On Notice: The Trouble with Notice and Consent

Solon Barocas
Media, Culture, and Communication
New York University
New York, NY
solon@nyu.edu

Helen Nissenbaum
Media, Culture, and Communication & Computer Science
New York University
New York, NY
helen.nissenbaum@nyu.edu

Abstract— *This paper scrutinizes the use of 'notice and consent' to address privacy concerns in online behavioral advertising (OBA). It is part of a larger project with Dan Boneh, Arvind Narayanan, and Vincent Toubiana to evaluate the social, political, and ethical standing of OBA and to develop a system (PRIVADS) for privacy-preserving OBA. We develop a distinction between the ethical implications of the (1) tracking that is required to develop user profiles to be used in the (2) targeting of individual users with particular ads. We show how tracking and targeting present both distinct and overlapping ethical concerns and how existing mitigations tend to treat these concerns as one and the same, even when they seem to address different problems. Anonymization, for instance, attempts to defuse the privacy concerns of tracking by excluding 'personally identifiable' or 'sensitive' information, but offers little to quell concerns over targeting. On the other hand, policy solutions, particularly notice and consent, attempt to render participation a matter of choice, but generally fail to explain whether a user agrees or disagrees to tracking, targeting, or both. Moreover, we show how various types of complexity render current notice mechanisms practically and inherently insufficient. This is due to (1) the confusing disconnect between the privacy policies of online publishers and the tracking and targeting third parties with whom they contract, each of whom have their own privacy policies; (2) the fickle nature of privacy policies, which may change at any time, often with short notice, and (3) the ever-increasing number of players in the ad network and exchange space, resulting in flows of user data that are opaque to users. To the extent that meaningful notice remains illusory under such conditions, we conclude that even an opt-in regime would lack legitimacy.*

Keywords: Online Behavioral Advertising; Behavioral Targeting; Privacy; Notice and Consent

I. INTRODUCTION

In March 2009, Google announced that its AdSense service would introduce "interest-based advertising," drawing on users' browsing behaviors to target them with ads. For example, "if users [were to] visit a number of sports pages," AdSense would "add them to the 'sports enthusiast' interest category" [1]. Online behavioral advertising (OBA) relies on the systematic tracking of users across websites and over time in order to develop user profiles from which to infer interests and preferences. These interests and preferences are then used as the basis upon which to selectively target users with corresponding ads. Though it promises an improvement over more scattershot approaches to advertising, until now, Google had been reluctant to adopt the practice [2]. Indeed, Google arrived strikingly late to OBA. Because of its prominent position in the public imagination, Google seemed concerned that its entry into a field fraught with privacy concerns might attract unwanted attention. Theses worries now appear to have been justified: Google's entry has drawn far more scrutiny than its competitors' despite its introduction of a number of novel privacy mitigation mechanisms. Google may have hoped to learn from its competitors, but nonetheless finds itself a part of a debate that now involves privacy and consumer advocacy organizations, professional associations and trade groups, and domestic and foreign government agencies, not to mention the many OBA industry actors and web users themselves.

It is important to note that OBA has borne the brunt of what might actually be a wider debate about the monitoring of user activity online, and even more widely, the aggregation of personal information for a variety of purposes. Because OBA has a public face in the form of ads, it attracts more attention than the less obviously visible user tracking that is essential to the business of research and analytic companies and certain content delivery firms. That said, the outcome of OBA regulatory efforts could have profound consequences on what counts as legitimate practice in online monitoring and beyond.

Generally, the threat of federal regulation looms large, even though the Federal Trade Commission (FTC), which so far has adjudicated much of the domestic debate, continues to support self-regulation. The most recent FTC report, from February 2009, lays out a set of guiding principles [3], many of which have been incorporated by the Network Advertising Initiative (NAI), the industry's voluntary self-regulatory cooperative. These principles have been supplemented by a July 2009 document that lays out an overlapping and complimentary set of principles developed by a joint panel of industry associations [4]. These principles—and the debate, generally—focus of five main clusters of concern: (1) transparency, commonly understood as a form of meaningful notice concerning the collection and use of user data; (2) choice, by way of active or passive user consent; (3) control, which amounts to a more granular form of choice concerning the precise types of collection and use of data to which a user may agree, particularly as it applies to so-called 'sensitive data;' (4) security, in terms of data integrity and protection from misuse or misappropriation; and (5) regulatory institutional design, namely the structural conditions necessary to ensure enforcement and accountability. These are not mutually exclusive categories; at the intersection of transparency and control, for examples, sits Google's effort to make user profiles open to review and editable by the user. It is important to note that at the heart of these principles and efforts—setting aside security and institutional design, which are less particular to

OBA—resides a notion of notice that we wish to unpack in this paper. Insofar as consent and control logically follows notice, transparency remains the crux of these principles.

