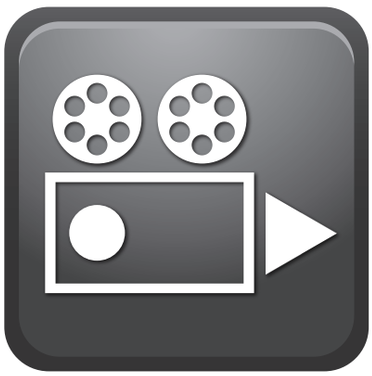
CHAPTER 4 **ETHICAL, SOCIAL, AND POLITICAL ISSUES IN E-COMMERCE**

CASE 2

Facebook and Google Privacy



SUMMARY The business model of many tech companies like Facebook and Google is to collect as much personal information on its users as is technically possible and then to sell that information to advertisers in the form of targeted advertising on Web sites and mobile apps, and on partner Web sites, who use the information to personalize ads. These videos provide some suggestions for how users can gain greater control over their personal information that they have placed online.

(a) Setting Facebook privacy controls

URL https://www.youtube.com/watch?v=IWlyut4zsko; L=4:21

(b) Google, Privacy and What It Means For You

URL https://www.youtube.com/watch?v=V7M_FOhXXKM; L=3:18

CASE In a 2010 interview, Mark Zuckerberg, the founder of Facebook, proclaimed that the "age of privacy" had to come to an end. According to Zuckerberg, social norms had changed and people were no longer worried about sharing their personal information with friends, friends of friends, or even the entire Web. This view is in accordance with Facebook's broader goal, which is, according to Zuckerberg, to make the world a more open and connected place. Supporters of Zuckerberg's viewpoint, including fellow tech titan Google, believe the 21st century is an age of "information exhibitionism," a new era of openness and transparency. However, times have changed, and in 2019 there are growing calls to put new limits on the personal information that Facebook, and Google, collect and provide to advertisers.

continued

Facebook has a long history of invading the personal privacy of its users. In fact, the very foundation of Facebook's business model is to sell the personal private information of its users to advertisers. In essence, Facebook is like any broadcast or cable television service that uses entertainment to attract large audiences, and then once those audiences are in place, to sell air time to advertisers in 30 to 60 second blocks. Of course, television broadcasters do not have much if any personal information on their users, and in that sense are much less of a privacy threat. Facebook, with over 2 billion users worldwide, clearly attracts a huge audience.

Although Facebook started out at Harvard and other campuses with a simple privacy policy of not giving anyone except friends access to your profile, this quickly changed as its founder Mark Zuckerberg realized the revenue-generating potential of a social networking site open to the public.

In 2007 Facebook introduced the Beacon program, which was designed to broadcast users' activities on participating Web sites to their friends. Class-action suits followed. Facebook initially tried to mollify members by making the program "opt in" but this policy change was discovered to be a sham, as personal information continued to flow from Facebook to various Web sites. Facebook finally terminated the Beacon program in 2009, and paid $9.5 million to settle the class-action suits.

In 2009, undeterred by the Beacon fiasco, Facebook unilaterally decided that it would publish users' basic personal information on the public Internet, and announced that whatever content users had contributed belonged to Facebook, and that its ownership of that information never terminated. However, as with the Beacon program, Facebook's efforts to take permanent control of user information resulted in users joining online resistance groups and it was ultimately forced to withdraw this policy as well. The widespread user unrest prompted Facebook to propose a new Facebook Principles and Statement of Rights and Responsibilities, which was approved by 75 percent of its members, who voted in an online survey. However, the resulting privacy policy was so complicated that many users preferred the default "share" setting to working through over 170 privacy options.

In 2009, Facebook also introduced the Like button, and in 2010 extended it to third-party Web sites to alert Facebook users to their friends' browsing and purchases. In 2011, it began publicizing users' "likes" of various advertisers' products in Sponsored Stories (i.e., advertisements) that included the users' names and profile pictures without their explicit consent, without paying them, and without giving them a way to opt out. This resulted in yet another class-action lawsuit, which Facebook settled for $20 million in June 2012. As part of the settlement, Facebook agreed to make it clear to users that information like their names and profile pictures might be used in Sponsored Stories, and also give users and parents of minor children greater control over how that personal information is used.

continued

In 2011, Facebook enrolled all Facebook subscribers into its facial recognition program without asking anyone. When a user uploads photos, the software recognizes the faces, tags them, and creates a record of that person/photo. Later, users can retrieve all photos containing an image of a specific friend. Any existing friend can be tagged, and the software suggests the names of friends to tag when you upload the photos. This too raised the privacy alarm, forcing Facebook to make it easier for users to opt out. But concerns remain.

In May 2012, Facebook went public, creating more pressure on it to increase revenues and profits to justify its stock market value. Shortly thereafter, Facebook announced that it was launching a new mobile advertising product that will push ads to the mobile news feeds of users based on the apps they use through the Facebook Connect feature, without explicit permission from the user to do so. Facebook reportedly may also decide to track what people do on their apps. It also announced Facebook Exchange, a new program that will allow advertisers to serve ads to Facebook users based on their browsing activity while not on Facebook.

In 2018 and 2019 Facebook's reputation for invading the personal privacy of its users took a turn for the worse when it was revealed that it had lost control of personal information on 87 million users to agents of the Russian government who had been able to use fake accounts and apps to target political ads designed to sway the 2016 presidential election. The Russian agents used 75,000 fake accounts, and 230,00 bots to send political messages to an estimated 146 million U.S. Facebook users. In 2018, Facebook revealed it had shared personal data with 60 device makers of smartphones and TVs, and to large advertisers like Nissan Motors. In 2019 a Wall Street Journal investigation found that eleven out of the top fifty Facebook apps were sharing data they collect with Facebook. Most of these apps involved health, fitness, and real estate data. In response, the app developers stopped sharing sensitive personal data with Facebook, and Facebook itself contacted large developers and advertisers and reminded them Facebook's policy prohibits sharing any sensitive information with Facebook's servers. It isn't just Facebook that allows app developers to share personal information with online ad platforms like Google. Facebook announced that this was "industry standard practice." But clearly, Facebook's ability to effectively monitor and police exactly what information apps and advertisers share with Facebook's SDK (software development kit) is limited, at best, and at worst, not possible given the scale of Facebook's platform which is the most widely used app platform on the Internet with tens of thousands of app developers and advertisers.

Not to be outdone, Google has also taken liberties with user personal information, with services like Google Street View taking pictures of your neighborhood and your house and driveway, without consent, advertisements served using the content of your Gmail messages (though Google claims the content is anonymized), and pervasive tracking

continued

cookies following you across the Internet. Echoing Mark Zuckerberg, Google CEO Eric Schmidt has stated that "true transparency and no anonymity" is the best policy for Internet users.

VIDEO CASE QUESTIONS

1. Do people who use Facebook have a legitimate claim to privacy when they themselves are posting information about themselves?
2. How can using the privacy controls help preserve your privacy on Facebook? In what ways is the sharing control ineffective?
3. Why would Google combine information from separate accounts across its services and sites have privacy implications for its users?
4. Look up your address on Google Street View. Do you believe Google Street View constitutes a breach of privacy? Why or why not? Should Google seek your permission before putting pictures of your house online?