<u>Privacy and Marketing Online</u>

by

Ruth Rose Sachs

Ever since the first portable cameras were invented in the late 19^{th} century, bringing with them the ability to quickly and surreptitiously collect data, the issue of privacy as it relates to technology has continued to re-appear in our society in various forms. The present day is no exception, with internet tracking, mostly for the sake of advertising-data mining, taking the place of snapshots and wiretapping. Online targeted advertising is still in its early stages, and thus long-term outcomes cannot be definitively known. Yet whether or not businesses have particular moral obligations in the area of privacy, whether or not customers are troubled by targeted advertising- and whether or not these feelings are justified-, and whether or not privacy itself is undergoing a radical change, are all inescapable questions in today's increasingly public online landscape.

The days in which a product could be advertised on one television channel and thereby effectively reach the entire intended audience, are long gone. Marketing has instead become a highly individualized endeavor, and as a result, personal data can provide marketers with an unparalleled advantage. As our culture increasingly prides itself on individuality, our buying and consuming habits reflect this individuality as well. The market has become ever-more fragmented, with products that are purchased not only out of necessity, but in keeping with the consumer's individual identity. In their quest for a product that suits them personally, customers often find large-scale interruption-technique advertising irrelevant, and easy to ignore.

No longer able to shout their messages and be assured of takers, companies must now go out and meet their buyers, presenting a product where it is needed and desired. One of the most effective ways of “meeting” a potential buyer is through targeted advertising. In other words, using data complied about individuals or groups of buyers in order to send the most relevant ads to that demographic, thereby increasing the percentage of those who take advantage of the advertisement versus those who ignore it.

Targeted advertising can positively, and significantly, impact a company's finances in a variety of ways. First, it can have the potential to save money. If, for instance, after compiling information about the customer base, the company chooses to send out a print catalogue, it can save on postage by soliciting only those who are likely to buy, rather than papering the entire neighborhood. Similarly, it can also save costs on online ads by only advertising on sites in which the user population is likely to be interested in the product. Most importantly, however, targeted ads can have the potential to generate large amounts of revenue. Sending a well-targeted ad to a customer at the right moment could, for instance, cause the customer to develop an interest in a product he had previously not known about, or had previously never intended to buy. Additionally, many routine purchases are made by habit, and customers are often brand-loyal merely because it's what they're accustomed to. At specific points in people's lives (such as at the birth of a child or after a divorce), they are particularly likely to change brand loyalties. A company that can identify these life events and effectively market towards them may gain new customers who will continue to habitually buy their products (Duhigg).

Yet targeted ads come at a price. When targeting occurs in a sensitive topic, such as sexuality or medical history, (or, for that matter, the birth of a child or divorce) a customer may feel “spied upon”, and the reaction to the ad can quickly turn negative. Google and Target are two companies that have methods of continuing to use highly targeted ads, but assuaging customers at the same time. They both operate under the idea that as long as a customer does not have a “big brother” feeling from the advertising, it is acceptable to compile large amounts of personal data, and use highly personalized ads.

For example, the Guest Analytics Department at Target has such an effective tracking system that it can tell with an extremely high rate of accuracy if a customer is in her second trimester of pregnancy. It can then use this information to effectively market to the new mother at a time when she is most likely to buy large quantities of new products. However, since pregnancy can be seen as a sensitive topic, Target includes ads for non-pregnancy related items as well when reaching these customers in order to give the impression that the baby-themed items were simply there by chance. “We found out that as long as a pregnant woman thinks she hasn't been spied on, she'll use the coupons,” said Andrew Pole of the Target Analytics Department in an interview with the New York Times' Charles Duhigg. “As long as we don't spook her, it works” (Duhigg). Similarly, Google promises in its privacy policy not to associate tailored ads to sensitive topics such as sexuality, race, religion, etc. Nowhere, however, does it promise not to compile enough data about users in order to easily infer sensitive information, though it promises not to acquire *personally identifiable* information from ad servers without a user's explicit permission.

