technologies weren’t originally designed to do)?
15. Should the companies be required to inform each consumer of the actual information they have and how they are using it?
   a. Would this solution scale knowing the large amount of notification data that would be sent to users?
   b. Is there an increased risk of identity theft by sending this information out?
   c. If so, is this an ethical issue?
16. Is it ethical that your information be collected without your knowledge and permission?
17. Who are the stakeholders’ (individuals, corporations, and communities) in the discussion of behavioral advertising? Put yourself in the shoes of each stakeholder and describe your interests.
18. Should behavioral advertising be regulated? If so, how and by whom (self-regulation, standards, states, federal government)?
19. Consider what happens if some unintended entity were to acquire and sell behavioral advertising data? Who would be victims and why?
   a. Does this suggest that regulations, controls and policies and penalties be mandated? On whom and by whom?
20. Suggest a way of doing behavioral advertising without violating ethical principles?
21. Is DPI ethical?
   a. Should there be another way for ISPs to collect information without DPI?
22. Should Behavioral Advertising/DPI be limited to a subset of some user group or markets?
23. Is it ever ethical for a firm in a market relationship with a consumer to deceive the consumer?