Reuben Feinman

Center for Neural Science, New York University
4 Washington Pl, Room 809, New York, NY 10003
reuben.feinman@nyu.edu • http://www.cns.nyu.edu/~reuben

EDUCATION

New York University, New York, NY — Sep 2017 – Present
Ph.D., Neural Science
- Advisors: Brenden M. Lake & Eero P. Simoncelli
- Focus: Computation, perception & learning

Brown University, Providence, RI — Sep 2011 – May 2015
Sc.B. with Honors, Applied Mathematics
- Honors thesis: A Deep Belief Network Approach to Learning Depth from Optical Flow
- Thesis advisors: Thomas Serre & Stuart Geman
- GPA: 3.9 / 4.0

HONORS & AWARDS

Google PhD Fellowship in Computational Neuroscience, Google — 2018 – 2020
Fellowships awarded annually to ~30 PhD students around the globe studying CS and related disciplines.

Henry Mitchell McCracken Fellowship, NYU GSAS — 2017 – 2018
Fellowships awarded annually to promising first-year PhD students in the GSAS.

CTO Recognition Award, Symantec Corporation — May 2016
Awarded by CTO Steve Trilling for significant contributions to the company's technologies.

Sigma Xi Honor Society, Brown Chapter Sigma Xi — May 2015
Awarded for strong academics and promising research achievement in a field of applied science.

PUBLICATIONS & PATENTS

PUBLICATIONS

Feinman, R. and Lake, B.M. (2018). Learning inductive biases with simple neural networks. In *Proceedings of the 40th Annual Meeting of the Cognitive Science Society*.

PREPRINTS

Feinman, R., Curtin, R.R., Shintre, S., and Gardner, A.B. (2017). Detecting adversarial samples from artifacts. *arXiv preprint arXiv:1703.00410*.

Papernot, N., Goodfellow, I., Sheatsley, R., Feinman, R., and McDaniel, P. (2016). Cleverhans v1.0.0: an adversarial machine learning library. *arXiv preprint arXiv:1610.00768*.

PATENTS

Feinman, R., Echauz, J., and Gardner, A.B. (2016). Systems and methods for trichotomous malware classification. *US Patent App. No. 15/356,526*.

Feinman, R., Gardner, A.B., and Parikh, J. (2016). Efficient feature selection. *US Patent App. No. 15/282,645*.

Feinman, R. and Parikh, J. (2016). Systems and methods for detecting malware based on event dependencies. *US Patent App. No. 15/188,950*.

RESEARCH TALKS

Learning Inductive Biases with Neural Networks, NYU CILVR lab meeting — Feb 2018
Artifacts of Adversarial Examples, NYU LCV meeting — Nov 2017

WORK EXPERIENCE

Symantec Corporation, Mountain View, CA — Jul 2015 – Jun 2017
Machine Learning Engineer, Center for Advanced Machine Learning
- Worked as the only non-PhD in a team of 10, with the consulting of ML pioneer Ruslan Salakhutdinov.
- Led an R&D effort that resulted in the dramatic improvement of known and unknown malware detection rates on 100+ million endpoints worldwide.
- Developed a ML model that caught and blocked 22 million attempts of the global and infamous "WannaCry" ransomware attack.

PRESS COVERAGE

Security Week, Symantec Adds Machine Learning to Endpoint Security Lineup — Sep 2016
eWeek, Symantec Adds Deep Learning to Anti-Malware Tools to Detect Zero-Days — Jan 2016

SKILLS

Python, Jupyter, TensorFlow, PyTorch, Pyro, Docker, Git, MATLAB, LaTeX, Java, C

INTERESTS Running, skiing, scuba diving, tennis, fishing, music production

REFERENCES *Mentors and colleagues who have written recommendations for me:*
Dr. Brenden Lake, Assistant Professor of Psychology and Data Science, New York University
Dr. Thomas Serre, Associate Professor of Cognitive Linguistic & Psych. Sciences, Brown University
Dr. Stuart Geman, James Manning Professor of Applied Mathematics, Brown University
Dr. Andrew Gardner, Senior Technical Director of Machine Learning, Symantec Corporation
Dr. Nikolaos Vasiloglou, Technical Director of Machine Learning, Symantec Corporation