II. The Socio-Technical Practice of OBA

Behavioral targeting stems from the ability to track users across the web as they navigate within and between sites, capturing a consistent flow of information about users' behavior, including their interaction with ads themselves. This requires that a third party (not isolated publishers) be able and allowed to follow users across sites so as to develop user profiles which can then be subject to various data mining techniques, yielding predictive models that serve as the engine for ad decisioning and targeting systems. This is more than context-dependent advertising. In OBA, users are presented with ads not because of one-off search queries (otherwise known as sponsored search) or the content of their email (as in Google's Gmail); rather, they are presented with ads because of their specific behavioral history, which may reveal a richer portrait of the users' interests, as well as a calculated propensity to respond to ads in question, given trends in the receptivity of users with similar interests and behavioral histories.

A. Ad Network

In many respects, OBA bridges what had previously been the irreconcilable divide between so-called media buying and direct marketing: advertisers, in the tradition of direct marketing, can target specific individuals across multiple online publishers. These publishers still provide the crucial space for the presentation of ads, but they themselves are no longer the isolated, exclusive, or necessary passage point to specific audiences.

In principle, ad networks constitute a form of outsourcing. An online publisher may choose, for instance, to enroll in an ad network, which amounts to the outsourcing of (some of) its advertising sales force. The ad network acts as a third party that connects pools of online publishers with advertisers. The ad network allows advertisers to buy space across an entire network of member online publishers; it facilitates, through a process of aggregation and centralization, the sale and purchase of ad space. So rather than buy space directly from an online publisher, a company may decide to buy space through the ad network, of which the online publisher is but a member.

This hand-off entails other forms of out-sourcing, including the hosting and serving of the company's ad on the publisher's webpage (through a so-called ad server) and the tracking of user impressions, clicks, and conversions (when a click leads to a purchase or some other agreed upon action). The ad network also performs the crucial task of decisioning, the process by which the most appropriate ad—however defined—is selected for presentation on a particular site and to a particular user.

Most ad networks own and operate their own ad servers which generally stand outside the institutional boundaries and technical infrastructure of the independent publishers with whom they contract. The ad server is the backbone of the ad network ecology: it delivers the content that fills the ad space on publishers' pages and, in turn, collects information about the users who view its content. This is so because web protocols allow individual pages to present a unified look and feel even if the content that ultimately appears on the page arrives from multiple servers. This fact explains much of the attraction of online advertising: the delivery and selection of ads can be largely decoupled from the publisher's extant, and often less flexible, infrastructure. Much like direct marketing, ad networks allow delivery and selection decisions to be rendered at the level of individual users rather than individual publications. Ad networks are owned and operated by many familiar companies besides Google (AdSense), including AOL (TACODA), Microsoft (Atlas), and Yahoo (Right Media), to name just a few.

B. Ad Exchange

New players have also emerged who seek to provide a standardized market place for the purchase and sale of impressions. So-called ad exchanges function as a common platform for a wider range of market participants than ad networks. An ad exchange does not act as a broker for publishers or advertisers; rather, an ad exchange sets a common and public pricing and bidding mechanism to facilitate transactions between and among various kinds of market participants, including ad networks themselves. For example, ad networks within an ad exchange can bid on one another's impressions and user data. Ad exchanges are thought to bring greater transparency and efficiency to the market through increased aggregation and impartial bidding mechanisms, helping to ensure that proper market dynamics of supply and demand prevail, but in so doing also introduce enormous complexity into information flows. Ad exchanges replace semi-stable contractual relationships concerning the sale of impressions or transmission of user data with fleeting relationships based on real-time auctions that may nonetheless result in the equally permanent transmissions of user data.

