Facebook Privacy: Your Life for Sale

CASE STUDY

Facebook describes its corporate mission as giving people the power to build community and bring the world closer together. In 2017 and 2018 these lofty objectives took a serious blow when it became known that Facebook had lost control of the personal information users share on the site. Facebook had allowed its platform to be exploited by Russian intelligence and political consultants with the intention of intensifying existing political cleavages, driving people away from community and from one another during the U.S. presidential election of 2016.

In January 2018, a founder and former employee of a political consulting and voter profiling company called Cambridge Analytica revealed that his firm had harvested the personal information of as many as 87 million users of Facebook, and used this information in an effort to influence the U.S. presidential election of 2016. Facebook does not sell the personal information of its users, but it did allow third-party apps to obtain the personal information of Facebook users. In this case, a U.K. researcher was granted access to 50,000 Facebook users for the purpose of research. He developed an app quiz that claimed to measure users' personality traits. Facebook's design allowed this app to not only collect the personal information of people who agreed to take the survey, but also the personal information of all the people in those users' Facebook social network. The researcher sold the data to Cambridge Analytica, who in turn used it to send targeted political ads in the presidential election.

In a Senate hearing in October 2017, Facebook testified that Russian operatives had exploited Facebook's social network in an effort to influence the 2016 presidential election. More than 130,000 fake messages and stories had been sent to Facebook users in the United States using an army of automated software bots, built and operated by several thousand Russian-based hackers working for a Russian intelligence agency, the Internet Research Agency. (A bot is a software program that performs an automated task, and is often on the Internet for malicious purposes—see Chapter 8.) Using 75,000 fake Facebook accounts, and 230,000 bots, the Russian messages were sent to an estimated 146 million people on Facebook. The messages targeted people based on their personal information collected by Facebook in the normal course of business, including users' religion, race, ethnicity, personal interests, and political views. The ads targeted groups who had opposing political views, with the intention of intensifying social conflict among them.

How could all this happen? As it turns out, it was quite easy and inexpensive, given the design and management of Facebook. Once Facebook grants access to advertisers, app developers, or researchers, it has a very limited capability to control how that information is used. Third-party agreements and policies are rarely reviewed by Facebook to check for compliance. Facebook executives claimed they were as shocked as others that 87 million Facebook users had their personal information harvested by Russian intelligence agencies and used by Cambridge Analytica to target political ads.

It gets worse: In early June 2018, several months after Facebook was forced to explain its privacy measures and pledge reforms in the wake of the Cambridge Analytica scandal, the *New York Times* reported that Facebook had data-sharing partnerships with at least 60 device makers. Facebook allowed Apple, Samsung, Amazon, and other companies that sell mobile phones, tablets, TVs, and video game consoles to gain access not only to data about Facebook users but also personal data about their friends—without their explicit consent. As of 2015, Facebook had supposedly prohibited app software developers from collecting information about customers' friends. Apparently, these restrictions did not extend to device makers.

Shortly thereafter, it was also revealed that Facebook had struck customized data-sharing deals that gave select companies such as Royal Bank of Canada and Nissan Motor Co. special access to user records, even though Facebook claimed it had it walled off that information in 2015. Certain companies were also allowed access to additional information about a user's Facebook friends.

Facebook again came under attack from the press, privacy advocates, and government authorities for pleading ignorance and for allowing uncontrolled data sharing to happen. For the first time since its founding, Facebook is facing a serious existential crisis, and potentially a threat to its business model. Facebook's current crisis follows from a history of privacy abuses

in its short 14-year life. Facebook has quickly morphed from a small, niche networking site for mostly Ivy League college students into a publicly traded company with a market worth of $534 billion in 2018. Facebook boasts that it is free to join and always will be, so where's the money coming from to service 2.1 billion worldwide subscribers? Just like its fellow tech titan and rival Google, Facebook's revenue comes almost entirely from advertising (97 percent of $40.6 billion in revenue in 2017). Facebook watches what you do on Facebook and then sells that information and information about your friends to advertisers, not just on Facebook but all over the web. As Tim Cook, CEO of Apple, noted, at Facebook, the product they sell is you.

