**Notes:**

Furthermore, traditional approaches treated privacy as a property of the output of an analysis, whereas it is now understood that privacy should be viewed as a property of the analysis itself. Any privacy preserving method including differential privacy must adhere to this general principle in order to guarantee privacy protection.

**Question:**

What do Wood et al. mean when they say “privacy should be thought of as a property of a computation?” Explain.

**Answer:**

In *Differential Privacy* by Wood et al. the authors talk broadly about the new and emerging field of differential privacy, which is a mathematical definition of privacy in the context of statistical and machine learning analysis. Furthermore, differential privacy aims to protect individuals’ privacy/information essentially as if their information was not used in the analysis as all. In general, the results of the analysis wouldn’t change if any individual were to have their data omitted from the analysis.

Further on in the text, Wood et al. state that “privacy should be thought of as a property of a computation.” To understand what the authors mean by this we need a little background information. Many traditional approaches treated privacy as a property of the output of the analysis, as long as researchers could ensure that the outputs of an analysis could anonymize the subjects then they were all good. However, due to things such as information collected by attackers outside of the system, a data set that appears anonymous may still be used to learn sensitive information about individuals in the data set. A more modern approach reveals that privacy is now viewed as a property of the analysis/computation itself, instead of just the output. Thus when Wood et al. state that “privacy should be thought of as a property of a computation,” they mean privacy should be seen as the informational relationship between the input and the output, and not just the output alone.