Social Media Scanning: The Next Generation Privacy Threat?

- -
- Aa
- +

- **Author**Nikki Williams
- **Published** Wednesday, November 26th, 2014
- **Comments**0
-

Advertisers have always tried to get into the minds of the masses in order to sell more products. Demographic studies, focus groups, phone surveys and observation were the primary tools prior to the advent of Internet technology. But in late 1990s, the boom of online shopping on the worldwide web changed the landscape of marketing psychology by giving advertisers a new ability to track consumer habits through page visits, search fields, and online comments. In the past, consumers would agree to be tracked in exchange for a prize or discounts on shopping. In the present day, some retailers still offer loyalty card discounts to give their marketing folks an in-depth look at your shopping habits. But that's a far cry from the way the newest web-reliant data collection technologies can peer into your personal habits to build a profile.

Although consumer information discovery has always had its detractors, a newly developed data technique, social media monitoring, troubles many consumers and watchdog groups alike. Typically, social media monitoring is described as collecting or "scraping" available information about Internet users from sites like Facebook, Twitter, YouTube, Tumblr, discussion boards, blogs and more. Companies are keen to access this type of material because it offers a snapshot of the consumer when he is unaware of scrutiny, offering the most authentic customer opinions. Cheaper and less cumbersome than research methods like surveys and focus groups, social media monitoring has become a panacea to companies in today's highly competitive economic environment.

Unlike older methods of monitoring such as loyalty cards, social media scanning catches many consumers off-guard. According to a survey by Consumer Action, half of the individuals polled thought that such tracking was illegal, and more than a third are unaware of the extent of online tracking. Given those numbers, it's probably safe to say that most people are not expecting the level of data depth that Ditto Labs' software, the newest entry into the online tracking world, can offer marketers. Ditto Lab's unique software analyzes photos from social sites using background detection and geocoding information. The program can identify the photo location and can also analyze faces and assign them a "facial mood score" (FMS) to determine the emotion being portrayed in the shot. In addition, logo detection capability is provided to discern if there are any branded items in the picture. With the ability to scan for up to 2,500 items in every photo, Ditto Labs' product can give marketers a detailed outline of a person's daily habits, inclinations, and travels.

But does this actually impact your privacy? Scanning your private photos for clues about what you're eating or drinking, what activities you like and whom you hang out with certainly seems invasive. But the fact is, even code from Facebook's "Like" button and Twitter's "Tweet" can associate your identity with websites you've visited, giving marketers a look at your online habits. In truth, many data collectors view social media posts as public and not subject to privacy considerations. They further contend that if the data collected is for a group of individuals that are not personally identifiable then there is no invasion of privacy, even though it may "feel" like it to many people. Their primary argument is that the information collected is anonymous. As defined by the Federal Trade Commission (FTC), "anonymous" in the online data collection world means that there was no access to PII (personally identifiable information). Unfortunately, the new software by Ditto, as well as other emerging technologies, can harvest PII. Personal information is being collected and shared, regardless of what data collectors claim. For example, Facebook gives information on users who click a "Like" button to advertisers, LinkedIn sells information about everything you click on to other users of the site, and firms who purchase user information from Twitter sell it to analytics firms.

A definite ethical problem also occurs when companies spy on social media sites to tailor pricing to individual customers using geolocation. In the social media world, one's location can be quite easy to track with apps like Four Square on Facebook and the location feature on Twitter. Ditto Labs' software can take geolocation on-the-fly, finding you as you post pictures from your grandma's house at Thanksgiving, the Riviera on vacation, or your hotel on your latest business trip. The Wall Street Journal found many large retailers such as Home Depot, Staples, Rosetta Stone and Discover Financial Services offered discounted or inflated prices depending on customers' online habits and physical location. This locational profiling results in what economists term "price discrimination" and offers retailers a perceived unfair advantage, allowing them to discern customer loyalties and willingness to spend in advance of offering a price. For example, a consumer located in a large metropolitan area where prices are relatively high will be more likely to buy an online item at an inflated price than someone from a geographic area with a lower cost of living. Online companies can tailor their prices to each consumer based on their social media-based location.

Another issue is that companies that collect data through social media can combine that data with court records, income data and tax records on individual consumers to get an identifiable profile. This industry, called data brokering, is growing by leaps and bounds and is rife with duplicity. An appeal for transparency and accountability by the Federal Trade Commission (FTC) investigation resulted after investigators found that "data brokers collect and store billions of data elements covering nearly every U.S. consumer."

Even more concerning was the unanticipated uses of data collection. The FTC noted that, although the category of "biker enthusiasts" might enable a motorcycle manufacturer to offer discounts to bikers, it can also be used by life insurers to flag consumers that exhibit risky behavior. Data of this type is considered a gray area for groups who gather data from social media sites using software like Ditto's current offering.