III. Profiling and Predictive Modeling

Online advertising is a two-way exchange; data flows in both directions. Indeed, users have multiple forms of contact with ad servers. When a user navigates to a publisher who contracts with an ad network, the ad server simultaneously transmits an ad, looks-up the ad network's cookie in the user's browser, and logs certain information about that user's activity in a database. In the most basic set-up, the ad server may log the fact that this particular user received an impression of a particular ad. But it could also log whether the user happened to click on the ad. Much of this information actually figures in the industry's pricing scheme: advertisers may enter into contract with publishers or ad networks on a cost-per-click (CPC), cost-per-thousand impressions (CPM), or cost-per-action (CPA) basis. Careful and detailed logging is therefore paramount to many of the existing business models, not least to combat click fraud.

What this reveals, however, is a far more powerful system of tracking and data capture than has ever existed offline. While direct marketing may draw upon much the same information (e.g., interests inferred from magazine subscriptions, catalogue purchases, etc.), the infrastructure that exists to capture this information is far less comprehensive. Indeed, offline behavior is only really visible to direct

marketers when an individual takes a specific action that produces a transactional record; casual behavior slips through the cracks. Online, such actions are easily logged. An ad network is well positioned to note casual browsing, for instance, whether or not that browsing results in a purchase. The OBA infrastructure offers ad networks unprecedented opportunity to develop persistent records of individual online behavior.

There are, of course, certain technical features that limit the reach of these networks. First and foremost, a user's browsing behavior can only be tracked across websites with whom an ad network has an existing relationship. This is due to the particular technical features of cookies, which serve as each site's unique identifier for its users: for reasons of privacy and security, cookies are only readable by the company (i.e., server) that issues them. Let's consider a user who navigates from nytimes.com to espn.com. In this case, neither the *Times* nor *ESPN*—who both issue their own distinct cookies—would be able to determine whether the user was a reader of the other's site. But the ad network, with which both have hypothetically contracted, can identify the user on both sites. The ad network relies on its own cookie to identify the user. Market dominance is a key issue here: the more market share, the more comprehensively an ad network can track users (a recent report from the School of Information at the University of California, Berkeley, puts Google's reach at over 88% of a sample of nearly 400,000 unique domains [5]; this might explain why Google has been unable to skirt controversy). Which is all to say that so long as a webpage includes a line of code that directs a user's browser to access the ad server, the ad network will be able to follow the user across websites. This is inherently true for sites that make space available for ads served by an ad network, but it is also true for sites for which there is no advertising whatsoever. This is the case of so-called web bugs of pixel tags: clear, one pixel-by-one pixel (i.e., invisible) images that reside somewhere on a page and that send a simple request to an ad server essentially announcing the user's presence on the website, whether or not the user receives an ad. These are inserted into the code of participating publishers' pages for the simple purpose of expanding the range of tracking an ad network can undertake. And contracting advertisers who maintain their own ecommerce sites may also agree to insert a web bug on their websites so as to recognize users who have been exposed to their ads, as these are key in conversion metrics.

An ad network can therefore track users over the entire lifecycle of an advertising campaign: from first exposure on one publisher's site, to follow-up targeting on other publishers' sites, to identification on the advertiser's online store, to the user's ultimate choice to purchase a product or service. But what of this tracking? How do advertisers and ad networks make use of all this information? Aggregated user data can be subject to computerized analyses to produce predictive models that can then be used to estimate other like users' propensity to respond to certain ads. Systematically tracking user behavior allows ad networks to develop detailed records that can be mined to reveal interests, but also to reveal subtle correlations between behavioral variables and click-through and conversion rates. Google, for example, may infer interests from a user's past behavior, assigning them a place in specific predetermined interest categories, but they can also generate a percent score of the likelihood that the particular user will click on the specific ad given the receptivity of users with similar behavioral histories. These predictive models, which are the product of discrete, iterative data mining sessions, are pushed back out to the ad server where they update or replace the existing decisioning and targeting system.

IV. TARGETING VERSUS TRACKING

To grasp the ethical issues at stake in OBA, it is important to tease apart at least two distinct issues frequently conflated in both positive and critical evaluations. One is the issue of the differential targeting of ads selected according to interests, dispositions, or propensities inferred from online behaviors (as well as any other information that an ad network may draw upon in this selection). Another is the relentless tracking and capture of online behavior (which then figures in the decisions to serve particular individuals specific ads on specific occasions).

