Case Study: The Power and Politics of Privacy on Social Networking Sites

Facebook, with an estimated 1.6 billion monthly active users worldwide, SnapChat, with 150 million active users across the globe, and Twitter, with more than 310 million monthly U. S. users, are three of the most popular social networking sites around the world. These companies state that they do not distribute users’ information to third parties. However, advocacy groups concerned about online privacy rights and some users are increasingly wary about how these and other networking sites might be using and whether they are adequately protecting personal information. A common source of discomfort is whether users’ personal information will be used to generate targeted ads directed at them. A recent manifestation of this wariness occurred in 2009, after Mark Zuckerberg, CEO of Facebook, quietly changed the terms of use that govern how and for how long Facebook can use users’ information posted to the popular website. About two weeks later, the consumer-advocacy blog Consumerist.com highlighted that the change in user policy would allow Facebook to continue to use information posted by users for marketing, promotional, or other purposes even after users had deleted the information from their Facebook accounts. Consumerist.com stated that the change in policy would allow Facebook to do anything it wanted with posted content, for as long as it wanted (even after a user closed his or her Facebook account). Following this realization, many users and consumer privacy advocacy groups railed against the change in terms of use at Facebook. Presumably as a result of the public’s reaction, Zuckerberg declared two weeks after the initial change that the company would return to its original terms of use while the feedback was analyzed. Zuckerberg announced that the company would work on a major revision of the terms and invited users to provide ideas on its website: “Facebook Bill of Rights and Responsibilities.”

This wasn’t the first time that Facebook experienced problems related to user privacy. In November 2007, Facebook launched an advertising program, Beacon, that was developed to track the purchasing and other activities of Facebook users on 44 websites and then send notifications of these activities to the users’ friends on Facebook. For example, if a user made an online purchase of a book on one of the 44 websites, this would act as an indirect referral to his or her friends on Facebook, which might spur additional purchases of the book. The problem started when a senior research engineer from a Palo Alto–based antispyware company, CA Inc., discovered that Beacon was also “tracking the activities of both members and nonmembers on Facebook and partner sites.” Moreover, the program was set up in such a way that a message would be sent to a user’s friends automatically unless the user figured out how to change his or her preferences on the Facebook website. Within two months of rolling out the Beacon software, CEO Zuckerberg apologized for how the rollout was handled and took steps to increase users’ privacy related to their activities on the partner sites.

Zuckerberg is at the cutting edge of the intersection between technology and online privacy. In a recent blog post, he complained that his Facebook users can be inconsistent; on one hand, they want continually expanded services (e.g., more relevant ads and information about their friends), but on the other hand, they expect that their privacy will be protected and their information will not be shared with outside advertisers and third parties. The battle over online privacy does not stop with social networking websites in the United States. Social network users in the 28-nation European Union are protected by strict privacy laws. The regulations “require websites to warn users of privacy risks and limit the sites’ ability to target advertising based on members’ race, religion or other sensitive categories.” In the United Kingdom, privacy activists have reacted to Google’s announcement that it would use “behavioral targeting” to generate display advertising when search results appear on users’ screens. And the British government recently announced it awarded contracts to seven companies to monitor social media platforms including Facebook, Twitter, LinkedIn, and other blogs to track keywords, hashtags, and phrases used on these sites—particularly during “crisis situations” or events of heightened public interest. In sum, the debate over online privacy is not going away anytime soon. Several politically influential and powerful stakeholders with different priorities have a stake in the outcome: Users want their personal information protected; social networking companies want to use personal information to generate advertising revenue; advertising firms want to target their products/services to specific market segments; privacy advocacy groups want to limit the disclosure of users’ personal information; technology companies want to facilitate greater information sharing; and governments want to monitor networking websites for signs of malevolent activities.