The Do Not Track Me Online laws: creating a ceiling when the sky’s the limit and we are halfway to heaven

Nada Mohamed*

School of Law, Case Western Reserve University, Cleveland, OH, USA

This comment examines a recent Wall Street Journal article discussing proposed plans of MasterCard or VISA to provide customers with targeted ads as they surf the Web using information attained by tracking customer purchases in brick-and-mortar stores. Since the online behavioral advertising industry is largely self-regulated, this raises concerns as to whether the companies amassing this information are giving customers adequate disclosure of their collection and dissemination practices and an opportunity to give sufficient informed consent. The lack of legislation specific to these practices, or regulatory oversight, has paved the way for organizations to race to discover increasingly intrusive ways of compiling consumer information. Finding a balance between an individual’s right to privacy and commercial access to personal information represents the fundamental regulatory issue that needs to be resolved. The Do Not Track laws proposed by Representative Jackie Speier of California in February of 2011 represent a good start to creating this balance. This comment will examine the specific plans proposed by VISA and MasterCard, discuss the current regulatory status of online behavioral advertising, and conclude by arguing that the proposed Do Not Track laws provide the appropriate balance between consumer privacy protection and marketing needs.

Keywords: privacy; e-payments; online behavioral marketing; marketing; online behavioral advertising; information exchange; informed consent; consumer rights; right to privacy; consumer privacy; consumer privacy protection

Introduction

According to a recent Wall Street Journal article, every purchase you make with your MasterCard or VISA could be used to provide you with targeted ads as you surf the Web (Steel, 2011). The companies are investigating using methods of tracking customer purchases in brick-and-mortar stores in order to deliver ads tailored to their needs online (Steel, 2011). Today, none have the capability to accomplish this feat of linking an individual’s offline purchase activity to an online profile (Steel, 2011). However, the credit card system, with its massive customer base and the capacity to track millions of purchases daily, both online and offline, may represent the best candidate for meeting this need (Woolsey & Shulz, 2011). With the online behavioral advertising industry being largely self-regulated, however, this raises concerns as to whether the companies amassing this information are giving...
customers adequate disclosure of their collection and dissemination practices and an opportunity to give sufficient informed consent (Reisinger, 2011).

Tracking customer purchases and online behavioral advertising are not novel marketing tools. However, MasterCard’s and VISA’s plans represent an advent to obtaining consumer information – one that is not restricted to the confines of an ISP. The lack of legislation specific to these practices, or regulatory oversight, has paved the way for organizations to race to discover increasingly intrusive ways of compiling consumer information. The more information obtained, the higher the companies’ profit will likely be when they sell it to marketers attempting to solve what it is consumers desire in order to target them in the most effective way, at the least cost (Vartanian, 2000).

Finding a ‘balance between an individual’s right to privacy and commercial access to personal information’ represents the fundamental regulatory issue that needs to be resolved (Mann, 2001). The Do Not Track laws proposed by Representative Jackie Speier of California in February of 2011 represent a good start to creating this balance (Simpson, 2011). This comment will examine the specific plans proposed by VISA and MasterCard, discuss the current regulatory status of online behavioral advertising, and conclude by arguing that the proposed Do Not Track laws provide the appropriate balance between consumer privacy protection and marketing needs.

Online behavioral advertising: how VISA’s and MasterCard’s plans represent a new frontier

Online behavioral advertising involves ‘the tracking of consumers’ activities online’ in order to deliver advertising targeted to the individual consumer’s interests online (Ballon, 2011). Typically, the entity tracking and collecting the information has gained the business of the individual whose information is being collected through a sale, service, or transaction using cookie files deposited on that user’s hard drive (Ballon, 2011). The information gleaned often includes ‘a review of the searches consumers have conducted . . . the purchases made, and the content viewed’ (Shelton, 2011).

These companies then, ‘use the data to build a “profile” of their users. These profiles are then frequently sold to advertising companies that focus marketing based on each user’s preferences’ (Mann, 2001). Companies tracking purchase behavior argue that this type of advertising is more valuable to advertisers and more relevant to users (Ballon, 2011). Marketers purchasing the information describe it as aligning marketing efforts ‘more closely to the inferred interests of their audience,’ but acknowledge that these mechanisms ‘involve[] practices that are largely invisible to users’ (Ballon, 2011).