A. Targeting

The selective targeting of ads based on past behaviors and, possibly, other personal information, raises concerns over an insidious form of discrimination that Oscar Gandy has called the 'panoptic sort'. Aggregating information drawn from diverse sources and different contexts, individuals are profiled and assigned to categories of treatment [6]. If you are of the wrong color and ethnicity, living on the wrong side of the tracks, working in the wrong job, with the wrong bank balance, you will not receive the enticing discounts, dazzling offers, opportunities for self-development, or inducements to partake in exciting experiences. Not only does this compound sources of entrenched injustice by giving to those who, historically, are already well-endowed and holding back from those who, historically, are deprived, but it can also unfairly place individuals into categories in which they do not, strictly, belong, as occurs in redlining, for example.

Differential ad placement may also raise concerns over threats to individual autonomy because third parties may define and limit the choices open to individuals. The objection is that this practice not only treats humans as means to others' ends, but unduly interferes with construction of identity. Individuals might see it as their prerogative to select the products, books, locales, or services they want to hear about and not to have their choices limited and shaped by others on the basis of past behaviors and inferred dispositions.

Though to some extent one might see this as a problem for all advertising insofar as ads selectively appear in certain geographic contexts or media and not others (e.g., a billboard in a wealthy area, a print ad in a high-end fashion magazine, etc.), it is the specific purpose of OBA to selectively present different ads to different people who otherwise undertake the same immediate action (e.g., reading the same newspaper article online). Which is to say that the problem is not, generically, the selective presentation of ads, but the active decision to show specific ads to only specific audiences and not others under otherwise identical conditions.

Taking this line further, behavioral targeting might not only lock individuals into past habitual choices from which they would like to escape, but may open them to manipulation and illegitimate control by others. If someone can identify your weaknesses and vulnerabilities by closely monitoring past behaviors and dispositions, that person may be able to shape your choices, actions, transactions, and purchasing decisions in ways that do not accord with principles and purposes to which you are committed. Even if you succeed, in your deliberate actions, to stay true to these purposes and principles, others may have their own reasons for targeting your weaknesses, prejudices, or vulnerabilities, and, thereby undermining your autonomy [7].

Proponents of OBA are likely to enthusiastically agree with the premise of these critiques, but conclude that this precisely is its virtue. Like supporters of direct mail before them, they say that selective presentation of ads based on past behaviors and inferred dispositions serves individuals better than irrelevant ads and even if it deprives some of opportunities and offers there is, in fact, not all that much at stake. It is not as if core benefits are at stake, such as healthcare, salary, or education. Further, on the positive side, greater success in advertising is likely to draw greater investment in the online world.

This is as far as we will go in developing these issues, acknowledging that we have merely described and not presented conclusive arguments for one side or the other. To do so would involve specifying where legitimate influence ends and manipulation begins; it also would require a theoretical stance on acceptable and unacceptable grounds for discriminatory treatment of individuals—a issue that confounds the notion that ethical issues arises only in the case of personally identifiable or sensitive information. We have, however, sought to establish that this cluster of moral concerns, associated with selective presentation of ads based on past behaviors and, possibly, other information is different than (thought related to) the cluster of objections we discuss in the next section, namely the tracking and aggregation that is common to various forms of OBA.

B. *Tracking*

In defense of OBA, one frequently hears reactions such as, "What's the big deal if advertisers are able to serve ads more selectively?" This response, in our view, conflates concerns over tracking with those over targeting; one might be unmoved by the worries discussed above but still resent the backend machinations of OBA. A common formulation of this concern is that OBA constitutes a grave threat to privacy insofar as it subjects users' online activity to persistent scrutiny.

Although one might have expected those concerned with privacy to raise loud challenge—even calls for a ban on OBA—such resistance has not, as yet, materialized. Several factors may account for this, including, no doubt, power mongering by incumbents, who naturally might want to avoid major disruptions of a profitable pursuit. We look beyond this, however, to substantive factors, which we are better qualified to analyze. One, is that the privacy threat has not been properly characterized and evaluated; another, is that the business model thought to sustain free content, services, and vibrant activity on the web requires privacy be traded off in order for advertisers to flourish.

