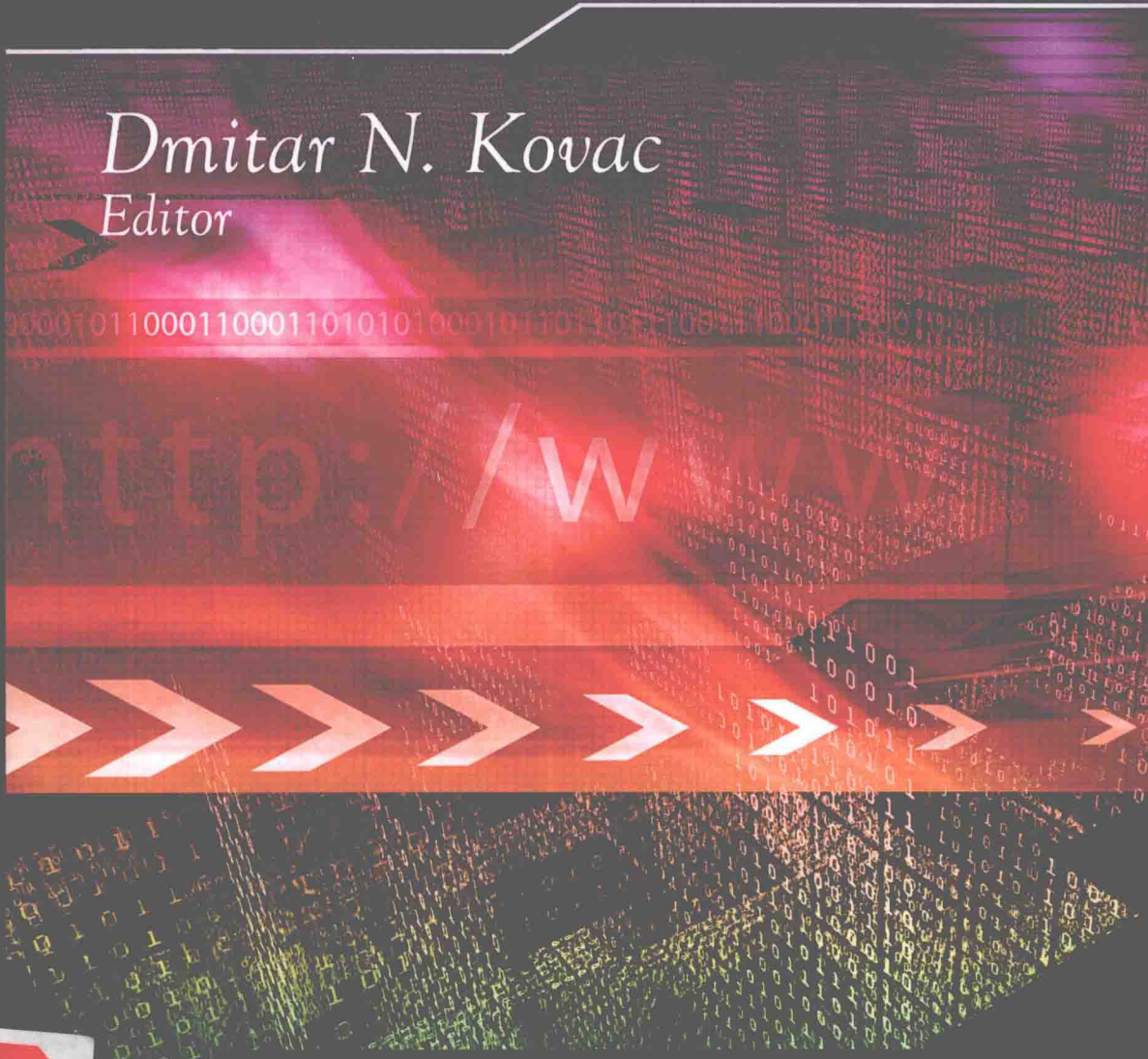
ELECTRONIC BREADCRUMBS

Issues in Tracking Consumers



Dmitar N. Kovac
Editor

Business Issues, Competition and Entrepreneurship Series

NOVA

ELECTRONIC BREADCRUMBS: ISSUES IN TRACKING CONSUMERS

DMITAR N. KOVAC
EDITOR

Nova Science Publishers, Inc.
New York

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA
Electronic breadcrumbs : issues in tracking consumers / editor, Dmitar N. Kovac.
p. cm.
Includes index.
ISBN 978-1-60741-600-5 (hardcover)
1. Data protection--Law and legislation--United States. 2. Web usage mining--United States. 3. Internet advertising--Law and legislation--United States. I. Kovac, Dmitar N.
KF1263.C65A2 2009
342.7308'58--dc22

2009032472

Published by Nova Science Publishers, Inc. ✦ New York

PREFACE

This book looks at the issue of "behavioral marketing" which involves the tracking of consumers' online activities in order to deliver tailored advertising. The digital information age, against a backdrop of rising globalization, allows anyone to collect and share information on any subject, corporation, government - or in many cases, other individuals. Companies from retailers to search engines to software makers all collect consumer data - enough to fill vast server warehouses. Of-course, websites have long collected and marketed information about visitors. The latest twist is that behavioral marketing firms "watch" our clickstreams to develop profiles or inform categories to better target future advertisements. Unarguably beneficial, the process however stokes privacy concerns. Thus this book also discusses the Federal Trade Commission's examination of online privacy issues.

This is an edited, excerpted and augmented edition of various government publications.

CONTENTS

In: Electronic Breadcrumbs: Issues in Tracking Consumers ISBN: 978-1-60741-600-5
Editor: Dmitar N. Kovac

Chapter 1

BROADBAND PROVIDERS & CONSUMER PRIVACY HEARING- ATTWOOD TESTIMONY

Dorothy Attwood

Thank you, Chairman Inouye and Ranking Member Hutchison, for providing AT&T Inc. the opportunity to discuss online advertising and, more specifically, the issue that has received a good deal of recent attention, so-called online behavioral advertising. We trust that this hearing will help the discussion evolve past slogans and rhetoric to a more thoughtful examination of the facts and the development of a holistic consumer privacy policy framework that all participants in the online behavioral advertising sphere can and will adopt.