Today, organizations do not have the capability to track customer purchases made in brick-and-mortar stores and then link the ‘consumer’s identity and spending history to an online profile’ (Dawson, 2011). However, MasterCard and VISA are both investigating means to fill that void. They certainly have the numbers to accomplish this: as of yearend 2010, VISA boasted 666 million users of their credit and debit cards, while MasterCard laid claim to 294 million users (Woolsey & Shulz, 2011).

The ability for credit-card systems, in general, to collect personal purchase information is powerful. So much so that their usage as a national ID has been
recently debated (Hunter, 2002). After all ‘[p]eople are what they do, and much of what people do can be inferred from the things they choose to buy’ (Hunter, 2002). This concept seems to be center of MasterCard’s ‘you are what you buy’ campaign, as it explores ‘ways to anonymously group a person’s purchase history with others to create marketing “segments”’ in its (Reisenger, 2011).

VISA has filed at least eight patent applications, published in April of 2011 (Dawson, 2011), covering identity matching mechanisms capable of ‘generating transaction profiles based on the transaction data, the account data, and/or other data, such as non-transactional data, wish lists, merchant provided information, address information, information from social network websites, information from credit bureaus, information from search engines, information about insurance claims, information from DNA databanks, and other examples’ (Shanks, 2011). VISA’s plans ‘also describe the potential to track whether or not a person who sees an online ad ends up buying the advertised product’ (Steel, 2011). Once they have compiled the relevant data and meaningfully organized it, VISA and MasterCard would then sell this information to third party ‘marketing firms who will target consumer’s surfing the web accordingly’ (Reisenger, 2011).

Tracking customers to collect information for marketing purposes represents a three-fold benefit. For the credit card companies, it ‘represents a potential source of revenue’ as they re-sell consumer information to third party marketers (Reisenger, 2011). For the consumer, it represents the benefit of more targeted marketing that presents them with goods and services in which they are likely to be interested (Mann, 2001). For the marketer, it represents more efficient and effective online marketing and likely improved sales (Vartanian, 2000). However, given that the advertising was unsolicited, many consumers view this information exchange as an invasion to their ‘private property and object to its misappropriation’ (Mann, 2001).

The subject of consumer privacy protection has aroused much interest. ‘As of March 2011, there were 449 comments from industry groups, advertisers and consumer advocates’ regarding the need for more protection (Sheltion, 2011). However, VISA, MasterCard, and other organizations engaging in similar practices assert that these mechanisms would be strictly voluntary, thus, there is no need for increased protective measures (Reisinger, 2011). By giving their customers the freedom and ability to ‘opt-out,’ they argue they will have obtained adequate consent from customers to collect and disseminate their private information (Steel, 2011). If a customer does not wish to take part, they may simply opt-out (Worlton, 2008). However, this is misleading given that the average consumer is unaware they are being tracked to begin with (Worlton, 2008). Moreover, an opt-out clause, typically buried beneath pages of legalese where the majority are unlikely to find it or know of its existence – is simply not enough to qualify as adequate informed consent to the collection and dissemination of private information for a profit (Worlton, 2008).

Concerns with consumer tracking, online behavioral advertising, and current law

Three main concerns typically arise when considering tracking mechanisms and online behavioral marketing. First, since both processes are largely invisible, they go unknown to consumers, and through this, although there is implied consent since the customer did not opt-out, this should not be a substitute for prior informed consent (Ballon, 2011). Second, tracking and targeting consumers without their knowledge
or approval diminishes customer trust (Ballon, 2011). Third, there are reasonable concerns about the possibility of collected consumer data ‘falling into the wrong hands or being used for unanticipated purposes’ (Ballon, 2011). For example, issuers are increasingly using data gained from tracking ‘as a basis for increasing interest rates, reducing credit limit or both on customers considered more risky by virtue of where they shop or what types of goods and services they buy’ (Prater, 2009).

Marketers, however, dispel these concerns, arguing that building profiles raises minimal privacy concerns as users are not identified by name or contact information (Worlton, 2008). Similarly, some issuers, such as MasterCard, assure that although that they may ‘collect[] data, such as when a purchase was made and where . . . [they] never include[] who actually makes the purchase’ (Reisinger, 2011). Further, it is indisputable that tracking customer also has some benefits. For example, ‘detailed data about purchase habits can help a company notice suspicious or fraudulent activity quickly’ (White, 2011). Moreover, ‘online and mobile coupon or reward programs are designed to give customers a discount in exchange for information’ (White, 2011). However, even with these assurances and benefits, a consumer retains the right to complete disclosure prior to information collection and sharing; and their consent should be unequivocal, not assumed.