Software of this sort, with its ability to peer into the everyday activities of ordinary people, opens the door to some pretty significant privacy issues. Perhaps most notable is the question of whether government or law enforcement agencies are using this amped-up scanning software to find or track persons of interest. Based on my research, the answer is a resounding "yes". One social media analysis firm, Snaptrends, presents evidence that these type of scanning systems are already in action. The Guildford County Sheriff's Office in North Carolina patrols social accounts to locate parties and have used this information to charge over 230 teens with alcohol and drug related offenses. It's a booming market—there are various companies that sell social media scanning software directly to law enforcement agencies. For example, one product, BlueJay by BrightEvents, is used by many police departments to scan tweets for location and download instant photographic evidence during a disturbance. Using even more sophisticated scanning products, like Ditto's, could give these agencies an insidious and possibly deleterious influence on casual social interaction. Besides the obvious problem with this kind of "stalking" by the authorities, there is the question of what effect this online observation will have on an individual's perceived freedom of speech. As a practical matter, it would make it easier to have a jesting conversation misconstrued to the detriment of both the online participants and the authorities.

Much of the "creepiness" of social media scanning software like Ditto's derives from evidence that it identifies individuals, rather than groups of subjects, in stunning detail. An email to Ditto asking whether their software aggregated or individualized information resulted in a response centered on the fact they exclusively analyze public information on social media sites. They offered a link to an article to further explain their stance, but the article also fell short of a direct answer. Their position, which appears to be that anything in the public realm is fair game, was echoed in the words of their chief marketing officer, Mary Tarczynski. She notes that Ditto is, "looking at public photos, so anyone who wants to keep their information more private certainly has ways to share things just with their friends without [the photos] being available to Ditto." In other words, batten down the privacy filters or prepare to be "scraped."

For their customer, Kraft Foods, Ditto Labs uses software to detect patterns in behavior, such as what drink people like best with their macaroni and cheese dinner and where they are eating. Based on photo location and content, Ditto then categorizes photos into groups such as "foodies" and "sports fans." It's not evident what happens with the data next, but it is clear that some organizations misuse the information they receive, regardless of their promise to protect it. For example, one marketing analytics startup, Piqora, was found in violation of Pinterest's rules of image use for the practice of collecting competitor's photos in a graphical dashboard and keeping them indefinitely. So, perhaps the problem is not scanning software per se, but what marketing teams are doing with information gleaned from it.

The long and short of it is, if you don't want marketers analyzing your social media images you might want to forgo posting on social media. Even if you are proactive and read up on your social media sites' privacy policies, much of the language is ambiguous or non-existent, making it difficult for social media users to understand. A recent Wall Street Journal article addresses the fact that third-party usage of posted photos is not correctly noted in many sites' privacy policies. They also don't address the practice of caching (storing images or posts) in their guidelines and many use nebulous language like "reasonable periods" to define how long developers can store photos. Even when rules are clear, some companies find a loophole or just ignore them. Companies can have any number of policies, rules and regulations, but if they choose to violate or ignore them, your information will be up for grabs.

It is apparent that data obtained through scanning software is susceptible to misuse. Despite mobile marketers' assertions of self-regulation through organizations such as the

Digital Advertising Alliance, it is plain that once your information is out there, it can be used to assemble a personal profile and aggressively market you or even be sold to a third party. The FTC makes an attempt at consumer protection by recommending that individuals have access to collected data and are allowed opt-outs from sharing. They also seek to require companies to inform consumers that inferences are being drawn from raw data about them and allow them to correct false data. In regard to sensitive data, such as health information, the FTC affirms that there should be a written consent before it is collected and shared. Regardless of their assertions, the FTC has only developed guidelines, not provided legally enforceable measures—it is clear that consumers whose photos are audited by Ditto Labs are not aware of the scrutiny.

Until there are detailed laws regarding social media scanning, the pictures you post might give clues to your brand loyalties, health, food preferences, marital status, leisure activities, family status and more. Even with legislation in place, you can't rely on businesses to treat your information appropriately. Scanning software that can check your online posts for evidence of alcohol, cigarettes, prescription (or other) drugs, brand preferences and lifestyle choices can give a frighteningly candid picture of your lifestyle, perhaps to your detriment. Many marketers and businesses hide behind the current trend that makes anything in the public realm fair game. But the deeper issue is the expansion of what comprises public space. Legislative organizations need to scrutinize and, perhaps, redefine "public" to exclude those online social spaces that are used for intimate exchanges among invited users so individuals can feel free to be their authentic selves without fear of leaving traceable personal details.

Nikki B. Williams is a freelance writer based in Houston, TX. She has written for a variety of clients from the Huffington Post and D.C.-based political action committees to Celtic jewelry designers in Ireland. You can contact her through her website nikkibeewilliams.com.