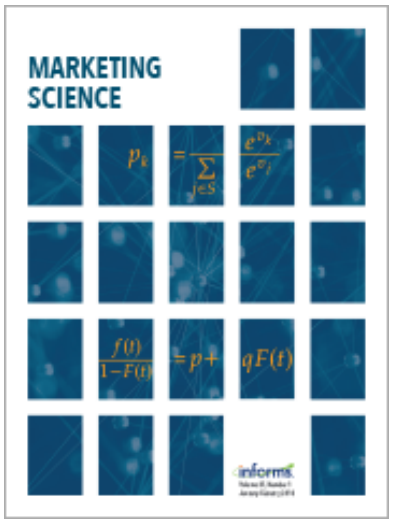

Marketing Science

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Commentary—Discussion of "Online Display Advertising: Targeting and Obtrusiveness" by Avi Goldfarb and Catherine Tucker

Andrea M. Matwyshyn,

To cite this article:
Andrea M. Matwyshyn, (2011) Commentary—Discussion of "Online Display Advertising: Targeting and Obtrusiveness" by Avi Goldfarb and Catherine Tucker. Marketing Science 30(3):409-412. https://doi.org/10.1287/mksc.1100.0599

MARKETING SCIENCE
CELEBRATING 30 YEARS
Vol. 30, No. 3, May–June 2011, pp. 409–412
ISSN 0732-2399 | EISSN 1526-548X | 11 | 3003 | 0409

informs

DOI 10.1287/mksc.1100.0599

Commentary

Discussion of "Online Display Advertising: Targeting and Obtrusiveness" by Avi Goldfarb and Catherine Tucker

Andrea M. Matwyshyn
Legal Studies and Business Ethics Department, The Wharton School of the University of Pennsylvania, Philadelphia, Pennsylvania 19104, amatwysh@wharton.upenn.edu

In "Online Display Advertising: Targeting and Obtrusiveness," Avi Goldfarb and Catherine Tucker present an empirical investigation and discussion of consumers' reactions to obtrusive and targeted Internet advertisements. They find, among other things, that obtrusive advertisements when combined with targeting tend to generate no greater effectiveness in consumer response than either method used alone. Perhaps one of the most interesting findings in their results involves the authors' focus on privacy salience and its connection to advertisement presentation. This brief discussion of their work (1) highlights the importance of further research in line with the well-crafted privacy preference inquiries of Goldfarb and Tucker's study and (2) complements the authors' discussion regarding possible public policy implications with a legal discussion elaborating on existing legal grounds for liability and restrictions on advertising consumers perceive as privacy invasive.

Key words: law; policy; privacy
History: Received: July 19, 2010; accepted: July 19, 2010. Published online in *Articles in Advance* February 9, 2011.

1. Beyond Demographic Variables: Consumer Privacy Preferences

Goldfarb and Tucker (2011) empirically explore whether privacy concerns drive, at least in part, the lack of improved effectiveness they observed when targeted and obtrusive ads were combined. They assert that "[c]ontextual targeting and high visibility (obtrusiveness) are much stronger substitutes for people who refused to answer a potentially intrusive question on income. They are also stronger substitutes in categories in which privacy might be seen as relatively important (such as financial and health products)" (p. 390). Therefore, in addition to their major finding that obtrusiveness and targeting do not work well in combination, they find a link with consumer perceptions of privacy.

Because of this focus on privacy salience in particular, the piece highlights the importance of variables other than strictly demographic variables in assessing factors driving consumer behavior and advertising. However, the authors correctly stipulate a noteworthy shortcoming of their work: they are, in fact, likely underestimating the magnitude of the privacy salience trade-off effects. The salience of privacy concerns will be highest in the group of consumers not represented—those who refuse to participate in such survey research on the grounds that it is privacy invasive. Consequently, average consumer privacy preferences regarding advertising are not necessarily optimally represented in the sample. A truly representative sample of consumers would likely demonstrate an even stronger privacy effect.

The authors' work highlights the importance of moving beyond standard demographic variables of race, gender, and socioeconomic status in research on consumer behavior; cross-cutting variables such as privacy preferences demonstrate a need for more research similarly sensitive to these types of nuanced attitudinal variables.