Your interest in these matters surely is warranted. Online advertising fuels investment and innovation across a wide range of Internet activities, and provides the revenue that enables consumers to enjoy many free and discounted services. Likewise, website publishers make most of their money from advertising, which revenue in turn funds today's vast wealth and diversity of Internet content and information — most of which consumers enjoy, again, for free. On the other hand, online advertising, especially next-generation forms of highly targeted behavioral advertising that involve tracking consumer web browsing and search activities, raise important consumer-privacy concerns that policymakers and industry must carefully weigh. In short, setting proper policy in this area will be crucial to a healthy and growing Internet ecosystem that benefits consumers.

AT&T does not today engage in online behavioral advertising, but we understand the uniquely sensitive nature of this practice. We have listened to our customers and watched the debate unfold, and are responding by advocating for a consumer-focused framework. As described in more detail herein, the pillars of this framework — *transparency, consumer control, privacy protection, and consumer value* — can be the foundation of a consistent regime applicable to all players in the online behavioral advertising sphere — including not just Internet Service Providers ("ISPs"), but also search engines and third party advertising networks — that both ensures that consumers have ultimate control over the use of their personal information and guards against privacy abuses.[1]

In particular, we believe that effective customer control for online behavioral advertising requires meaningful consent and therefore commit that *AT&T will not use consumer information for online behavioral advertising without an affirmative, advance action by the consumer that is based on a clear explanation of how the consumer's action will affect the use of her information.* This concept — often generically referred to as "opt-in" — means that a consumer's failure to act will *not* result in any collection and use by default of that consumer's information for online behavioral advertising purposes. This affirmative consent model differs materially from the default-based privacy policies that advertising networks and search engines — which already are engaged in online behavioral advertising — currently employ. Given the obvious consumer benefits of such a model, we encourage all companies that engage in online behavioral advertising — regardless of the nature of their business models or the technologies they utilize — likewise to adopt this affirmative-advance-consent paradigm.

