CASSIDY LAIDLAW

laidlaw.cassidy@gmail.com
cassidylaidlaw.com

EDUCATION

University of California, Berkeley
2020 – Present

- Ph.D. in computer science, focusing on human-AI cooperation, learning human preferences, and robustness in machine learning.
- Supported by a National Defense Science and Engineering Graduate (NDSEG) Fellowship.

University of Maryland, College Park
2014 – 2018

- Double B.S. in computer science and math, Middle East studies minor, GPA 4.00/4.
- Selected as one of top five graduating seniors for "academic distinction, exemplary character, and service to the campus or public communities."

RESEARCH EXPERIENCE

Research in Adversarial Robustness
April 2019 – Present

- Developed the first adversarial defense that generalizes to unseen threat models, perceptual adversarial training (PAT). Paper sunder review.
- Invented the ReColorAdv attack, which when combined with other attacks leads to the strongest existing attack even after adversarial training. Paper presented at NeurIPS 2019.
- Investigated adversarial robustness with an abstain option.

Research at Max Planck Institute for Intelligent Systems
May 2017 – January 2018

- Improved statistical face models developed at the institute.
- Designed a protocol to capture tens of thousands of 3D scans of human faces.
- Used deep learning to model the relationship between speech and facial motion.
- Coauthored paper presented at CVPR 2019, a leading computer science conference.

Research in Cross-Lingual Connotation
January 2016 – March 2016

- Researched differences in word connotation across languages with Prof. Marine Carpuat at the U. of Maryland.
- Worked with Google teraword n-grams and scraped news sites in multiple languages.

PUBLICATIONS AND PREPRINTS

Cassidy Laidlaw, Sahil Singla, and Soheil Feizi. **Perceptual Adversarial Robustness: Defense Against Unseen Threat Models**. *arXiv preprint*.

Cassidy Laidlaw and Soheil Feizi. **Playing it Safe: Adversarial Robustness with an Abstain Option**. *arXiv preprint*.

Cassidy Laidlaw and Soheil Feizi. **Functional Adversarial Attacks**. *NeurIPS 2019*.

Daniel Cudeiro, Timo Bolkart, Cassidy Laidlaw, Anurag Ranjan, and Michael J. Black. **Capture, Learning, and Synthesis of 3D Speaking Styles**. *CVPR 2019*.

SOFTWARE DEVELOPMENT EXPERIENCE

Mobile Developer, Blip Labs
November 2018 – July 2020

- Building an app to streamline the bill payment process.
- Using React Native, Django, and APIs from Plaid, Finovera, and Q2.

App Developer, Why Weight? **March 2018 – August 2020**

- Building an app to help clients of Why Weight, a weight loss and life coaching company.
- Implemented features to let users track their weight, connect with Bluetooth scales, log food and water intake, and message the company's life coaches.
- Writing the app in React Native with a Django backend hosted in AWS.

Data Scientist and Web Developer, Builda.co **November 2016 – November 2019**

- Built an analysis and visualization pipeline for data from Fortune 500 companies using Apache Spark.
- Created a web-based mentoring platform using Django, Bootstrap, jQuery and APIs from LinkedIn, Braintree, and Office365.

Web Developer, WorkStrive **March 2019 – July 2019**

- Developed a website and platform that turns gyms and yoga studios into coworking spaces during the day (see workstrive.com).

Insider Threat Analysis Tool, Center for Study of Terrorism and Responses to Terrorism **November 2016 – December 2018**

- Built a tool to analyze insider threats in airport cargo systems with a team of three other developers.
- Implemented the user interface in JavaFX.
- Met with and presented tool to government officials in Department of Homeland Security, FBI, etc.

Other Freelance Software Development Work **June 2014 – August 2020**

- Including data science, mobile apps, and web development.

HONORS AND AWARDS

National Defense Science and Engineering Graduate (NDSEG) Fellowship

University of Maryland University Medal Finalist: selected as one of five finalists for the highest honor that the university can bestow on an undergraduate student based on the criteria of "academic distinction, exemplary character, and service to the campus or public communities."

Banneker/Key Scholarship: the University of Maryland's most prestigious scholarship.