Nicholas Chen, applying for PhD in Computer Science

I am applying for graduate school to study effective and secure deep learning systems. As software, hardware, and theory advance, I expect deep learning to become widely integrated in industry over the next few decades. I want to directly contribute to this innovation, which will require a stronger understanding of why certain architectures, training procedures, and data engineering methods perform better than others. In addition to developing the most powerful, accurate models possible, I'm becoming increasingly concerned with security and privacy. As deep learning grows more widespread in applications of computer vision, NLP, and robotics, I'm worried about the massive security threats that these technologies will raise when deployed in practice.

Addressing these problems will require more in-depth knowledge of deep learning, security, and the research process. I expect graduate studies will help me develop these skills in preparation for a career in research. I'm not completely certain whether I want to eventually work in industry, academia, or found a startup, but I expect that it will involve designing robust and effective deep learning technologies.

I became particularly interested in the promise of deep learning as an intern at the Trade Desk. Faced with massive scale, unstructured data, many of The Trade Desk's statistical models relied on methods like one-hot encoding to process sparse non-numeric features such as website URLs and device IDs. Though functional, one-hot encoding produces a high dimensional feature vector which leads to overfitting and inefficient computation. Critically, this naïve method treats all possible feature values as equally and entirely different. To address this problem, I designed and implemented an object embedding pipeline to efficiently convert discrete data to continuous features. Leveraging deep networks for learned feature representation in this way enabled data scientists to progress on challenging, or even impossible problems such as website demographic prediction and user lookalike modeling. I was amazed that an artificial mathematic construct was capable of learning to solve a problem that humans could not.

My experience at The Trade Desk spurred a strong interest in research as a long-term career. It was incredibly satisfying to realize theoretical technologies in solving a real-world open problem. I enjoyed the process of studying related work in deep learning-based feature representation, then adapting and improving upon it for a new purpose. Most of all, I was thrilled with the freedom to explore and pursue questions for which no one in the world has provided a definitive answer. In this case, how should an object embedding be evaluated when the problem inherently lacks an objective ground truth? Why does one architecture or feature engineering method facilitate better learning and faster convergence than another? For the first time, my questions couldn't be simply answered by a mentor, or even Google search; at best, there would be conflicting answers from dubious sources. Gradually, I found that I not only accepted, but began to enjoy the uncertainty involved in research. Failures in the process of iterative discovery are what make success worthwhile.

For the last year, I've been continuously working on what I consider a beautiful application for prediction: stock trading. No industry has lower barriers to entry – anyone can open a brokerage account and place orders with zero commission - and if you can accurately predict the future, you win. I have developed and continue to refine an automated trading system centered around a convolutional neural network to predict stock price movements based on recent market data. Through closely scrutinizing every step of the process, from feature construction to model design and training procedure, I've become painfully aware of how much I have yet to learn about deep learning theory. I still rely on papers and web searches to schedule training, explain weaknesses and fine tune architecture. I have learned the technical "what" and "how" of deep learning to make a functional model, but now want to dive in more depth to study "why" some choices work better than others. In undergraduate coursework, many of these finer level details are abstracted away as beyond the scope of the class and I'm no longer satisfied with that.

Nicholas Chen, applying for PhD in Computer Science

While most of my work has primarily focused on developing the most powerful, accurate models possible, I'm becoming increasingly concerned with matters of security and privacy. As analytical studies frequently require the collection and analysis of sensitive user information, researchers face a trade-off between privacy and effective decision making. This year, I've worked on a team led by Prof. Sanjay Patel developing RokWall, a privacy preserving computation infrastructure, and CoTracer, a decentralized Bluetooth contact tracing app. Our mission was to develop technologies to safely reopen UIUC for the Fall 2020 semester while upholding user privacy rights.

My contribution was designing an exposure mapping application to visualize high risk areas on campus, which requires analysis of each user's GPS data and COVID-19 test status. Through group discussions with Profs. Andrew Miller and Chris Fletcher, I considered threats ranging from user attacks to malicious service providers, or even foreign national level threats. Ultimately, we proceeded with an efficient, lightweight implementation built with Intel SGX enclaves to provide several key guarantees. Critically, a user's data is completely anonymized and used solely for its designated application; with data sealing and remote attestation protocols, even a malicious service provider cannot compromise the enclave or access decrypted user data. Our paper was recently accepted to the upcoming NDSS CoronaDef Workshop and I found the pressure involved in the publication process to be particularly exciting; the night of the conference's submission deadline, I stayed up closely scrutinizing every phrase of the paper until literally 11:59. I am proud to have contributed towards such an impactful project and hope to continue doing so for the rest of my career.

More generally, RokWall and CoTracer have reinforced the importance of not only providing a powerful technology, but also developing it to be resilient against both internal and external threats; as a product scales in importance, so does its potential danger when compromised. Applying the same security-conscious mentality to the field of artificial intelligence, I believe that deep learning exhibits significant vulnerabilities which could pose massive threats to society – most notably in lack of model interpretability and adversarial machine learning.

Deep learning is notoriously referred to as a black box technique, and with reasonable cause. While traditional statistical learning methods like regression and Bayesian modeling help researchers draw direct connections between features and predictions, deep neural networks require complex compositions of many-to-many functions. Layered architectures enable universal approximation but make it difficult to recognize and react to costly mistakes encountered in practice. Moreover, a lack of model interpretability obfuscates bias in machine learning, which hurts both technologists and consumers alike through unfair and suboptimal decision making. Meanwhile, malicious attackers can exploit model sensitivity to cripple neural networks with small perturbations to input data; even in benign settings, deep networks may react unexpectedly to seemingly insignificant noise. While deep learning can change the world in performance critical applications like autonomous driving or medical diagnosis and treatment, mistakes may represent proportionately disastrous consequences. I want to explore how to best address these vulnerabilities and ensure that my work drives positive impact.

In summary, I aspire to research deep learning and its intersection with security so that I can better describe the world and predict the future. My goal is to develop innovative, socially conscientious technologies and defend them with confidence, competence, and integrity. Eventually, I hope to develop robust, explainable models that reliably solve important problems facing humanity.