But could the information collected by marketers actually pose a realistic threat? Jeff Jarvis, author of *Digital Parts* expressed a common view when he sarcastically stated “Oh my God! I watched CNN yesterday and there was a guy doing a report on internet privacy and he looked at a bunch of sites about vacations, and, guess what, now they're trying to sell him a vacation- isn't that scary!” (Albanese). Does, then, the information collected for marketing purposes pose a greater potential danger than merely offering a sandy beach and a spa? I would argue that it does.

Far from being an even trade-off of ads in exchange for minute bits of unimportant, unidentifiable information, tracking for marketing purposes can have deep and long-lasting consequences. One of the primary long-term outcomes is the gradual loss of online anonymity. This outcome is not without significant controversy, as online anonymity can both protect individuals (by, for instance, ensuring freedom of speech without the possibility of retaliation), or harm them (by creating a space where libel, character defamation, and predatory behavior can thrive). Yet some of the other consequences are more immediate, and are directly tied to marketing, with the very techniques that were intended to better serve online customers in fact causing harm. The results can include political manipulation, emotional distress, and actual material loss, whether or not the information compiled is true or is falsely inferred.

For example, in the 2010 presidential elections, the Republican party collected information on individuals through data aggregation that allowed the party to direct tailor-made ads to potential voters, giving the impression that the candidate would suit the voter's needs exactly. These tailor-made promises also had the benefit of never having to be scrutinized publicly for accuracy or viability (Andrews 12). Well-targeted ads also create the possibility for psychological harm; for instance, someone who feels self-conscious due to a weight problem may be bombarded by weight-loss ads (Andrews 37-38).

Falsely inferred information can be just as harmful, with one credit card user having his credit limit dramatically lowered after visiting a tourist destination, the company's justification being “other customers who have used their card at establishments where you recently shopped have a poor repayment history” (Andrews 20).

A more subtle risk exists as well: that by controlling to some degree what information an internet user sees (what appears on a search, what ads are shown, etc.), targeted advertising can have the power to control a person's perceptions of the world at large. As Lori Andrews wrote in her 2011 book *I Know Who You Are and I Saw What You Did,* “As behavioral advertisers increasingly dictate a person's online and offline experiences, stereotyped characteristics may become self-fulfilling. Rather than reflecting reality, behavioral analysis may inevitably define it”(29). Let's take, for example, a young person in a disadvantaged neighborhood who is not aware of opportunities outside of his current situation, and whose internet searches reflect this. He may therefore not receive publicity about, say, educational opportunities that would benefit him, but rather ads and search results that reflect his current reality. With the internet, ostensibly a window to the world at large, reinforcing his very specific, limited view of the world, he may never learn about such opportunities, or come to believe that they are just too foreign to him to be of interest.

Yet a common perception nonetheless exists that while internet users superficially complain about privacy loss, they in fact appreciate the benefits of data collection. According to a 2012 Pew study, there may be some truth to that idea, though the situation is more nuanced than that. 65

percent of respondents reported that they disliked targeted advertising because it could potentially limit their search results, 73 percent felt that targeted advertising was an invasion of privacy, and 68 percent simply did not like the idea of being tracked. The corresponding views in favor of targeted ads were only 29, 23, and 28 percent respectively. However, at the same time the overall opinion of search engine performance was extremely high, with 91 percent claiming to always or almost always find the information they wished to find. The majority of respondents also found that over time, their search results had become more relevant, with only 7 percent finding the results less relevant than previously (Madden and Smith).

If the privacy concerns are so prevailing, why, then, do internet users engage nonetheless in the very behaviors they should logically be avoiding? Part of the answer may lie in a kind of informal cost-benefit analysis that internet users employ when visiting a site. If the site offers them something of sufficient value to them in exchange for personal information, they may readily part with this data. However, even when users are aware of privacy concerns, at times the steps necessary to ensure them make other activities difficult or impossible to perform. Aol mail, for example, will not open when the privacy setting is set above medium high (a full two rungs below the maximum privacy). Since e-mail is an essential part of communication, the user is not left with much of a choice. Similarly, it would be absurd to advise anyone who is troubled by privacy to simply not use a search engine.