WHAT IS ONLINE BEHAVIORAL ADVERTISING?

There is no single, settled definition of online behavioral advertising in statute or case law, but the FTC and others have used the term to refer to it as the tracking of a consumer's web search and web browsing activities — by tracking either the person or a particular Internet access device, be it a computer, data-enabled mobile phone, or some other communications vehicle — to create a distinct profile of the consumer's online behavior. In this sense, it can clearly be distinguished from the simple practice of tracking a consumer's use of an individual website or obviously- related websites (such as those operated under a common trademark, trade name or conspicuously disclosed corporate affiliation), which practice does not necessarily raise the same privacy concerns as online behavioral advertising but which nonetheless can and should expressly be disclosed to Internet users. Privacy concerns about online behavioral advertising are not new — indeed, DoubleClick's (now a Google subsidiary) use of tracking cookies to collect and use information about consumer web browsing activity was the subject of an FTC proceeding in 2000.[2] More recently, the FTC and Congress have appropriately asked questions about the privacy implications of emerging online advertising businesses that involve the tracking of consumer web browsing and search activity. Thus, consistent with the focus of recent public discussion, we consider online behavioral advertising to be (1) the tracking of user web browsing and search activity across unrelated websites, (2) when the tracking and association of the websites or their components are largely invisible to the user, and (3) the resulting information is used to create a distinct user profile and deliver targeted advertising content.

Online behavioral advertising can take many forms. It can, for instance, involve the use by an ISP of technologies to capture and analyze a user's Internet browsing activities and experience across unrelated websites. These more ISP-specific methodologies are not, however, the only — and certainly are not nearly the most prevalent — forms of online behavioral advertising. Advertising-network technologies have evolved beyond solely tracking consumer web surfing activity at sites on which they sell advertising. They now also have the ability to observe a user's entire web browsing experience at a granular level. Techniques include the ad network "dropping" third-party tracking "cookies" on a consumer's computer to capture consumer visits to any one of thousands of unrelated websites;

embedding software on PCs; or automatically downloading applications that — unbeknownst to the consumer — log the consumer's full session of browsing activity.

Ad networks and other non-ISPs employ these capabilities at the individual browser or computer level and they are as effective as any technique that an ISP might employ at creating specific customer profiles and enabling highly targeted advertising. Already ad networks and search engines track and store a vast trove of data about consumers' online activities. Google's practices exemplify the already extensive use of online behavior advertising, particularly by nonISPs. Google logs and stores user's search requests, can track the search activity by IP address and a cookie that identifies the user's unique browser, and can even correlate search activities across multiple sessions, leading to the creation of a distinct and detailed user profile. Through DoubleClick, Google can drop tracking cookies on consumers' computers so that whenever the consumer visits web sites that contain a display ad placed by DoubleClick (which can be for virtually any product or service), the consumer's web browsing activity can be tracked across seemingly unrelated sites (e.g., CNN.com or ESPN.com). Google further has access to enormous amounts of personal information from its registered users, which its privacy policy expressly confirms can be combined with information from other Google services or third parties for the "display of customized content and advertising." And it even scans emails from nonGmail subscribers sent to Gmail subscribers for contextual advertising purposes.

Thus, if anything, the largely invisible practices of ad-networks and search engines raise at least the same privacy concerns as do the online behavioral advertising techniques that ISPs could employ, such as deep-packet-inspection, which have application beyond mere targeted advertising, including managing network congestion, detecting viruses and combating child pornography. In short, the privacy and other policy issues surrounding online behavioral advertising are not technology-specific. The relevant touchstones are the manner in which consumer information is tracked and used, and the manner in which consumers are given notice of and are able to consent to or prohibit such practices. Those factors are entirely technology- neutral.