Goldfarb and Tucker's research can also be read to offer evidence that targeted or behavioral advertising is not the only effective means of catching consumer attention. In fact, their research argues that targeted ads may add no value when coupled with another, possibly less privacy-invasive means of advertising. As such, this work contributes valuable insight for the regulatory discussion of fair trade practices and consumer information control.

2. Potential Legal Liability and "Privacy-Invasive" Advertising

The authors hint at some of the potential policy implications that may result from their research. Goldfarb and Tucker correctly note the mounting pressure in the United States and European Union to

regulate in the area of behavioral targeted advertising. In the United States, in July 2008, the House of Representatives and the Senate conducted hearings about privacy and behavioral targeting practices,[1] and, in August 2008, four members of the United States House of Representatives Committee on Energy and Commerce sent letters to 33 companies[2] requesting information regarding the types of information they are collecting from consumers and the relevant privacy standards.[3] The authors encourage regulators to weigh the two potential types of advertising—obtrusiveness and targeting—against each other when choosing future regulatory approaches. Pointing to survey data, they advise that consumers have expressed dislike for both data collection about browsing behaviors and highly visible ads.

However, the authors do not mention that certain types of targeted and behavioral advertising may run afoul of already-existing law—not merely of regulation in the future. As such, some forms of targeted advertising are potentially currently illegal. Recent Federal Trade Commission privacy enforcement activity and two recent corporate promotional efforts that went awry offer harbingers of future legal issues faced by advertisers experimenting with targeted advertising techniques. Advertising perceived by consumers as "privacy invasive" already leads to possible legal ramifications, including class action lawsuits, as well as public relations debacles.

The legal issues raised by behavioral targeting in online advertisements potentially implicate existing fair trade practices law, contract law, privacy law, computer intrusion law, and other statutes. Conceptually, they are bound up in the meaning of consumer "consent" to the information collection and the fairness of advertisers' disclosure practices. In both such inquiries, a reasonable consumer's capacity to understand the process of collection and the use of data is an integral part of the inquiry.

Section 5 of the Federal Trade Commission Act empowers the Federal Trade Commission to bring enforcement action against companies engaged in "unfair and deceptive trade practices" that are in or affecting "commerce."[4] The Commission has begun to use its authority under §5 with growing frequency in connection with consumer complaints regarding privacy and information security practices. For example, the FTC filed a complaint against Sears Holding Management Corporation in 2009, asserting the company "disseminated or caused to be disseminated via the Internet a software application . . . in connection with SHMC's 'My SHC Community' market research program . . . [which] runs in the background at all times on consumers' computers and transmits tracked information, including nearly all of the Internet behavior that occurs on those computers, to servers maintained on behalf of [Sears]."[5] According to the FTC complaint, Sears

> failed to disclose adequately that the software application, when installed, would . . . monitor nearly all of the Internet behavior that occurs on consumers' computers . . . . These facts would be material to consumers in deciding to install the software [and] failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice . . . that constitute[s] unfair or deceptive acts or practices in or affecting commerce in violation of §5(a) of the Federal Trade Commission Act.

Most advertisers engaged in this type of targeting and information collection, particularly those in the United States, would likely argue that their data collection and sharing practices are a simple matter of contract: when consumers agree to a company's terms of service through, for example, a website, consumers agree to data practices that include the collection and use of their information for targeted advertising purposes. On the other hand, consumers who object to these targeting practices would argue that they did not consent in a meaningful sense: if they had understood that the agreement would subject them to extensive

[1] In particular, in 2008, the actions of two companies triggered closer examination of advertising practices and behavioral targeting—NebuAd in the United States and Phorm in the United Kingdom. One of the controversial techniques they used to obtain consumer data was deep packet inspection, which allows analysis of network traffic to identify the application that sent the data, differentiation of data, and analysis of the contents of the data packets that are unencrypted, including which website originated the packets. See ZDNet.

[2] Companies who received these letters included Google, Microsoft, Comcast, AT&T, AOL, Time Warner, and Cox Communications. See Clifford (2008).

[3] Meanwhile, the EU Information Commissioner has stated that behavioral targeting in advertising must be structured on an "opt-in" basis for consumers, and she raised questions regarding the legality of certain behavioral targeting practices. See Swearingen (2008).