Yet it is also possible that many are simply ignorant of the full extent of internet tracking. For instance, the percentage of people who are knowledgeable enough and concerned enough to take precautions against standard cookies is high: when considering both people who install cookie-inhibiting anti-virus software and the number of people who manually delete cookies, the number is nearly 60 percent. However, most users, according to J.C. Sipior et. al., are not even aware of the existence of flash cookies, a far more invasive type of cookie (Sipior et al.). This is not surprising, as data aggregation, as the process of compiling personal information is formally known, is often done invisibly, and without a user's consent, or even awareness. While social media sites such as

Facebook are often popularly viewed as the main source of personal information useful to advertisers, they are in fact not responsible for the majority of it. Information gleaned from Facebook in fact accounts for only 14.6 percent of data aggregation (Andrews 19).

The majority of personal information is collected for marketing purposes, with over 85 percent of ad agencies making use of behavioral advertising in 2010, and by companies that the average internet users knows nothing about. The data aggregator Acxiom, for instance, was described by its former CEO as being “the biggest company you've never heard of” (Andrews 20). It collects both online and offline data in an attempt to compile as complete a profile of an individual as possible, for both marketing purposes and risk mitigation for companies, and is far from the only company to engage in this practice, competing with other aggregators such as Rapleaf and Choicepoint. Acxiom stores an average of 1500 pieces of data on each person, including social security numbers, driver’s license information, and credit card purchases, in addition, of course, to online activity. While hacking and fraud has occurred among these companies resulting in personal information leaking to disreputable sources, there are nonetheless protections in place to keep information from being indiscriminately spread (Andrews 20).

Other sites, while not having as detailed information as, say, Acxiom, are far less discriminating about who views the information they compile. Profiles on PeekYou- whose stated goal is to have a “comprehensive directory of all Internet users that tracks every individual's online presence” (Andrews 41), and Spokeo can be viewed by any internet user (Andrews 9-11). The advertising company NebuAd used similar practices, employing deep packet inspection to track every online transaction (Andrews 19), and though it is now defunct, other companies using the same technology have taken its place (Andrews 45).

Innovators in social media may make sweeping claims about a changing social climate in which privacy is no longer valued, or is an outdated, repressive trait needing to be overcome, but this obscures the fact that most internet users have no conception of the degree to which their information is public. They can therefore hardly be called willing participants in, or proponents and proof of, this supposedly changing value system. For example, in a Consumer Reports poll it was found that 61 percent of Americans were certain that their online actions were completely private. When told of the existence of data aggregation companies, 70 percent wanted them to be heavily fined for taking information without consent (Andrews 21). Some data aggregators allow users to opt-out of information sharing, yet when most internet users do not even know of the existence of data aggregators, they cannot realistically be expected to take advantage of this option (Andrews 58).

Interestingly, those who are very familiar with and knowledgeable about the internet do exhibit a strong concern regarding privacy. A University of California survey in 2010 found that young people ages 18-24 were actually quite concerned about privacy, with 88% saying that there should be a law requiring websites to delete information after a certain period of time (Holson). Young people between the ages of 18 and 29 are also the group most aggressively involved in online reputation management, and are the most vigilant in the use of online privacy controls. Additionally, the younger generation is the only age group currently more likely to limit information sharing than in previous years (the older age groups have become more willing to share than in previous surveys). The younger generation, however, also has a much higher incidence of posting information, and later regretting it. Also, this age group generally posts far more personal information online than do older age groups, and thus the higher use of privacy settings may simply be relative, and may be out of necessity. This is in fact not surprising, as the survey also found that the most visible online users are- perhaps surprisingly- the ones most selective about what they share (Madden and Smith).

However, this data does not imply that Mark Zuckerberg's oft-quoted comment about privacy no longer being a social norm (pamorama.net) can be dismissed offhand. Value systems do not remain static, and perceptions, like technology, do change in time. The question is probably not one of *whether* there is a change in privacy values, but *to what degree* values have changed.

