Report

Apple uses local differential privacy to keep track of what its users are up to while protecting their privacy. Differential privacy alters data communicated with Apple before it leaves the user's device, ensuring that Apple will never be able to duplicate the original data. Apple's differential privacy technology is based on the premise that slightly biased statistical noise can hide a user's personal data before it is shared with Apple. When a huge number of people submit the same data, the noise may be averaged out over a vast number of data points, allowing Apple to see important information emerge.

Privacy budget: To protect a user's privacy, Apple's differential privacy implementation incorporates the concept of a per-donation privacy budget (quantified by the parameter epsilon) and places a stringent restriction on the number of contributions a user can make. The reason for this is that the slightly biased noise employed in differential privacy tends to average out over many contributions, allowing information about a user's activities to be determined over a large number of observations from a single user.
Apple tries to keep the privacy budget low for each feature while still collecting enough data to improve the functionality. Apple keeps the information for a maximum of three months. IP addresses are not stored, and no identifiers are included in the donations.

Techniques: By adding slightly biased noise to the data that is shared with Apple, local differential privacy ensures that it is impossible to tell whether a specific user contributed to the computation of an aggregate. However, before we can add this noise, we need to build a data structure that can capture a rough sketch of user input in a minimal number of bits.

When the sketch matrix information is delivered to Apple, the Apple server tallies the responses from all sharing devices and outputs the mean value for each element of the array. Even though each submission has numerous randomized elements, the average value over a large number of submissions provides Apple with useful aggregate data.

Controlling participation: The user setting for Device Analytics is linked to the data-gathering features that use differential privacy. When setting up a device running macOS or iOS, users are given the option of sending diagnostic information, which they can adjust later in System Preferences on macOS or the Settings app on iOS.

The first steps Differential privacy was originally introduced by Apple in macOS Sierra and iOS 10. Since then, we've added more types like Safari and Health to our repertoire. We look forward to leveraging differential privacy algorithms to improve user experience in other areas of Apple's products as we continue to work to protect our users' private information as Apple refines differential privacy algorithms.