In the larger project of evaluating OBA, of which this paper is a part, we explore these factors, drawing on the theory of contextual integrity [8] to reveal the radical shifts in flow of personal information that OBA brings about, and the worrying violation of entrenched social norms it entails. In the remainder of *this* paper, however, we limit our scope to a third factor, namely, the view that a combination of anonymization and notice and consent can solve the privacy conundrum. This view is promoted by key actors, including incumbents, trade organizations, and regulators, and seems even to have mollified activist members of the FTC, such as, Commissioner Pamela Harbor Jones, responding to the industry's proposed seven principles, "I am gratified that a group of influential associations—representing a significant component of the Internet community—has responded to so many of the privacy concerns raised by my colleagues and myself" [9].

V. MITIGATIONS

Supporters of OBA, including practitioners, frequently point to ways that fears can be and have been addressed.

A. *Anonymization*

Anonymization is an example of an attempt to mitigate the privacy concerns of tracking by excluding 'personally indefinable' or 'sensitive' information, which offers little to quell concerns over targeting. While anonymization may assure us that we are not targeted as Solon Barocas or Helen Nissenbaum, it cannot ensure that we are not selectively presented or selectively shielded from ads on the basis of some set of criteria to which we might object, even if that set is otherwise unremarkable in isolated pieces. This is true both philosophically and technically: a detailed portrait of an anonymous user's online behavior may enable a level of discrimination to which one would not want to be subjected. Furthermore, it may actually incorporate a sufficient range of information that, when combined, reveals precisely the kind of linchpin information that is supposedly protected by anonymization [10]. For example, if an ad network were to know enough about a person's interests, it might begin to know something about that persons' race, gender, age, etc. An ad network might even be able to identify a particular individual with a high degree of certainty, even if that was not its intent. To this extent, anonymization fails to respond to targeting concerns and may even fail to fully address tracking concerns.

B. *Notice and Consent*

To mitigate privacy threats, it is common to see calls for notice and consent (equivalent to 'informed consent'), which impose a requirement upon actors who collect or use information to explicate their collection and use practices ('give notice') and to allow users an opportunity to choose whether or not to participate ('consent'). Accordingly, much of the controversy that surrounds OBA stems from competing visions of the proper implementation of notice and consent. In our view, this is something of a red herring. Moving

backwards from consent to notice, we explain why this particular strategy is fundamentally inadequate under the technical and institutional conditions that currently hold, and why this strategy likewise fails to address properly the peculiar threats that stem from targeting and tracking.

1) Consent (Choice)

The opt-out/opt-in approach to consent is hegemonic across a range of online practices. It is the main approach around which both proponents and critics of OBA have coalesced. Whereas proponents favor and have championed an opt-out regime, based on a notion of passive consent with opportunities for revocation, critics have pushed for an opt-in regime, based on active consent. At present, opt-in regimes for OBA and other practices of online tracking are nearly non-existent; consent currently amounts to the choice to opt-out. Despite their popularity, opt-outs are plagued by ambiguity. There is, as yet, no uniformity in interpretation of opt-out across the industry. If a user chooses to opt-out of OBA, it is unclear (because generally unstated) whether the user opts-out of targeting or tracking or both, and whether the user's existing profile is simply frozen (but retained) or completely erased. It also appears practically impossible to opt-out of tracking under the current mechanisms put in place by certain ad networks. Microsoft and Yahoo!, for instance, issue uniquely identifiable opt-out cookies, which means that while users may avoid targeting, they continue to be tracked. To this extent, existing mitigations based on opt-out cookies do not respect the different ethical concerns that stem from targeting as compared to tracking. This ambiguity imperils both an opt-out *and* opt-in model of consent. Under such conditions, they cannot appropriately model the more particular decisions a user might want to take. Though this may well amount to an issue of appropriate notice, the continued failure to articulate in clear detail the terms of opt-out (and thus also the terms of participation) betrays a larger problem with notice in general.

