Assignment 5: Essay Question
Gunnar Yonker

Issue:

Are Uber's security practices considered "unfair acts or practices" or "deceptive acts or practices" or both under Section 5 of the Federal Trade Commission Act, assuming that all of the allegations are true?

Rule:

Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce".

Unfair Acts or Practices

An act or practice is unfair where it

- Causes or is likely to cause substantial injury to consumers,
- Cannot be reasonably avoided by consumers, and
- Is not outweighed by countervailing benefits to consumers or to competition.

Deceptive Acts or Practices

An act or practice is deceptive where

- A representation, omission, or practice misleads or is likely to mislead the consumer;
- A consumer's interpretation of the representation, omission, or practice is considered reasonable under the circumstances; and
- The misleading representation, omission, or practice is material.

Analysis:

To evaluate if Uber's security practices are considered "unfair acts or practices" or "deceptive acts or practices" or both we need to consider the following:

For "Unfair" Acts or Practices:

1. Has Uber's trade practice caused or is likely to cause substantial injury to customers?

Yes, in this case Uber's practice of collecting and then storing large amounts of personal information from both riders and drivers, but then not actively monitoring employee access to it has the potential to cause substantial injury to customers if this information were to be leaked.

2. Do benefits to Uber's consumers outweigh the injury?

This question is more unclear in this case as the Uber app provides a convenient way to connect riders with drivers at a moments notice, but the collection and storage of the consumers' personal information by Uber may not be necessary for the service to be provided through the app. This means that it is unclear if the benefits to Uber's consumers would outweigh the potential injury.

3. If the consumers exercised reasonable care, could they have avoided the injury in the first place?

No, consumers may not be able to avoid the injury in this case because they are required to provide personal information to Uber to use the app and the service. If the consumer wants to request a ride, they need to make an account on the Uber app which requires submitting their personal information.

For "Deceptive" Acts or Practices:

1. Was there a representation, omission or practice that was likely to mislead the consumer?

Yes, because Uber's representation that its policies prohibit all employees from accessing a rider or driver's data except for a limited set of authentic business purposes, and that access to rider and driver accounts is being closely monitored and audited by data security specialists was likely to mislead consumers into believing that their personal information was safe. This is untrue because Uber did not always closely monitor and audit its employees' access to consumer personal information since November 2014.

2. If we examine the practice from the perspective of a consumer acting reasonably in the circumstances, is the consumer being misled?

Yes, a reasonable consumer could be mislead by Uber's representation in this case given that they would reasonably expect that their personal information is to be protected and secure when using the Uber app.

3. Was the representation, omission, or practice a “material” one?

Yes, the representation that Uber has strict policies concerning access to rider and driver data is a “material” one. This is because it concerns the protection of personal information, which is important to consumers. The omission of the fact that these policies were not always followed and that access to consumer personal information was not closely monitored and audited is considered a “material” omission.

The case presents allegations of Uber’s business practices including the collection and storage of personal information from both riders and drivers, as well as the employee’s internal access to such information. This case also noted that Uber had issued a statement in November 2014, to reassure consumers that the access was being closely monitored and audited. However, this case indicates that Uber did not always comply with its representation and that there were incidents of improper access and use of personal information through the use of an internal tool called “God View” that displayed the personal information of riders.

Conclusion:

Based on the allegations presented in the case, assuming that they are true, Uber’s security practices would be considered both “unfair acts or practices” and “deceptive acts or practices” under Section 5 of the Federal Trade Commission Act. The collection and storage of personal information from riders and drivers, including aspects such as precise geolocation information, without adequate security measures could cause or could be likely to cause substantial injury to consumers, which is not reasonably avoidable by the consumers themselves. This is because unauthorized access to such information could result in identity theft, stalking, or other harm. Also, Uber’s statement that its access to rider and driver data is closely monitored and audited could be considered deceptive if Uber did not comply with its representation as alleged in this case.