THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (800) 668-6481 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

Intellectual Property

Facebook data sweep raises legal and ethical issues

By **Sharon Bauer**

Sharon Bauer

(April 9, 2018, 9:37 AM EDT) -- Privacy law has been in the spotlight following the reveal of the Facebook/Cambridge Analytica scandal, raising important legal and ethical issues. Corporate entities, which advertise on social media or collect data through online tools, need to be apprised of the ever-changing legal framework around these practices.

There is no doubt that online tools make our lives more convenient. Amazon tells us when we need more paper towels. Google Maps gives us with directions when we get in our cars. Instagram allows us to peek into our friends' lives without having to talk to them. Facebook conveniently allows us to get news, games, photos and music all in one place. As it turns out, the more personal information these online tools have about us, the more convenient and personalized the experience becomes. If convenience is the product, then our privacy is the currency.

As we use these online tools, we leave data crumbs trailing behind. Data companies sweep up these data crumbs, analyze them and reassemble them to create a digital copy of ourselves. Through machine learning and sophisticated algorithms, data companies predict intimate details about our digital selves, even when we have consciously decided not to share such details. By deconstructing and analyzing our subconsciousness, these companies can influence the way we think, feel and behave. They can also increase our dependency on these tools. When was the last time you went to the washroom without your phone?

So how much privacy are we willing to give up for convenience? Any hesitation we experience, if only for a brief second, before accepting terms and conditions for an app is overshadowed by its convenience. If we actually understand what we are giving up, to whom and the consequences of allowing data miners to surveille us, then we might think twice about accepting those terms and conditions.

Collecting and analyzing data for the purpose of influencing consumers is not a new concept. Historically, marketers and political campaign leaders have relied on demographic profiling to influence groups of people. Demographic data includes, among other attributes, age, sex, social class and religion.

Data miners and marketers have moved beyond demographic profiling. Our online activities, including our "likes," our friends, our shopping lists and even our heartbeat reveal our psychological traits and values. By collecting data on our psyche, data miners, such as the now infamous Cambridge Analytica, understand how we think, how we feel and how we can be influenced. Marketers can now use psychographic data to micro-target ads and influence our emotions and behaviour.

Facebook, being the largest social media network, provides a host of services for its users. Through the use of these services, data miners and marketers collect personal data about Facebook users and their friends. Perhaps even more valuable are the over 52,000 attributes which Facebook uses to tag its users. Some of these attributes are as obscure as "pretending to text in public." By categorizing its users, Facebook makes it easier for marketers to reach their desired audience, saving them money. It also allows them to tailor their ads based on the psychographic data they have on a particular group of users. While psychographic data can lead to positive results for marketers, it can lead to questionable outcomes for Facebook users.

ProPublica, a non-profit organization made up of investigative journalists, investigated microtargeting advertising on Facebook. Its investigation revealed that, in addition to choosing user attributes to target ads and news, marketers can intentionally exclude users from seeing their ads based on their attributes. The 52,000 user attributes include various "ethnic affinities" such as Hispanic ethnic affinity, African-American ethnic affinity and Asian ethnic affinity.

It is worth noting that an ethnic affinity does not necessarily correlate to one's ethnicity. Rather it directly relates to a user's activity on the social media platform. A user may be placed in the Hispanic ethnic affinity because, based on an algorithm, the user either has Hispanic friends or likes things or topics associated with Hispanic ethnicity. Users do not know what attributes they are placed in nor can they request to be removed from them.

As part of its investigation, ProPublica placed a housing ad on Facebook and chose to exclude Hispanic and African-American ethnic affinities. The ad was approved by Facebook. It is not difficult to see how excluding users grouped within an ethnic affinity is discriminatory. A lawsuit was recently filed against Facebook by fair housing groups for allowing companies to illegally tailor their ads on the basis of race, sex, gender, religion, etc.

Facebook explains that the process of excluding groups of people from ads is known as "exclusion targeting" and is common practice in marketing. It allows marketers to target its intended audience. According to Facebook, their ad policy prohibits advertisers from targeting in a discriminatory manner. Ads must comply with the law. They argue that excluding an affinity is not discriminatory as it is an affinity and not actually an ethnicity. Facebook, which self-regulates, claims it takes quick action when ads do not conform with its policy.

But how effective are they at self-regulating? Mark Zuckerberg, CEO of Facebook, admitted Facebook made mistakes in enforcing its own policy. He also suggested, "I'm actually not sure we shouldn't be regulated." Zuckerberg was more adamant about having regulations around digital advertising; similar to the regulations in place for ads on TV and print.

As users who give up our privacy, we need robust regulations and regulatory enforcement of online platforms with strict monetary penalties. The *General Data Protection Regulations* (GDPR), a comprehensive set of privacy regulations coming into force in Europe this spring, provides for this. The GDPR suggests that *we,* the users of online tools, are the owners of our data and are therefore free to decide what data to share, with whom and when to take it back. *We* need to set the terms and conditions.

The GDPR mandates that online tools, such as social media platforms, be transparent with the way they handle our personal data. They must seek unprecedented user consent in order to collect, use and share user data. Users will also have the ability to revoke consent, have access to all their data and a right to erasure. While Facebook is bound by the GDPR for users in the EU, it claims it will extend the GDPR privacy protection beyond the EU borders.

The convenience of online tools and our dependency upon them make it difficult of us to stop using those tools, despite feeling violated. If we cannot remove ourselves from the digital world, we should demand transparency as we lay out the law of the digital land. We should be *users* of social media, not be *used* by social media.

Sharon Bauer is a partner at Wolfe Lawyers *and can be reached at* sbauer@wolfelawyers.com.

Photo Credit / filo ISTOCKPHOTO.COM