2) Notice

This line of reasoning might beg the question: What counts as adequate notice? After investigating the subject of behavioral targeting intensively and extensively, our own ongoing uncertainty over what really is happening with information about our online activities suggests that notice, as yet, may not be sufficient for meaningful consent. Users who are subject to OBA confront not only significant hurdles but full-on barriers to achieving meaningful understanding of the practice and uses to which they are expected to be able to consent. This stems from various types of complexity and volatility in the ecology and dynamics of the industry, its policies, and its information flows.

a) Disharmonious privacy policies

Although online publishers mediate interactions between users and the third parties that engage in targeting and tracking, the publishers do not set the policies for the third parties with whom they contract. In fact, even though ad networks interact directly with users, it is by no means apparent to users that when they visit a fixed-domain online publisher, they are connecting to several other servers simultaneously. Website owners, in their privacy policies, often reveal to users what information they gathered (e.g., behavioral information, registration information, etc.), how it is may be used, and which third parties may form a part of their sites' larger ecologies. However, for all their efforts at achieving transparency and integrity, even conscientious companies, which, for example, we assume the New York Times to be, do not fully grapple with what counts as personal information, and still cannot tell users what contracting third parties do with behavioral information. As of July 27, 2009, NYTimes.com, whose privacy policies are otherwise relatively clear and complete, lists 14 of "the *most common* third-party servers that advertisers use on NYTimes.com" (emphasis added) [11]. We assume, though it is unclear, that some of these, including those not mentioned in the 14 most common, are also tracking users' behaviors. As the Berkeley report cogently argues, "[w]hile most [publisher] policies state that information would not be shared with third parties, many of these sites allowed third-party tracking through web bugs […] It makes little sense to disclaim formal information sharing, but allow functionally equivalent tracking with third parties […] Users do not know and cannot learn the full range of affiliates with which websites may share information" [5]. To make an informed choice, users must fathom: (1) Which actors have access (which is not at all obvious); (2) What information they have access to (which varies significantly across actors); (3) What they do or may do with this information; (4) Whether the information remains with the publisher or is directly or indirectly conveyed to third parties; and (5) What privacy policies apply to the publisher as compared to the all the third parties, assuming these are even known to the users.[1] These still constitute, no doubt, only a subset of what a user might need to know in order to be meaningfully informed.

b) Ficke privacy policies

Carrying on with the New York Times example, the company's privacy policy informs users that with thirty days' notice, NYTimes.com is entitled to change policies, including its relationships with targeting and tracking third parties. There is an expectation that users will check back on a monthly basis if they wish to remain informed. And this is for only one website! Such fickleness likewise applies to the individual policies of the long list of targeting and tracking third parties with whom the NYTimes.com contracts. Google's move into OBA is instructive. In July 2007, Susan Wojcicki, Google vice president of product management for advertising, suggested that OBA was "not something that we have participated in, for a variety of reasons," and that Google wanted to "be very careful about what information would or would not be used" for the purposes of advertising [2]. And yet, as we know, Google is now potentially the most dominant player in the OBA field. This about-face should give us pause, not only because it revels how flimsy privacy commitments may be, but because, as Chris Hoofnagle points out, users who relied on Google's aversion to behavioral targeting from 2000-2006 may "have already used Google for years and may have some lock in from adopting the company's many service […] when these

[1] We acknowledge that for ad networks that belong to and are governed by the NAI there is a degree of efficiency. That said, although there is a universal opt-out, we stress that there is no universal privacy policy that governs all members.

practices change, one must ask whether revocations of trust can be effective, because individuals have no right to require a service to erase personal data collected about them" [12]. The short shelf-life of privacy policies makes notice all the more important, but likewise results in a still more onerous burden on the user, who, even if she were to vigilantly follow the privacy policies of the relevant actors, may find that prior commitments no longer apply retroactively.

c) Complex and opaque information flows

There are other circumstances where notice and consent have been adopted as a legitimate condition of engagement even when subjects are similarly not assumed to have a full grasp of their circumstances. For example, patients about to undergo major surgery sign consent forms, considered acceptable even though no one assumes they fully understand exactly how the surgery is performed, or fully grasp the probabilities of negative side effects. For human subjects participating in scientific experiments, the circumstances are similar.

Complexity constitutes a challenge, generally, for achieving meaningful notice, but OBA is unlike surgery in two significant ways. First, given adequate time, training, and education, a person confronted with a medical decision could, in principle, fully understand what they were consenting to. In the case of OBA, however, there is a degree to which the tracking, analysis, and use (current and future) of data is not only difficult to grasp, but unknowable. As we noted above in our description of the capture and processing of information, there is potentially an unending chain of actors who receive and may make use of behavioral and other data. New companies bloom, novel analytical tools emerge, business relationships begin and end. In the currently preferred model, when people consent to OBA—or fail to opt out—they literally cannot know what they are consenting to.