More than ever, companies such as Facebook and Google, which made approximately $110 billion in advertising revenue in 2017, are using your online activity to develop a frighteningly accurate digital picture of your life, and then selling access to their platform of personal information to advertisers. Facebook's goal is to serve advertisements that are more relevant to you than anywhere else on the web, but the personal information it gathers about you both with and without your consent can also be used against you in other ways.

Facebook has a diverse array of compelling and useful features. It has helped families find lost pets and allows active-duty soldiers to stay in touch with their families; it gives smaller companies a chance to further their e-commerce efforts and larger companies a chance to solidify their brands; and, perhaps most obviously, Facebook makes it easier for you to keep in touch with your friends, relatives, local restaurants, and, in short, just about all the things you are interested in. These are the reasons so many people use Facebook—it provides real value to users. The cost of participating in the Facebook platform is that your personal information is shared with advertisers and with others you may not know.

Facebook has a checkered past of privacy violations and missteps that raise doubts about whether it should be responsible for the personal data of billions of people. There are no laws in the United States that give consumers the right to know what data companies like Facebook have compiled. You can challenge information in credit reports because of the Fair Credit Reporting Act, but until recently, you could not obtain what data Facebook has gathered about you. It's been different in Europe: for several years, users had the right to demand that Facebook turn over a report of all the information it had collected on individuals. In 2018, Facebook allowed users to download all the information they had collected on a person, even though users had no legal right to demand that information.

Think you own your face? Not on Facebook, thanks to its facial recognition software for photo tagging of users. This "tag suggestions" feature is automatically on when you sign up, and there is no user consent. A federal court in 2016 allowed a lawsuit to go forward contesting Facebook's right to photo tag without user consent. This feature is in violation of several state laws that seek to secure the privacy of biometric data.

A *Consumer Reports* study found that among 150 million Americans on Facebook every day, at least 4.8 million were willingly sharing information that could be used against them in some way. That includes plans to travel on a particular day, which burglars could use to time robberies, or Liking a page about a particular health condition or treatment, which might prompt insurers to deny coverage. Credit card companies and similar organizations have begun engaging in weblining, taken from the term *redlining*, by altering their treatment of you based on the actions of other people with profiles similar to yours. Employers can assess your personality and behavior by using your Facebook Likes. Thirteen million users have never adjusted Facebook's privacy controls, which allow friends using Facebook applications to transfer your data unwittingly to a third party without your knowledge.

Why, then, do so many people share sensitive details of their life on Facebook? Often, it's because users do not realize that their data are being collected and transmitted in this way. A Facebook user's friends are not notified if information about them is collected by that user's applications. Many of Facebook's features and services are enabled by default when they are launched without notifying users, and a study by Siegel + Gale found that Facebook's privacy policy is more difficult to comprehend than government notices or typical bank credit card agreements, which are notoriously dense. Did you know that whenever you log into a website using Facebook, Facebook shares some personal information with that site and can track your movements in that site? Next time you visit Facebook, click Privacy Settings and see whether you can understand your options.

However, there are some signs that Facebook might become more responsible with its data collection processes, whether by its own volition or because it is forced to do so. As a publicly traded company, Facebook now invites more scrutiny from

investors and regulators. In 2018, in response to a maelstrom of criticism in the United States, and Europe's new General Data Protection Regulation (GDPR), Facebook changed its privacy policy to make it easier for users to select their privacy preferences; to know exactly what they are consenting to; to download users' personal archives and the information that Facebook collects and shares, including facial images; to restrict click bait and spam in newsfeeds; to more closely monitor app developers' use of personal information; and to increase efforts to eliminate millions of fake accounts. Facebook hired 10,000 new employees and several hundred fact-checking firms to identify and eliminate fake news. For the first time in its history, Facebook is being forced to apply editorial controls to the content posted by users and, in that sense, become more like a traditional publisher and news outlet that takes responsibility for its content. Unfortunately, as researchers have long known, and Facebook executives understand, very few users—estimated to be less than 12 percent—take the time to understand and adjust their privacy preferences. In reality, user choice is not a powerful check on Facebook's use of personal information.

