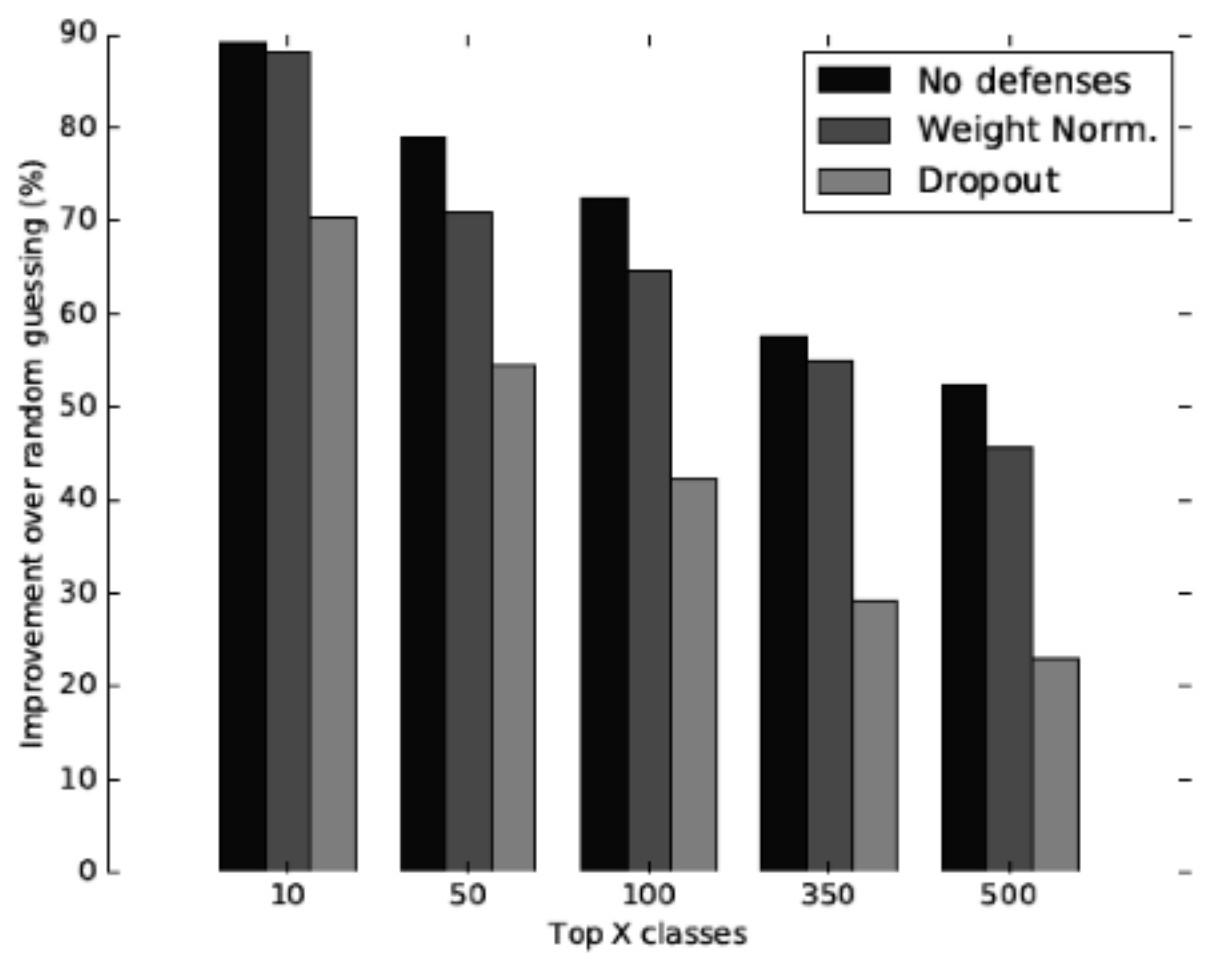
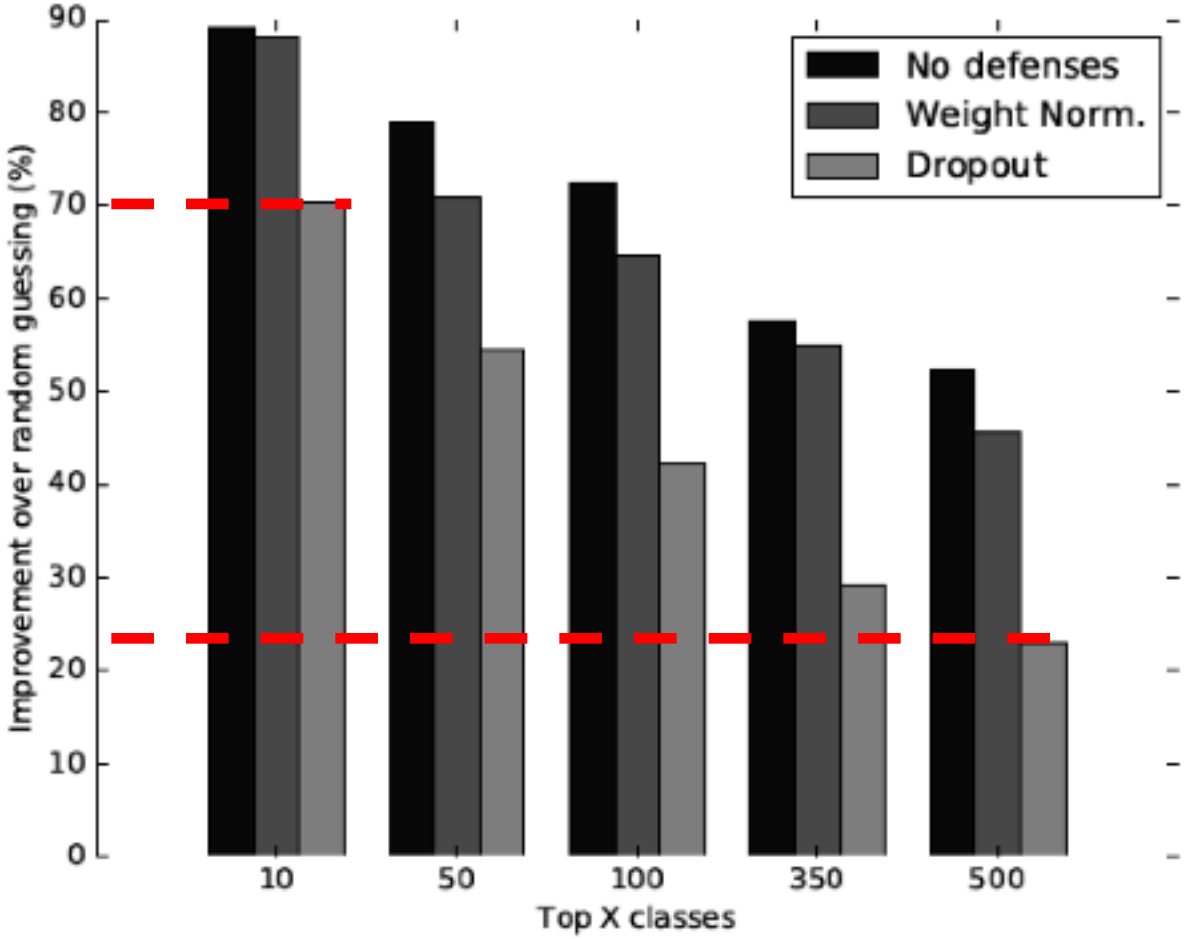
Defenses - Training Regularizers


No defenses
Weight Norm.
Dropout
Improvement over random guessing (%)
0
10
20
30
40
50
60
70
80
90
10
50
100
350
500
Top X classes

White-box, LFW

Defenses - Training Regularizers



White-box, LFW

Mobility Analytics on Aggregate Time-Series