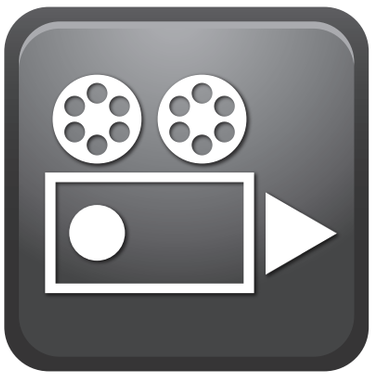
CHAPTER 4 **ETHICAL, SOCIAL, AND POLITICAL ISSUES IN E-COMMERCE**

CASE 2

Data Mining for Terrorists and Innocents



SUMMARY A look at anti-terrorism efforts of the U.S. government and the impact on individual privacy online.

(a) How does internet surveillance program PRISM work?

URL https://www.youtube.com/watch?v=JR6YyYdF8ho; L=1:59

(b) FBI director, Apple CEO talk privacy and security

URL https://www.youtube.com/watch?v=VhaRR22s-bY; L=1:56

CASE Anti-terrorism agencies around the world have made effective use of new surveillance technologies that offer unprecedented abilities to identify and apprehend potential terrorists. Today's terrorists are by nature difficult to track, as disconnected groups of individuals can use the Internet to communicate their plans with lower chance of detection. Anti-terrorist technology has evolved to better handle this new type of threat.

But there are drawbacks to these new strategies. Often, innocent people may find their privacy compromised or completely eliminated as a result of inaccurate information. Surveillance technologies are constantly improving. While this makes it more difficult for terrorists and other criminals to exchange information, it also jeopardizes our privacy, on the Internet and elsewhere, going forward. Is this reason for worry? Are comparisons to Orwell's 1984 appropriate or overblown?

In 2013, U.S. government contractor Edward Snowden leaked documents revealing several widespread online surveillance programs in use by the United States, including the

continued

PRISM and XKeyscore programs. PRISM allows the government direct and legal access to users' Google, Yahoo, Microsoft, Apple, Facebook, and other accounts, and XKeyscore collects and analyzes global Internet data, including emails, Web site traffic, and more. These programs use word length, punctuation, syntax, and content to analyze messages and develop author profiles for suspected terrorists. The size and scope of these programs were surprising to many at the time, and Snowden was branded by some as a traitor to his country and by others a hero for shedding light on these surveillance efforts. Nevertheless, PRISM and other NSA programs were authorized by the Patriot Act of 2001 under President Bush following the attack on the World Trade Center, and re-authorized in 2011 by President Obama following a series of terrorist attacks in the United States and Europe. Except in unusual circumstances of imminent attack, these surveillance activities are reviewed by the FISA court (Foreign Intelligence Surveillance Court).

Many tech giants felt the impact of Snowden's leaks as other countries sought to move away from American companies and products. Germany ended its contract with Verizon to provide telecom services for German government agencies. Brazil canceled an agreement with Boeing to provide military equipment, instead choosing Saab, a Swedish company. Apple also watched as many companies accused the iPhone of being a security threat due to its location tracking ability and repository of sensitive information about its user.

Although Apple was already no stranger to accusations of privacy infringement, in 2016, Apple was on the other side of the issue. After the mass shooting in San Bernardino, CA, committed by Syed Farook and Tashfeen Malik, the FBI struggled to unlock Farook's iPhone in search of intelligence. The FBI sued Apple, demanding Apple provide access to the phone. In February, a U.S. district court judge ordered Apple to provide a "backdoor" workaround allowing the FBI to bypass the iPhone's encryption and security measures. Apple CEO Tim Cook responded by announcing Apple's intent to challenge the ruling and reaffirming his commitment to the security measures of the iPhone. Cook claimed they did not possess the keys to open the phone's encrypted files, and they did not have the software to break the code. Apple claimed that to force Apple to write the code would be a violation of the First Amendment protection of freedom of speech. The FBI withdrew its lawsuit against Apple after it successfully broke the encryption on Apple iPhones without Apple's assistance. As it turns out, there are many firms and individuals who offer the capability to break into encrypted phones. The dispute between Apple and law enforcement remains unresolved.

Both the PRISM program and the battle over the iPhone backdoor illustrate the tug-of-war between privacy and legitimate law enforcement and anti-terrorism efforts. In 2019 U.S. government policy makers suggested the PRISM program of bulk warrantless searches of phone logs would come to an end, and the program no longer funded. More targeted warrantless searches of suspected terrorists may continue, rather than bulk mass searches that involved nearly the entire population of the United States. Searches of phone logs of suspected terrorists pursuant to a FISA warrant would also continue, as in the past.

continued

VIDEO CASE QUESTIONS

1. How is PRISM, a U.S. government program, able to surveil foreign communications?
2. Describe an example of PRISM providing intelligence about a suspected terrorist.
3. What is Tim Cook's argument for challenging the order to provide an iPhone back door?
4. What is FBI director James Comey's argument in favor of introducing the back door?