A second consideration more starkly distinguishes OBA from medical treatment and weighs against the legitimacy of notice and consent. It is background context. Implicit in the consent forms that patients and human subjects sign is a set of assumptions, professional commitments and principles, guiding norms, laws, and regulations that provide supporting assurances for the leap of faith they call for. As a patient goes in for surgery, she consents to the possible risks and side-effects, trusting that the surgeon, staff, and hospital are working to promote her best (health) interests, whether because they are experts dedicated to a calling, bound by professional commitments, ambitiously seeking success, or merely seeking to avoid trouble, legal or otherwise. A decision to sign on to surgery or cancer treatments are not arbitrary even though we do not understand how they work because we trust the network of assurances built into the healthcare context. The same cannot be said for the massive monitoring schemes that enable OBA. For all but a tiny handful of users, the decision to participate—if it is even an active one—is at best an arbitrary pick.

VI. CONCLUSION

If the moral legitimacy of notice and consent stems from the belief that it respects individual autonomy, specifically, that it reflects rational and informed agency required of a competitive marketplace, OBA simply does not meet these requirements. This finding does not in itself imply that OBA is unethical, only that the particular approach to addressing privacy threats so favored by businesses and even consumer advocates is seriously flawed. It is not that notice and consent can play no possible role in relation to behavioral targeting, only that the surrounding context as currently holds, unlike in the medical arena, does not properly support a meaningful role for it. We would therefore support substantive direct regulation that would help establish these warranties.

[1] Aitan Weinberg, "Driving monetization with ads that reach the right audience," Weblog, 11 March 2009, http://adsense.blogspot.com/2009/03/driving-monetization-with-ads-that.html

[2] Eric Auchard, "Google wary of behavioral targeting in online ads," Reuters, 31 July 2007, http://www.reuters.com/article/technologyNews/idUSN3135052620070801

[3] Federal Trade Commission Staff Report: Self-Regulatory Principles For Online Behavioral Advertising, Washington, DC: Federal Trade Commission, http://www1.ftc.gov/os/2009/02/P085400behavadreport.pdf

[4] Self-Regulatory Principles for Online Behavioral Advertising, http://www.iab.net/media/file/ven-principles-07-01-09.pdf

[5] Joshua Gomez, Travis Pinnick, Ashkan Soltani, Know Privacy, Berkeley, CA: University of California, Berkeley, School of Information, http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf

[6] See Oscar Gandy, The Panoptic Sort: A Political Economy of Personal Information, Boulder, CA: Westview Press, 1993.

[7] See David Lyon, Surveillance as Social Sorting, New York, NY: Routledge, 2003.

[8] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford, CA: Stanford University Press, Forthcoming.

[9] Key Trade Groups Release Comprehensive Privacy Principles for Use and Collection of Behavioral Data in Online Advertising, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209

[10] See Alessandro Acquisti and Ralph Gross, Predicting Social Security Numbers from Public Data, Proceedings of the National Academy of Science, Vol. 106, No. 27 (2009): 10975-10980; Cynthia Dwork, Differential Privacy, Automata, Languages and Programming, Vol. 4052 (2006): 1-12; Bradley Malin, Latanya Sweeney, and Elaine Newton, Trail re-identification: learning who you are from where you have been, LIDAP-WP12, Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA: March 2003; Paul Ohm, The Probability of Privacy: Questioning efficacy of efforts to anonymize data to protect privacy in light of Computer Science theories about the probability of reidentification, Forthcoming; Vitaly Shmatikov and Arvind Narayanan, De-Anonymizing Social Networks, Forthcoming in Proceedings of 30th IEEE Symposium on Security and Privacy, May 2009; Vitaly Shmatikov and Arvind Narayanan, Robust De-anonymization of Large Sparse Datasets (How To Break Anonymity of the Netflix Prize Dataset), Proceedings of 29th IEEE Symposium on Security and Privacy, May 2008.

[11] http://www.nytimes.com/ref/membercenter/help/privacyinformation2.html

[12] Chris Jay Hoofnagle, Beyond Google and Evil: How policy makers, journalists and consumers should talk differently about Google and privacy, First Monday, Vol. 14, No. 4-6 (2009)