A Pew study conducted every two years since 2004 addresses this very question. Leading experts in media were asked, based on their experience and observation, if “digital natives”, that is, those who had grown up with technology, would in time outgrow the need for widespread sharing of personal information. In other words, they wished to know whether sharing was merely a passing fad which time would change, or if society's perception of privacy had fundamentally shifted.

In the 2010 study, of the nearly 900 “technology stakeholders and critics” interviewed, the majority believed that the digital natives, or “millennials” would not outgrow the need to share information, and would continue doing so into their childbearing and mature years. The explanations as to why this would occur varied, of course, according to the responder, yet a strong common theme did emerge among many responders: it was not ignorance of the consequences that led millennials to share information, but rather a difference in social values (Anderson and Rainie 2010).

In an earlier study, one interviewee, Brian Trogdon, president of First Semantic, likened it to the manner in which tattoos, once viewed as a sign of- if not a reason for-societal rejection, are now commonplace and accepted (Anderson and Rainie 2008). The same theme continued to be present two years later, with responses such as networks specialist Steve Boyd's: “Publicy will replace privacy. Privacy will appear quaint, like wearing gloves and veils in church”. Some responses, however, were quite nuanced, like that of Andreas Kluth of The Economist, who, while agreeing that “over-sharing” would continue, predicted that as internet users age, they will share “more *banal* and less *intimate* information” (Anderson and Rainie 2010).

Among the respondents were those who saw distinct social benefits to the loss of online privacy. In contrast to Chris DiBona, an engineering manager at Google, who stated that he was “shocked” at what people shared online, and expected “employers and significant others” would be as well, Stephen Downs, a senior research officer at the National Research Council of Canada, believes that the loss of privacy will force us to become more forgiving. “It will be clear by 2020 that everyone has...skeletons...in the closet, and it will be seen as absurd to make morality judgments based on these” (Anderson and Rainie 2010).

Other respondents stressed that the changes in values were not due to age, but due solely to technology. Older internet users, they claimed, who became familiar with forms of new media were as likely to be comfortable sharing as younger ones. Doc Searls, fellow at Harvard's Berkman Center, also believes that technology has increased users' willingness to share, yet he believes that technology could also have the power to limit sharing in the future. He stated that the internet is still in its most primitive stages, and that excessive sharing is a result of individuals not yet having the technological tools with which to feasibly control the destination of their output. According to Searls, user-controlled privacy terms that take privacy out of the hands of the seller, and into the hands of the individual, will be the way of the future. Once this becomes a reality, he believes, sharing will once again become more cautious (Anderson and Rainie 2010).

As for myself, I willingly own up to a strong personal bias against marketing data aggregation. Not because I am frightened when Amazon.com offers me ads for my favorite type of food in restaurants at my price point and in my area (though that admittedly is more than a little creepy), but because I see the issue as inseparable from that of internet privacy at large. I believe that in an effort to increase sales, marketers and advertisers have unleashed a problem that is far beyond their control and their area of expertise, a problem which will have tremendous consequences in years to come.

With regards to marketing purposes specifically, I cannot help but think of- and side with- Immanuel Kant's categorical imperative when I object to data aggregation. His concept essentially states that no human may use another as merely a means to an end, and I strongly believe that people have the right to simply exist as people, not as commodities or means to a profit. Widely condoning business practices in which a person's every action can be seen as a potential profit reinforces our society's vision of other people as a means to an end, not as an end in and of themselves. Will these practices pay off monetarily? Certainly. But whether they are worthwhile in terms of the attitudes they will imprint on generations to come, is a harder question to answer.

Yet my main objections lie not in the marketing itself, but in the general impingements on privacy that I believe stem in large part from marketing efforts. In a way, I do like the idealism of those who say that privacy is a barrier to true communication, and something to be done away with. I see their point- in a perfect world, complete openness would only increase understanding between people, limit deceit and defamatory remarks, perhaps go so far as to promote a sense of human equality when even public heroes have no choice but to own up to previous misdeeds. But for a number of reasons, I am skeptical.