Although U.S. Facebook users have little recourse to access data that Facebook has collected on them, users from other countries have done better. In Europe, over 100,000 Facebook users have already requested their data, and European law requires Facebook to respond to these requests within 40 days. Government privacy regulators from France, Spain, Italy, Germany, Belgium, and the Netherlands have been actively investigating Facebook's privacy controls as the European Union pursues more stringent privacy protection legislation.

While Facebook has shut down several of its more egregious privacy-invading features, and enhanced its consent process, the company's data use policies make it very clear that, as a condition of using the service, users grant the company wide latitude in using their personal information in advertising. The default option for users is "opt-in"; most users do not know how to control use of their information; and they cannot "opt out" of all sharing if they want to use Facebook. This is called the "control paradox" by researchers: even when users are given controls over the use of their personal information, they typically choose not to use those controls. Although users can limit some uses of their information, an advanced degree in Facebook data features is required. Facebook shows you ads not only on Facebook but across the web through its Facebook Audience Network, which keeps track of what its users do on other websites and then targets ads to those users on those websites.

Critics have asked Facebook why it doesn't offer an ad-free service—like music streaming sites—for a monthly fee. Others want to know why Facebook does not allow users just to opt out of tracking. But these kinds of changes would be very difficult for Facebook because its business model depends entirely on the largely unfettered use of its users' personal private information, just as it declares in its data use policy. That policy states very openly that if you use Facebook you agree to their terms of service, which enable it to share your information with third parties. In 2019 Facebook has come under withering fire for knowingly violating UK privacy rules, and global lobbying against stronger data privacy laws.

Sources: Tony Romm, "Facebook 'Intentionally and Knowingly' Violated U.K. Privacy and Competition Rules, British Lawmakers Say," Washington Post, February 17, 2019; Carole Cadwalladr and Duncan Campbell, "Revealed: Facebook's Global Lobbying Against Data Privacy Laws," The Guardian, March 2, 2019; Deepa Seetharaman and Kirsten Grind, "Facebook Gave Some Companies Access to Additional Data About Users' Friends," *Wall Street Journal*, June 8, 2018; Natalia Drozdiak, Sam Schechner, and Valentina Pop, "Mark Zuckerberg Apologizes to EU Lawmakers for Facebook's Fake-News Failures," *Wall Street Journal*, May 22, 2018; Cecilia Kang and Sheera Frenkel, "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users," *New York Times*, April 24, 2018; Eduardo Porter, "The Facebook Fallacy: Privacy Is Up to You," *New York Times*, April 24, 2018; Jack Nicas, "Facebook to Require Verified Identities for Future Political Ads," *New York Times*, April 6, 2018; Sheera Frenkel and Natasha Singer, "Facebook Introduces Central Page for Privacy and Security Settings," *New York Times*, March 28, 2018; David Mayer, "Facebook Is Giving You New Privacy Options, But It's Clear What It Wants You to Choose," *Fortune*, March 19, 2018; Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *New York Times*, March 17, 2018; Georgia Wells and Deepa Seetharaman, "New Facebook Data Shows Russians Targeted Users by Education, Religion, Politics," *Wall Street Journal*, November 1, 2017.

CASE STUDY QUESTIONS

4-13 Perform an ethical analysis of Facebook. What is the ethical dilemma presented by this case?

4-14 What is the relationship of privacy to Facebook's business model?

4-15 Describe the weaknesses of Facebook's privacy policies and features. What management, organization, and technology factors have contributed to those weaknesses?

4-16 Will Facebook be able to have a successful business model without invading privacy? Explain your answer. Could Facebook take any measures to make this possible?