In recent years, ‘the FTC has expressed increasing concern over the adequacy of privacy self-regulation by the online advertising industry with regard to the collection, use and sharing of information from consumers for behavioral advertising purposes’ (Weikers, 2011). In a staff report from 2009, ‘the FTC issued detailed self-regulatory guidelines for behavioral advertising which emphasized prominent disclosure of practices . . . and providing Internet users with meaningful choice mechanisms’. In expounding on this, the FTC stated that in light of ‘the heightened privacy concerns raised by the collection and use of consumers’ sensitive data[,]’ companies should ‘obtain affirmative express consent before collecting such data for behavioral advertising’ (Federal Trade Commission, 2009).

The FTC also urged ‘companies to provide reasonable security for any data they collect for behavioral advertising and to retain data only as long as it is needed to fulfill a legitimate business or law enforcement need’ (Federal Trade Commission, 2009). However, these suggestions have not been significantly materialized by companies collecting and disseminating the information, nor by the third parties purchasing the information. This should come as no surprise though, given the self-regulated nature of the industry.

To date, the U.S. has not passed general laws to protect personal information, but has passed laws to protect specific types of private information. The Gramm–Leach–Bliley Act (GLB) protects ‘the privacy of individual personal financial information collected by institutions and businesses’ (Weikers, 2011). The act ‘requires all financial institutions . . . to disclose to any consumer . . . their policies and practices for protecting the privacy of non-public personal information’. In its current form, however, the GLB would require no more of VISA and MasterCard than giving customers the ability to ‘opt-out’ and making periodic disclosures to customers regarding sharing their information with non-affiliated third parties (Weikers, 2011).

Unaided by legislation, some private certifying organizations have attempted to ‘assuage user concerns by offering certification that a specific company’s Web-based business is in compliance with certain minimum privacy standards established by the certifying organization’ (Popkin, 2011). TRUSTe and the Council of Better Business
Bureaus, Inc. represent two independent, nonprofit privacy certification organizations. The two award certification to the companies that adhere to their privacy principles ‘and agree to comply with its oversight and consumer resolution process’ (Popkin, 2011). Companies joining either ‘privacy program must agree to inform users of the site of what personal information is being gathered, how it will be used, with whom it will be shared, and whether the user has an option to control its dissemination. Based on such disclosure, users can make informed decisions about whether or not to release their personally identifiable information (such as credit card numbers) to the website’ (Popkin, 2011).

These organizations may provide Internet users with some assurance, however, there is no empirical evidence demonstrating that businesses certified by these organizations actually protect customer privacy any more than those that are not certified. In fact, one Harvard study has criticized these certifying organizations as granting certification too easily and with very little post-certification oversight to maintain their status (Edelman, 2006). The study also offered empirical evidence demonstrating that businesses exhibiting certification are actually less likely to be protective over consumer privacy or trustworthy than those that are not certified (Edelman, 2006).

Besides these certifying organizations, individual companies, in the interest of gaining customer trust and loyalty, ‘have adopted online privacy policies to make their customers feel more secure about using the companies’ websites...[by] expanding their privacy disclosure preemptively. For example, Yahoo!’s Ad Interest Manager allows users to see information about their browsing activities that Yahoo! collects for targeted advertising purposes and set their preferences accordingly’ (Popkin, 2011).

Likewise, Microsoft has recently announced ‘Internet Explorer 9 will feature a new “opt-in mechanism” and “Tracking Protection Lists” to help consumers control tracking of their online activity’ (Simpson, 2011). Microsoft has stated that they believe ‘the combination of consumer opt-in,’ options amongst other protective measures, would provide ‘a good balance between empowering consumers and online industry needs’ (Simpson, 2011).

Mechanisms such as these require active steps by the entity collecting consumer information to engage in them – this is not without a cost. Thus, it is no surprise that the majority of organizations in a self-regulated industry are not exercising these or any other major form of privacy protection of consumer content. Therefore, legislation targeting online tracking mechanisms to establish minimum standards is necessary.

