Security and Machine Learning

Points: Pervasiveness, Danger of untested systems, Growing threats, Big Tech, Governments, Privacy, MLaaS

In the past few years, there has been an incredible resurgence of interest in machine learning. A dream once lost of understanding and replicating intelligence resurrected in the minds of society overnight. enabled by both breakthroughs artificial neural networks research and large labeled data sets. Social network services and mobile devices collect voice data which have improved voice recognition, emails, text messages, and search engine queries for next word prediction and language translation, medical images detecting cancer, purchase history for product recommendation and ad placement, and location history for improved route recommendations.

the widely available technologies that have undammed a relentless deluge of labeled data.

…

The price of improving these systems comes at relinquishing ownership and privacy of our data.

Democratizing Machine Intelligence

Points: Data bias, sparsity, compute resource sharing, growth of data

“Age of machine intelligence”

“Perhaps deep learning can lead to a new age of enlightenment”