



*Issued 10/2/18*

## **You Gave your Number to Facebook for Security and It Used It for Ads**

What happens to the mobile numbers Facebook users add to their accounts to enable SMS two-factor authentication (2FA)? If you assume the answer is nothing beyond their described purpose, prepare for a bit of a surprise courtesy of a study by researchers from Northeastern University and Princeton University, backed by plenty of dissatisfied commentary from the privacy community and tech press. Facebook, the researchers found, has been adding these numbers to the other data it uses to target people with advertising. It is already known that Facebook lets advertisers upload their own data – including email addresses and telephone numbers – which is matched to the same data on user accounts. As the researchers explain: Facebook then creates an audience consisting of the matched users and allows the advertiser to target this specific audience. An article in Gizmodo – which worked with the researchers – calls this data “shadow contact information,” perhaps deliberately echoing recent controversy surrounding Facebook’s shadow profiles used to gather data on internet users who come into contact with its sites without having accounts. It is outrageous that Facebook is asking people to turn off SMS-based 2FA simply because they don’t like the fact that it is using that telephone number to target them with advertising. Facebook uses advertising to make money from what is a free service – it harvests PII to target advertising and perhaps anyone bothered by this shouldn’t be on Facebook. The good news is that however convenient SMS-based authentication might seem, it’s not secure enough anyway and Facebook users would be better migrating to alternatives such as an authentication app, or even the Facebook’s app’s own Code Generator function.