First, the push towards openness is hardly of popular origin. It has either been at the hands of corporations who track mainly without general consent or awareness of their doings, or at the hands of social media giants who gain immense power and wealth through loss of privacy. Perhaps I'm mistaken, but when I see a company advocating a practice that allowed it to amass 1.86 billion dollars in a single year, as Facebook's advertising did in 2010 (Andrews 9), I have to question its true motives. I also found Mark Zuckerberg's phrasing interesting in his explanation of the changes in Facebook's privacy policy during a videotaped TechCrunch interview with Michael Arrington. Though he began by describing his company as one that was attuned to and following evolving social norms, he eventually said the following "[w]e decided that these would be the social norms now and we just went for it" (pamorama.net). Did he merely misspeak under the pressure of having to talk spontaneously, or was it a Freudian slip?

Secondly, I don't think humans can be trusted to not harm one another with readily available, highly visible personal information. Predators (in the forms of individuals, hate-groups, or malicious governments) will always do their best to cause harm, even without detailed personal information on their victims. But I see no reasons to willingly aid them, and I think we are only deceiving ourselves if we deny that they exist now, will exist in the future, and will not be magically stopped by new-found "openness".

Also, I'm not convinced that information disclosure will be more egalitarian than any other area of life. I believe that here, too, there is a strong potential for the development of "haves and have-nots". People with more technological aptitude, time, and money, may in the future be able to control their information more effectively than those who lack the means, the knowledge, or the interest to do so, creating a new form of social divide.

I don't for a moment deny that shared personal information is valuable to companies, governments, and social circles, and can be used in positive and useful ways. But I believe that this is an area where we as a country and a society have to use caution to ensure that technology is being used to serve our best interests, rather than to merely exploit a new and poorly regulated area under the guise of social transformation.

Works Cited

Albanese, Andrew Richard. “Going Public: PW Talks with Jeff Jarvis.” *Publishers Weekly*. 7 Oct 2011 Web. 19 March 2012.

Anderson, Janna, and Lee Rainie. *Millennials Will Make Online Sharing in Networks a Lifelong Habit.* “Will Millennials Grow out of Sharing?” Pew Intenet. 9 July 2010. Web. 18 March 2012.

Anderson, Janna, and Lee Rainie. *The Future of the Internet III.* “Scenario 4: The Evolution of Privacy, Identity and Forgiveness.” Pew Internet. 14 Dec. 2008. Web. 18 March 2012.

Andrews, Lori. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy.* New York: Free Press, 2011. Print.

Duhigg, Charles. “How Companies Learn Your Secrets”. *The New York Times*. 16 Feb. 2012. Web. 21 Feb. 2012.

Fox, Susanne. “Trust and Privacy Online: Why Americans Want to Rewrite the Rules.” Pew Internet. 20 Aug. 2000. Web. 21 Feb. 2012.

Holson, Laura M. “Tell-All Generation Learns to Keep Things Offline”. *The New York Times*. 8 May 2010. Web. 21 Feb. 2012.

Madden, Mary, and Aaron Smith. “Reputation Management and Social Media”. 26 May 2010.
Web.

19 Feb. 2012.

Pamorama.net. *Zuckerberg Video Clip*. 8. Jan. 2010. Web. 21 March 2012.

Privacy Policy. *Google.com*. Effective 1 March 2012. Web. 25. Feb. 2012

Scott, David Meerman. *The New Rules of Marketing and PR, 3rd Edition.* Hoboken: Wiley, 2011. Print.

Sipior, Janice C., Burke T. Ward, and Ruben A. Mendoza. “Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons". *Journal of Internet and Commerce* 10.1-16 (2011): n. pag. Web. 21 Feb. 2012.

Spangler, William E., Kathleen S. Hartzel, and Mordechai Gal-Or. "Exploring the Privacy Implications of Addressable Advertising and Viewer Profiling." *Communications of the ACM* 49.5 (2006): 119-123. Web. 21 Feb. 2012.