10-5b Tracking Users

Tracking users has become a major issue for Google. A storm of criticism was unleashed when government regulators and consumers learned the company's phones tracked users' locations. It was revealed that Android phones contained location-logging features enabling the firm to collect GPS coordinates of its users as well as the coordinates of nearby Wi-Fi networks. Similar tracking features were found on the Apple iPhone. The revelations spurred legislators to write letters to Google asking for clarification on how it tracks users and uses this information.

Privacy advocates claimed these tracking features violated users' right to privacy, particularly since most users did not know about the feature. Google defended its phone tracking feature, stating the information it gathered was necessary to build Google's location-based network and allow it to effectively compete. It claimed this data is often necessary for certain mobile applications and websites to work.

Google also tracks users on the Internet. For Google, offering advertisers the ability to specifically target their ads to desired users based on their interests is invaluable to remaining competitive in the advertising market. Additionally, Google uses this information to customize its services to individual users. For example, users will see different results for the same Google search terms based on what Google believes they most likely want, based on what it knows about them. Many privacy advocates do not like this pervasive use of tracking, and there is ongoing concern by regulators and others over how Google uses the information it collects. Google's privacy policy does allow users to opt out of many tracking functions, but users must actively do so—the default is to be tracked. This is especially problematic for the many users that do not realize they are being tracked and/or do not know how to use Google's settings to opt out. All of the popular web browsers, including Google Chrome, now include a "Do Not Track" option, which indicates to websites that the user does not wish to be tracked. However, the designation has no legal or regulatory authority and has so far remained mostly symbolic, with many websites simply ignoring it.

On the other hand, supporters of Google maintain that tracking is necessary to provide the best services to users. These services are often free because Google is able to generate revenue through advertising. Tracking also allows Google to customize its services to individual user needs. Consumers must therefore be proactive in deciding whether they place greater value on their privacy or Google's free services.

Although some people do not appear to mind having their web activity tracked in exchange for Google's free services, Google received heavy backlash for bypassing anti-tracking mechanisms. In 2012 security analysts revealed that Google was using loopholes in Apple's Safari browser to ignore its default privacy settings while simultaneously telling Safari users they were protected. The browser's default settings prevented installation of certain types of Internet "cookies"—streams of data placed on a user's computer when he or she visits certain sites. However, Google's cookies were still being installed. Google claimed the bypass was a mistake, meant only to help its Google+ "+1" button (similar to Facebook's

“like”) work properly on third-party websites, and removed it immediately after it was made public. Still, the Federal Trade Commission (FTC) launched an investigation to determine whether Google had violated a previous agreement to refrain from misrepresenting its privacy practices to the public. Google eventually paid $22.5 million to settle the FTC charges and an additional $17 million to settle similar charges brought by 37 states and the District of Columbia.

Google has also been accused of failing to respect user privacy in the real world. In 2010 Google announced it had accidentally scanned data from some users’ personal wireless networks in the United Kingdom. Google uses vans with special detection equipment and cameras to drive around collecting data and photos for its location-based services. Unfortunately, because of software Google said had inadvertently been uploaded onto the company’s equipment, its vans also scanned wireless networks of nearby residences and collected activity data from any networks that were unsecured and open, including URLs, emails, text messages, video and audio files, and more. Google promised the Information Commissioner’s Office in the United Kingdom it would destroy the data it collected from U.K. users. However, a later investigation in 2012 revealed Google still retained some of this user data, placing the company in noncompliance with the agreement. Although Google apologized and called this retention of data another error, the violation exacerbated its image of being a firm that disregards privacy.

Soon after the U.K. incident, it was discovered Google had been collecting the same type of information from unsecured residential wireless networks in other countries as well. In the United States, Google was fined $25,000 by the Federal Communications Commission (FCC) for deliberately delaying and impeding its investigation. Evidence was uncovered suggesting that Google’s collection of this information may not have been accidental but rather intentionally set up by Google engineers. Google asked the FCC to keep its findings confidential, but later pre-emptively released them itself after the FCC refused. The investigation led to a $7 million settlement among Google, the FCC, and 38 states and the District of Columbia. At least seven other countries also found Google guilty of similar activity in their jurisdictions.

Yet another privacy-related incident for Google involved the Google Play App Store. A developer who started selling a mobile application through Google’s app store was shocked by the amount of information he was given about his customers, including their names, locations, and email addresses, even though nowhere in the app buying process were customers asked to give consent to release that information. The developer argued that this practice violated Google’s privacy policy, which at the time stated that identifiable information would never be given to third parties without user consent. Some privacy experts agreed with the developer; others did not, stating that the information shared was minimal and of the type commonly expected to be given out in making any purchase. Still, Google’s approach to privacy continues to be a subject of controversy and debate.