AT&T'S APPROACH TO ONLINE BEHAVIORAL ADVERTISING

AT&T does not today engage in online behavioral advertising.[3] This is not because AT&T sees no value in this next-generation form of online advertising. Indeed, if done properly, online behavioral advertising could prove quite valuable to consumers and could dramatically improve their online experiences. We do, however, believe it is essential to include strong privacy protections in the design of any online behavioral advertising program, which is why we will initiate such a program only after testing and validating the various technologies and only after establishing clear and consistent methods and procedures to ensure the protection of, and ultimate consumer control over, consumer information. We further intend to work with privacy advocates, consumer privacy coalitions and fellow industry participants in a cooperative, multifaceted effort that we trust can and will lead to a predictable consumer driven framework in this area. In any event, if AT&T deploys these technologies and processes, it will do so the right way.

Against this backdrop, AT&T has already listened closely to its customers and will adopt meaningful and flexible privacy principles that will guide any effort to engage in online behavioral advertising. We summarize this framework as follows:

- ***Transparency:*** Consumers must have full and complete notice of what information will be collected, how it will be used, and how it will be protected.
- ***Consumer Control:*** Consumers must have easily understood tools that will allow them to exercise meaningful consent, which should be a sacrosanct precondition to tracking online activities to be used for online behavioral advertising.
- ***Privacy protection:*** The privacy of consumers/users and their personal information will be vigorously protected, and we will deploy technology to guard against unauthorized access to personally identifiable information
- ***Consumer Value:*** The consumer benefits of an online behavioral advertising program include the ability to receive a differentiated, secure Internet experience that provides consumers with customized Internet advertisements that are relevant to their interests. But we think the future is about much more than just customized advertising. Consumers have shown that in a world of almost limitless choices in the content and services available on the Internet, they see great value in being able to customize their unique online experience. That is the ultimate promise of the technological advances that are emerging in the market today.

CALL TO ACTION

We believe these principles offer a rational approach to protecting consumer privacy while allowing the market for Internet advertising and its related products and services to grow. But, in order for consumers truly to be in control of their information, *all* entities involved in Internet advertising, including ad networks, search engines and ISPs, will need to adhere to a consistent set of principles. A policy regime that applies only to one set of actors will arbitrarily favor one business model or technology over another and, more importantly, represent only a partial and entirely unpredictable solution for consumers. After all, consumers do not want information and control with respect to just a subset of potential online advertising or the tracking and targeting that might underlie those ads. Thus, we urge all entities that engage in online behavioral advertising — including especially those who already engage in the practice — to join AT&T in committing to a policy of advance, affirmative consumer consent.

END NOTES

[1] The policy framework that AT&T proposes here is informed by and should complement the Online Behavioral Advertising Self-Regulatory Principles issued by staff of the Federal Trade Commission in December of last year. Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, available at http://www.ftc.gov/05/2007/12/P85900stmt.pdf.

[2] Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, Bureau of Consumer Protection, Federal Trade Commission, to ChristineVarney, Hogan & Hartson, Re: DoubleClick Inc. (Jan 22, 2001)(memorializing closure of FTC staff investigation).

[3] AT&T does engage in some of the more ordinary and established aspects of online advertising. Like virtually every entity with a retail Internet presence, AT&T tracks usage on its own websites, such as att.com, in order to improve the online experience, optimize a particular site's capabilities and ease-of-use, and provide the most useful information to consumers about AT&T's products and services. In addition, like thousands of other businesses that operate websites, AT&T does business with advertising networks and has partnered with providers of online search. For example, on the AT&T broadband Internet access portal, AT&T makes space available for advertising provided by the Yahoo! advertising network, and users of the portal may be shown advertising that is based on their activity across sites signed up to the Yahoo! advertising network. Also by way of example, we have arranged for the Google search box to appear on our my.att.net site. In this regard, then, we are no different than any other website publisher.

