How is privacy disclosed?

gradient
(as input features)
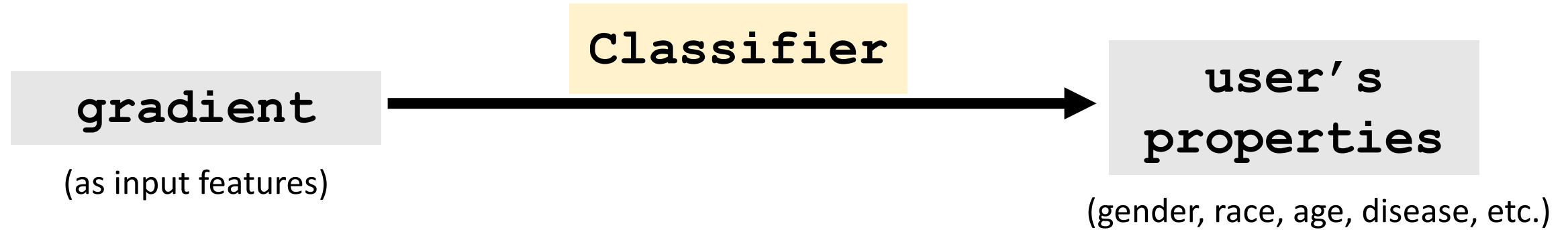
Classifier

→

user's properties
(gender, race, age, disease, etc.)

References

1. Melis et al. Exploiting unintended feature leakage in collaborative learning. In *IEEE Symposium on Security & Privacy*, 2019.