[4] The statute states, in relevant part, "...Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful . . . . The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." See *Federal Trade Commission Act*, U.S. Code 15 (1914), §§41–58, as amended (2006), §5 (http://www.ftc.gov/ogc/FTC_Act_IncorporatingUS_SAFE _WEB_Act.pdf).

[5] Information transmitted included "Web browsing, filling shopping baskets, transacting business during secure sessions, completing online application forms, checking online accounts, and, through select header information, use of Web-based e-mail and instant messaging services" (see *In the Matter of Sears Holdings Management Corporation, a corporation,* FTC File 082 3099 (June 4, 2009), http://www.ftc.gov/os/caselist/0823099/090604searscomplaint.pdf).

data collection behaviors they find objectionable, they would not have agreed.[6]

Contractual consent issues are also aggravated by questions regarding what constitutes meaningful contractual disclosure about data collection, a material term of the agreement. Consumers frequently perceive data collectors to ask them to consent in contract to behaviors that a consumer cannot foresee or understand. Subsequently, therefore, these consumers are more likely to become upset and find advertiser data behaviors retrospectively privacy invasive.[7] A consumer may argue—potentially persuasively—in a court complaint or in a complaint to the Federal Trade Commission that meaningful consent is absent in some targeted advertising scenarios. Prosecutors, legal scholars,[8] and legislators in the United States are divided on the best course of action in addressing this potential over reaching and inadequate disclosure. However, as recent Federal Trade Commission inquiries demonstrate, subjective consumers' perceptions of lack of control over their information matter. Consumers' beliefs that they have not been afforded fair opportunity to understand the collection process can be dispositive, at least with respect to initial fairness inquiries.

Another potential problem for advertisers experimenting with privacy-invasive advertising methods involves a different aspect of consent to data collection—if data are collected without consent it may constitute a computer intrusion or a wiretap. Legally, what constitutes an intrusion or an unwanted technological "touching" of a user's machine is contingent entirely on user consent; so too this notion of consent transfers into questions of data collection for behavioral targeting. The language used by wiretapping and computer intrusion statutes in the United States revolves around "interception," i.e., monitoring without consent, and "exceeding authorized access," meaning surpassing the extent of consent.[9] Two U.S. federal statutes, as well as a patchwork of state statutes, use this framework of consent in the context of criminal and civil computer intrusion—the Electronic Communications Privacy Act[10] and the Computer Fraud and Abuse Act.[11]

Finally, even if a particular advertising scheme appears on its face legal, it may still violate many consumers' and regulators' sense of acceptable privacy conduct. Even relatively sophisticated companies regularly misjudge the extent to which a particular promotion or advertising strategy will cause consumer outcry with respect to privacy invasiveness. Whereas some consumers may prefer a privacy-invasive behavioral advertising model, a significant number of consumers likely do not. As such, a company's choice of a privacy-invasive model of advertising may cause not only lower response rates to the advertising, but it may also alienate existing privacy-sensitive customers. Misjudging privacy sensitivities in consumers can result in possible loss of previously loyal purchasers.

Two recent examples of this underestimation of "privacy invasiveness" and existing user reactions involve Google and Facebook. In 2009, Google launched a product called Buzz (http://www.google .com/buzz). By external appearances, Buzz seemed to be a type of crossover product between a Facebook-like interface and a Twitter feed. To assist in its adoption, Google decided to repurpose the data in users' Gmail e-mail account contact lists for their individual starter group of "followers" in Buzz, making these lists public by default. Almost immediately, public outcry ensued. Gmail address books for some users contained contact information for individuals that were unwelcomed followers. In its zealousness to promote Buzz, Google had, according to press accounts,[12] cut short its usual beta testing process and unintentionally triggered the "privacy invasion" sensitivity of some of its users. This decision was subsequently labeled by an FTC Commissioner as "irresponsible conduct,"[13] and at least 11 U.S. lawmakers called for an FTC investigation.[14] Along similar lines, Facebook found itself in court arising out of its Beacon program, which collected data regarding user behaviors on "partner" websites.[15] The Beacon program involved embedded code in partner sites and caused a post regarding consumer conduct on those partner sites to be posted to a consumer's Facebook feed.[16] Some users did not understand how this

[6] For U.S. courts, the crux of the legal question revolves around the meaning of contractual consent in a digital context. Consumers would further argue that the extent of privacy invasion is frequently not explicitly identified in the agreements they are presented and not understandable to an average consumer.