In: Electronic Breadcrumbs: Issues in Tracking Consumers ISBN: 978-1-60741-600-5
Editor: Dmitar N. Kovac

Chapter 2

BROADBAND PROVIDERS & CONSUMER PRIVACY HEARING- SOHN TESTIMONY

Gigi B. Sohn

Chairman Inouye, Ranking Member Hutchison and Members of the Committee, thank you for giving me the opportunity to testify about broadband providers and consumer privacy. I'd like to focus today on the growing use of the collection of technologies known as "Deep Packet Inspection," or DPI, which has immense implications for the privacy rights of the American public. Over the past several months, Public Knowledge, in partnership with Free Press, has been analyzing these technologies and their impact on privacy and an open Internet. In June, our organizations published a white paper entitled *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking*, which examined the technical and policy aspects of DPI. I applaud the Committee for its continued scrutiny of the use of these technologies.[1]

I. INTRODUCTION

Today's hearing on consumer privacy comes in the wake of two high-profile online consumer privacy violations, both of which involved the use of Deep Packet Inspection (DPI) technology on an Internet Service Provider's (ISP) network.

The first instance came to light in October 2007, when an Associated Press report revealed that Comcast was interfering with its customers' BitTorrent traffic.[2] The report confirmed earlier tests conducted by independent network researcher Robb Topolski, who found that Comcast was analyzing its user's web traffic in order to determine the types of applications and protocols being used. The company then used a technique called "packet spoofing" to delay, degrade and in some cases, block traffic that was identified as being used for BitTorrent, a popular peer-to-peer file sharing protocol. Public Knowledge and Free Press filed a formal complaint with the FCC in November 2007, calling for the Commission to open a formal investigation into the ISP's practices.[3]

In January 2008, the FCC announced that it had opened a formal investigation into Comcast's blocking of BitTorrent traffic. This investigation concluded in August 2008 with the FCC upholding the Public Knowledge and Free Press complaint and reprimanding Comcast for its degradation of its user's traffic. In its ruling against Comcast,[4] the FCC ordered the company to stop blocking BitTorrent traffic and to develop a new set of network management practices that did not violate the FCC's Broadband Policy Statement.[5] In its letter of response to the FCC, Comcast confirmed that it had used DPI equipment from the Sandvine Corporation in order to identify and block BitTorrent traffic.[6]

The second instance surfaced in May 2008, when it was revealed that various regional ISPs had contracted with NebuAd, a company that provided highly targeted behavioral advertising solutions using DPI equipment. In test deployments of this technology, all of the traffic traveling over an ISP's network was routed through a DPI appliance which collected data on specific users, including web sites visited, terms searched for and services and applications used. This data was then sent to NebuAd, which in turn, used the data to create detailed user profiles. These profiles were used to display highly targeted advertisements, which were dynamically displayed to the user as he or she surfed the Web.

In May 2008, Representatives Edward Markey (Chairman, Subcommittee on Telecommunications and the Internet) and Joe Barton (Ranking Member, Senate Committee on Energy and Commerce) sent a letter to NebuAd[7],asking the company to put its pilot tests on hold, pending an investigation into the company's practices. A coalition of 15 consumer advocacy and privacy groups publicly voiced their support for this letter and urged the Congressmen to continue their investigation of NebuAd and other behavioral advertising companies.[8] In June 2008, Public Knowledge and Free Press released a technical analysis of NebuAd's behavioral advertising system, authored by networking researcher Robb Topolski.[9] The report revealed that NebuAd and its partner ISPs repeatedly violated the privacy of users, with little or no notification that DPI equipment was being used. Following the release of the report, the House Committee on Energy and Commerce convened a hearing on the topic of DPI, wherein NebuAd CEO Bob Dykes was asked to testify.

