Differential Policy

Apple uses a technique called local differential privacy, which allows them to see what many Apple users are doing while preserving the privacy of individual users. Apple cannot reproduce the true data because it transforms the information before it ever leaves the user's device.

Apple's differential privacy technology essentially shuffles an individual's data before sharing it with Apple using statistical noise that's biased. The noise that's added over huge numbers of data points averages out over large numbers of submissions, allowing Apple to uncover meaningful insights.

By incorporating a perdonation privacy budget, quantified by the parameter epsilon, the implementation sets a strict limit on the number of contributions from a given user in order to maintain their privacy. Further, before adding the biased noise, it is necessary to define a data structure that captures a sketch of user input with a small number of bits. Apple uses two techniques:

* Count Mean Sketch: In this technique, the information being shared with Apple is encoded by use of a series of mathematical functions known as hash functions. This makes it easy to represent data of varying sizes in a matrix of fixed size.
* Hadamard Count Mean Sketch: In this technique, the hashed encoding is transformed using a Hadamard basis transformation prior to privatization, just as in the Count Mean Sketch mentioned above. Furthermore, you only send one bit per row instead of the entire row as in Count Mean Sketch.

Last but not least, these techniques were first implemented in macOS Sierra and iOS 10 and have since been expanded.