California Management Review

ETHICS

Facebook, User Privacy, and Data Responsibility

by David Salisbury

With great power comes great responsibility. Despite public outrage and Congressional hearings over the Cambridge Analytica scandal, Facebook's profits and user numbers continue to soar. Can Facebook strike a balance between transparency and responsibility around personal data?

INSIGHT | NOTE 30 Apr 2018

With great power comes great responsibility. Boasting a usership of 2.2 billion people, Facebook has had to learn the hard way that selling the data of 87 million users for financial gain is not acceptable. Phone numbers, email addresses, political affiliation, pictures of every meal you've had – all common items users of the social platform share with seemingly little concern for who will see it other than their immediate circles. While

Facebook certainly deserves to answer why this breach of user privacy was allowed, users of online platforms should also consider why they assumed private information they willfully submitted into cyberspace had any guarantee of privacy.

It Takes Two

As business, commerce, and ways we connect move increasingly online, it's imperative for companies to strike a balance between the need to reach audiences (usually through ads and marketing) and generate revenue, while ensuring their consumers have desirable and positive online experiences. Additionally, with so many outcries of foul play in the 2016 presidential election, of increasing concern is a platform's efforts to ensure acquired data is not being used to manipulate their users for unethical business/political gains. It is possible for businesses and consumers to do a better job of striking that balance through shared responsibility. Adblock Plus, a major content-filtering and ad blocking extension that over 50 million internet users downloaded by 2009 for ad-free browsing, provides one such example. A recently published Berkeley Haas case study, Eyeo's Adblock Plus, looks into how the extension's popularity directly hurt companies relying on advertising for growth and sustainability. In 2011 Adblock Plus established "Acceptable Ads" guidelines as a compromise: advertisers can get their content through the filter with less-disruptive and covert ads, and users are ensured a more desirable online experience.

Corporate Responsibility

There is an assumed right to privacy people expect when using social media sites. If there's a lesson Facebook and other sites should learn from this debacle, it's that customers are demanding increased transparency on what data gets shared and with whom. Facebook not only admitted they sold their data willfully to analytics firms, but that they did not monitor what firms it went to. If they hope to keep a loyal client base that trusts their product, changes are necessary. That being said, Facebook's shares, profits, and number of users continue to increase, seeming to roll the litany of recent scandals off its massive shoulders.

There is evidence that people don't mind being marketed to if it's catered to their personal preferences. A recent marketing research study found only eight percent of respondents said they didn't want to receive any marketing from brands and retailers, while each respondent cited a preferred way of discovering new products. Millennial audiences brought up on social media seem to be more willing to share information than previous generations, and likewise prefer advertising geared towards them to inform them what products are available. Specifically, they don't want to be bombarded with non-relevant ads, but are more open to receiving ads that create a conversation of sorts with the businesses and political factions they are interested in.

Facebook has taken steps to ensure better data security, including the removal of third-party data sources like Cambridge Analytica, requiring political advertisers to provide increased transparency, and vowing to apply the European Union's General Data Protection Regulation. Though the company is right to put users' minds at ease with these proactive measures, users themselves must also look at what information they are giving to Facebook to begin with.

Personal Responsibility

Data security is not solely on the shoulders of business. Often when you click on a new game or invitation to take a personality quiz, you're asked if it's okay for the app to share your Facebook information. By clicking "yes", you're risking everything you've shared online being given to some unknown entity who's intentions for your data are very possibly not to your benefit. This may be how Cambridge Analytica gained your information; so in an online world of unknowns, you should consider protecting your data as much as possible. It's a good idea to get rid of old apps you've granted access to your account in the past and begin monitoring what apps you allow on your account in the future. You should also manage your ad preferences to not allow Facebook to send you targeted ads. Begin using private monitors with "intelligent tracking protection," and configure your privacy settings so that "friends only" can see what you post.

Of course at the end of the day, one of the appeals of social media is to share one's life and experiences with people en masse, opening communication beyond daily, face-to-face borders. As such, it would seem social media has the inherent risk of people's personal information landing in the hands of audiences they don't know. "Liking" Avicii and David Guetta's fan pages may result in your getting ads for every EDM festival, clothing line, radio show, etc. who rely on target data to find their market, and you have some responsibility for publically providing that information. Users should understand the possible consequences of putting their personal information online and how they can better secure it. And if you don't want certain, highly-sensitive aspects of your life known anyone outside your immediate circles, you may want to consider whether you share it online at all. Abstinence is the only 100% protection after all.

The Future is Listening

There are lessons for all to learn here. Large companies must design ethical frameworks to use its customer data respectfully and more responsibly. Consumers should make an effort to better understand the ways data can move through online channels and learn the risks sharing their personal information. And perhaps most importantly, in this rapidly progressing online world, companies and consumers must listen to each other in order to strike a balance that will see the modern tech age into a more peaceful co-existence.

David Salisbury Follow

David Salisbury is an Editorial Associate at California Management Review / Berkeley Haas Case Series. He holds a BA in Communications from Michigan State University and has worked six years in the San Francisco Bay Area tech industry. He is also an accomplished filmmaker and musician.