

# Ayrton San Joaquin

✉ ajsanjoaquin@gmail.com | 📍 Singapore | [in ajsanjoaquin](#) | [🔗 ajsanjoaquin.github.io](#)

## Education

### Yale-NUS College

BACHELOR OF SCIENCE (HONORS) IN DATA SCIENCE, MINOR IN PHILOSOPHY  
Awarded Scholarship to attend Full-time

Singapore

August 2018 - February 2023

## Experience

### Data Protection and Trustworthy Machine Learning Lab, NUS

Singapore

UNDERGRADUATE RESEARCHER

May 2021 - August 2021

- Pitched and led a project to analyze **Unlearnable Data** as a data protection method. Paper to be refined in a workshop.
- Collaborating with Google Brain on privacy attack research for my bachelor's thesis.

### NUS-Tsinghua Center For Extreme Search (NeXT++)

Singapore

DEEPAKE DETECTION RESEARCH INTERN

May 2020 - August 2020

- Read and adapted various robustness strategies against adversarial noises (e.g. Adversarial Training, Randomized Smoothing)

### Arterys (Freelance)

San Francisco, United States

DEEP LEARNING ENGINEER

March 2020 - June 2020

- Created a COVID-19 Pneumonia classifier four days after pandemic declaration in collaboration with A.I. Singapore.
- Contacted by Arterys, and **Deployed model in the Arterys platform**, alongside models from NVIDIA and Ping An Technology, for use by American hospitals and researchers.

## Open-Source Projects & Contributions

### Twitter Algorithmic Bias Challenge 2021

- Identified unintended sexualization of non-sexual images involving nudity by the **Twitter Image Cropper Algorithm**. Finished 9th out of 40 teams worldwide.

### Explaining Neural Networks with Meaningful Perturbations

- For explaining an image classifier's prediction, I implemented the algorithm described in *Explanations of Black Boxes by Meaningful Perturbation* (Fong, et. al., 2018).

### COVID-19 Pneumonia Classifier for Diagnosis Triage

- Trained a Resnet-34 Convolutional Neural Network (CNN) on ~ 26,000 images with Resampling to detect Pneumonia caused by COVID-19 on xray scans ultimately to triage patients for urgent diagnosis.

### Miscellaneous

- Contributed improvements to popular and massive projects including Pytorch (deep learning framework) and YOLOv4 (object detection model).

## Publications

\*No name indicates first or sole authorship.

April 2022 Tramer, F., ..., **San Joaquin, A.**, et.al. , **Truth Serum: Poisoning Machine Learning Models to Reveal Their Secrets**, To appear in ACM CCS 2022.

March 2020 , **Using Deep Learning to Detect Pneumonia caused by COVID-19** Towards Data Science

## Press

April 2022 **Machine learning models leak personal info if training data is compromised**, The Register

## Skills

**Programming Languages:** Python, Java, R

**Machine Learning in Python:** Pytorch, Pytorch Lightning, NumPy, Sickit-Learn, Tensorflow, Keras, Jax

**Data Management:** Pandas, SQL, MS Excel

**Application Deployment &**

**Version Control:** Docker, Google Cloud, Git, Singularity