Background

In this exercise, we return once again to that mobile-applications startup. You’re once more the chief technology officer working up a security framework for the startup’s network designed to protect the business’s documents and data.

Your goal this time is to consider what information the applications that your company is developing should collect about the users. Many modern mobile devices contain sensors that report all sorts of potentially interesting details both about the devices themselves (location, orientation, file system contents, display contents, network activity, uptime, battery status, etc.) and about the users (through touchscreens, cameras, and microphones).

Applications typically ask users at installation time for permission to access these sensors and input devices, but usually they will ask for more than the bare minimum that the applications need to perform their functions. Developers want to collect additional information about their users and their users’ devices for business reasons, such as quality assurance (making sure that the application is functioning correctly and reporting on faults and crashes), product improvement (e.g., watching how the users work with the application, to improve the design of the user interface and the performance of the most frequent operations), and customer relations (e.g., noting when a user is experimenting with a competing product so that the user can be targeted for advertisements about enhanced features, discounts, and so on).

The difficulty is to strike a balance between, on one hand, the need to know as much as possible about the company’s customers and their use of the company’s product, and on the other hand the data-protection responsibility (and liability) that the company assumes by collecting, storing, and mining large amounts of detailed personal information about customers.

The Proposal

Today’s assignment is to write up three new sections for the security-framework document:

6. A policy statement explaining what kinds of data the company will collect about its users, their devices, and their interactions with the company’s applications, and what kinds of data mining the company will perform on the data it collects from users in this way. Include a justification for the general policies that you lay down.

7. An assessment of the threats to data obtained from users as it is transferred from the users’ devices to the company’s databases, and recommendations for preventing or mitigating these threats.

8. An assessment of the threats to this data about users once it is stored in the company’s databases and mined (in ways that conform to the policies mentioned in part 6 above), and recommendations for preventing or mitigating these threats.

This exercise will be due at the beginning of class on Thursday, May 11.