The Do Not Track laws
Representative Jackie Speier of California introduced two pieces of legislation in February of 2011 aimed at protecting personal information (Lisko, 2012). The Do Not Track laws involve two separate bills: (1) The Do Not Track Me Online Act of 2011 (DNT), which ‘would give consumers the ability to prevent the collection and use of data on their online activities’ (Lisko, 2012); and (2) the Financial Information Privacy Act of 2011 (FIP), which ‘would give consumers control of their own financial information’ (Lisko, 2012). The two bills are currently awaiting the requisite approval by the Senate before being handed to the President for his consent (Lifsher & Guynn, 2011).
Specifically, DNT would create ‘a universal legal obligation for all online companies to honor consumer choice when consumers do not want anyone to collect information about their online activities,’ as well as allow the FTC to enforce it (Hachman, 2011). If a consumer does not allow his or her personal information to be tracked, the bill would allow companies ‘to collect only the information that is necessary for the website or online service to function and be effective, but then place a legal obligation on the online company to destroy or anonymize the information once it is no longer needed’ (Hachman, 2011). However, although the FTC has backed the creation of DNT, they have ‘not yet voted to endorse any particular proposal’ (McCullagh, 2011).

The FIP is an amendment to the GLB. In its current form, the GLB requires that consumers receive disclosures regarding collection of private information ‘at the time of establishing a customer relationship, and at least annually thereafter’ (Weikers, 2011). The Act also demands that customers be allowed to ‘“opt-out” of information sharing arrangements to non-affiliated third parties’ (Weikers, 2011). However, the GLB ‘permits financial institutions to share personal customer information with affiliates within the holding company and also contains exceptions from the “opt-out” requirement for certain disclosures to third-party service providers’ (Weikers, 2011).

The FIP amendments to GLB would ‘require that financial institutions obtain consumers’ express, opt-in consent before disclosing nonpublic personal information to nonaffiliated third parties [and]…from sharing such information with their affiliates without first providing consumers with notice and an opportunity to opt out’ (Simpson, 2011). Opt-in clauses better guard consumer information and give them the ability to provide their unequivocal informed consent more so than do opt-outs (Simpson, 2011).

Members of the European Union’s Article 29 Working Party, a group of representatives from the data protection authority of each European Union Member State, concur that opt-ins provide more protection than do opt-out clauses. In 2010, the Article 29 Working Party set minimum guidelines for protecting users when browsing the web (Simpson, 2011). These guidelines explicitly state that an opt-out clause is not enough (Simpson, 2011). Rather, for browsers to deliver valid consent, they should (1) reject third-party cookies by default, and (2) convey clear, ‘comprehensive and fully visible information’ and (3) ‘require prior opt-in consent since they are better suited to deliver informed consent’ (Simpson, 2011). Furthermore, this consent ‘must expire after a certain period of time,’ and there must ‘be a simple way for users to be able to revoke consent’ (Simpson, 2011).

The Do Not Track Me Online laws are not without opposition. Google and Facebook recently jointly sent a letter to the state of California as it considered statewide enforcement of the bill. The two companies implored the state not to enforce the bill, warning that it ‘would have disastrous consequences’ (Hruska, 2011). They argued that the bill would ‘sabotage the “rich content and free services” provided by the Internet’ and ‘[o]nline commerce would be rendered “unworkable” due to the “unprecedented and arduous regulatory burden”’ (Hruska, 2011). However, this is a misinformed perspective given that ‘[t]he law doesn’t make cookies illegal’, it simply requires that users be presented with prior and informed options to choose (Hruska, 2011). ‘Furthermore, the bill allows the Attorney General to modify the scope or application of the definition of “sensitive information” and to consider
the context in which the information is used, the ease with which it can be used to identify a person, and the potential adverse impact’ (Prater, 2009).

Conclusion
Matching everyday purchases consumers make in brick-and-mortar stores with an accurate online profile representing spending patterns epitomizes every marketer’s dream. The e-payment system in general, and credit cards in specific, with the capability to track customer purchases consistently and accurately, is likely the best candidate to meet this demand today. VISA and MasterCard, in particular, are privy to a wealth of purchase information that cannot be matched quantitatively or qualitatively (Woolsey & Shulz, 2011).

The new tracking mechanisms currently being explored by VISA and MasterCard, represent a new, higher level of intrusiveness unmatched with an appropriate balance in customer disclosure, consent, or privacy mechanisms. This is likely the outcome of the self-regulated nature of the industry. The Do Not Track Me Online laws represent a potential remedy to this problem, or, at the very least, a first step in the right direction. By requiring express opting-in as informed consent rather than opt-outs as implied consent, more choice mechanisms, and increased disclosure – these laws will likely create the appropriate balance that is currently missing between consumer privacy and effective targeted marketing.

References