[7] Every agreement that successfully obtains meaningful consumer consent for data collection is based on the assumption that the consumer has had a reasonable opportunity to read and understand the terms of the agreement. Ideally, the consumer has also had an opportunity to negotiate the terms of the agreement.

[8] For example, Professor Ohm argues that some types of ISP behavioral targeted advertisements likely constitute violations of the Electronic Communications Privacy Act (ECPA) (see Ohm 2009).

[9] The ECPA is composed of Title I, amendments to the Wiretap Act, and Title II, the *Stored Communications Act*; U.S. Code 18 (1986), §§2701–2712. See *Computer Fraud and Abuse Act*, U.S. Code 18 (1986), §1030.

[10] U.S. Code 18 (1986), §§2701 et seq.

[11] U.S. Code 18 (1986), §§1030 et seq.

[12] See Fildes (2010).

[13] See Steel (2010).

[14] See Gross (2010).

[15] See Perez (2007).

[16] For a discussion of the public relations problems for Facebook caused by the "Beacon" technology, see, e.g., Perez (2007).

information was being shared, and they considered the practice privacy invasive. This confusion resulted in what the media has termed a "public relations disaster"[17] and in a class action lawsuit against Facebook that resulted in a settlement in the amount of $9.5 million.[18]

Goldfarb and Tucker have made a significant contribution to the conversation around privacy invasiveness and marketing. Extensive additional research on users' perceptions of privacy-invasive practices is still needed, however. This is true both with respect to marketing approaches and with respect to optimal methods of legal regulation: preserving a fair marketplace for both consumers and advertisers first necessitates a better understanding of consumers' privacy invasiveness perceptions. Further research along the lines of this work should explore the various models of advertising that strive to offer consumers greater information control and flexibility in reflecting their privacy preferences, including rights of data editing and deletion.

References

Clifford, S. 2008. Web privacy on the radar in Congress. *New York Times* (August 10), http://www.nytimes.com/2008/08/11/technology/11privacy.html?_r=1.

Fildes, J. 2010. Google admits Buzz social network testing flaws. *BBC News* (February 16), http://www.bbc.co.uk/2/hi/technology/8517613.stm.

Goldfarb, A., C. Tucker. 2011. Online display advertising: Targeting and obtrusiveness. *Marketing Sci.* **30**(3) 389–404.

Gross, G. 2010. Lawmakers ask for FTC investigation of Google Buzz. *IDG News* (March 29), http://www.pcworld.com/businesscenter/article/192801/lawmakers_ask_for_ftc_investigation _of_google_buzz.html.

McCarthy, C. 2009. Facebook notifies members about Beacon settlement. *CNet* (December 3), http://news.cnet.com/8301-13577_3-10409034-36.html.

Ohm, P. 2009. The rise and fall of invasive ISP surveillance. *Univ. Illinois Law Rev.* **2009**(5) 1417–1496. http://www.law.uiuc.edu/lrev/publications/200s/2009/2009_5/Ohm.pdf.

Perez, J. C. 2007. Facebook's Beacon more intrusive than previously thought. *IDG News* (November 30), http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html.

Steel, E. 2010. Google Buzz exemplifies privacy problems, FTC Commissioner says. *Wall Street Journal* (March 17), http://blogs.wsj.com/digits/2010/03/17/google-buzz-exemplifies-privacy-problems-ftc-commissioner-says/.

Swearingen, J. 2008. Behavioral targeting has its day in the UK. *BNET* (September 29), http://www.bnet.com/blog/advertising/behavioral-targeting-has-its-day-in-the-uk/235.

ZDNet. Deep packet inspection. Accessed January 11, 2009, http://www.zdnet.com/search?q=deep+packet+inspection.

[17] See McCarthy (2009).

[18] *Lane et al. v. Facebook, Inc. et al.*, N.D. Cal 5:08-cv-03845-RS (2010), http://www.beaconclasssettlement.com/ (accessed July 15, 2010).