On August 1, 2008, the House Committee on Energy and Commerce followed up with a letter to 33 ISPs and software companies asking for details regarding how they were using DPI and whether and how they were disclosing those uses to their customers.[10] As a result of the Congressional scrutiny, all of NebuAd's ISP partners, including WOW! (Wide Open West), CenturyTel, Charter, Bresnan and Embarq, have decided to put a hold on their test deployments with NebuAd. In September 2008, Bob Dykes announced that he was leaving NebuAd and following his departure, the company announced that it was abandoning its behavioral advertising initiatives, in favor or more traditional advertising technologies.

II. Deep Packet Inspection

To put it simply, Deep Packet Inspection is the Internet equivalent of the postal service reading your mail. They might be reading your mail for any number of reasons, but the fact remains that your mail is being read by the people whose job it is to deliver it.

When you use the Internet for Web browsing, email or any other purpose, the data you send and receive is broken up into small chunks called "packets." These packets are wrapped

in envelopes, which, much like paper envelopes, contain addresses for both the sender and the receiver–though they contain little information about what's inside. Until recently, when you handed that envelope to your ISP, the ISP simply read the address, figured out where to send the envelope in order to get it to its destination, and handed it off to the proper mail carrier.

Now, we understand that more and more ISPs are opening these envelopes, reading their contents, and keeping or using varying amounts of information about the communications inside for their own purposes. In some cases, ISPs are actually passing copies of the envelopes on to third parties who do the actual reading and use. In others, ISPs are using the contents to change the normal ways that the Internet works. And for the most part, customers are not aware that their ISPs are engaging in this behavior–much like if the postal service were to open your letter, photocopy it, hand that copy to a third party and then re-seal the letter, so that you would never know it had even been opened in the first place.

III. The Privacy Implications of DPI

It should be clear that the very nature of DPI technology raises grave privacy concerns. An ISP, by necessity, sees every piece of data a user sends or receives on the Internet. In the past, ISPs had little incentive to look at this information and the related privacy concerns provided a strong deterrent against doing so. However, now that technology is widely available to make use of and monetize this information, companies are exploring the limits of what they can do permissibly.

When evaluating an implementation of DPI technology, there are three basic questions that must be answered in order to assess both the impact on a user's privacy and acceptability of use of the technology in question:

Purpose: What purpose is the collected data being used for?
Collection: How is the data collected and utilized?
Consent: How was affirmative informed consent obtained?

An understanding of these questions can inform legislators and policymakers in the formation of policies, which will adequately protect users of Internet connections and services. The uses for DPI are myriad, and most raise serious privacy concerns, but each use should be measured individually against a comprehensive privacy policy.

It is also important to note that there are two parties to any Internet communication. In almost all cases, the party on the other end of a user's line will have no meaningful ability at all to know what kind of monitoring is being employed by that user's ISP or what is being done with the collected data, and will have no opportunity at all to give or to deny consent. For example, if I send you an email and my ISP is using DPI to read the contents of my emails, your privacy has just been violated without your knowledge or consent. Any comprehensive privacy policy that addresses technologies like DPI must take into account not only the privacy rights of an ISP's customers, but also those of anyone who communicates with these customers.

A. Purpose

Given DPI's potential to be used as an intrusive tool, we must first ask why the user's traffic is being collected or analyzed at all. Is the use of DPI integral to the functioning of the network or is the technology simply being used to provide the ISP with an additional revenue stream? Does the technology in question primarily benefit the ISP's bottom line, or does it give direct benefits to the customer's use of the Internet? Is it used to protect users or the integrity of the network, or simply to offer new or improved additional services?

Not all uses of DPI are inherently problematic. The first widespread uses of DPI were for security purposes: to stop malicious programs like viruses and worms from passing from one infected computer to another over the Internet. However, as seen in the recent complaint and decision against Comcast at the Federal Communications Commission (FCC), DPI can also be used to engage in impermissible, discriminatory network management practices. Taken to an extreme, we can even imagine a future where DPI is used to record and disseminate every single move a user makes on the Internet–from Web browsing, email and instant messaging to VoIP phone calls and video chats–to the ISP's own business advantage.

Understanding the purpose of DPI use is the first step to understanding whether that use will violate a user's expectations of privacy.

B. Collection

After we understand the purpose of a particular use of DPI, we can analyze how the data is collected and used toward that purpose. Is the user's data being collected by the ISP for its own use, or is it being passed to a third party with no connection to the user? Is all of the user's data collected, or a smaller subset of the data? Is the amount collected narrowly tailored to achieve the stated purpose, or broader than necessary, or is the amount of data actually used smaller than that collected?

It is important to note here that we should evaluate both the amount of data which reaches the party using it, and the amount of that data which is used. This is because additional data that is sent to a third party provides more opportunity for abuse of user privacy – even if that third party later chose to discard some of the more personal information. For instance, even though companies like NebuAd may choose to ignore the personal medical records or emails of its partner's customers, they were provided the data to do exactly that. This problem is compounded by the fact that an ISP or partner must engage in DPI to even discover what type of data is being transmitted, thereby possibly violating the user's privacy before any decision is made regarding what is to be done with the data.

It is also necessary to identify the ways in which the collected data might be tied to the user's actual identity. Is the data obtained using DPI explicitly tied to data obtained through other means–for example, the ISP's billing information, demographic information, or personal information stored on a third-party website? Can the collected data be later aggregated with this type of information? Will the data itself contain personally identifying information (PII), such as names, addresses, and credit card information submitted to web sites? These questions are important because if the data in question contains PII or if it is later connected with other user data, the privacy implications are multiplied.

Implicit in the data collection question are also questions about data storage. Is the collected data kept by the party using it? If so, for how long? Is it kept in its original, complete form, or in some type of summary? Is any PII kept with the stored data?

Understanding what and how data is collected and how well that comports with the stated purpose of the collection is necessary to evaluating whether the collection will violate users' privacy expectations.

C. Consent

No inspection of a user's data will be acceptable without that user's affirmative, informed consent or law enforcement obligations. To ensure this is obtained, we must evaluate both how users are notified of the ways in which their ISP and its partners intend to use DPI, and the method by which those users affirmatively consent (or decline to consent) to those uses. To do this, we must ensure that before a user's data is inspected, the user actually receives complete, useful information, and that the user knowingly and affirmatively assents to the stated uses.

Are the answers to the above questions about purpose and collection accessible for users, and complete in the information they divulge? If any third parties are involved in the monitoring, are their identities provided for the user? Are the answers written so that the average user can make sense of them? Are the policies in question detailed in a place and manner that ensures that the user is likely to read them? Is the user actively notified of the presence of and changes to policies and monitoring activities, or are changes made to Web pages and written into the Terms of Service–without any notification to the user? Without accurate and easily understandable information that a user is actually aware of, that user cannot make informed choices about how best to manage his or her privacy online.

Finally, what is the process by which users agree (or decline to agree) to the use of these technologies? Are they subject to DPI *before* they receive meaningful notice of its use, or is the user required to take an affirmative action before his or her data is recorded or analyzed? Is the information and the action specific to the monitoring activities, or is it hidden in a larger "Acceptable Use Policy," "End User License Agreement," or other document? Does the user have the meaningful ability to change his or her choice later? Is the user actively offered a periodic chance to withdraw consent, or is he or she only asked once? And is the option not to consent a real one, without crippling or disabling of the user's service as the only alternative?

Without meaningful, informed, affirmative consent on the part of the user, personal data should not be used for any purpose that is not necessary to providing basic Internet service.

IV. ISP Disclosures

In response to Chairman Dingell and Ranking Member Barton's letter, 33 ISPs and software companies described whether and how they were using DPI and whether and how they were disclosing those uses to their customers.[11] These responses are helpful in understanding how, to date, the above three questions have been answered unsatisfactorily.