Dr. Eric Rozier is an Assistant Professor of Computer Science and head of the Trustworthy Data Engineering Laboratory at Iowa State University. He has previously been named a Frontier’s of Engineering Education Faculty member by the National Academy of Engineering, a two time Eric and Wendy Schmidt Data Science for Social Good Faculty Fellow at the University of Chicago, and an IBM Research Fellow. Dr. Rozier’s research interests revolve around the intersection of Data Science and Engineering with Cybersecurity, Reliability, and Performability Engineering, with a focus on dependable computing for critical infrastructures. His work in Adversarial Machine Learning was recently featured as one of the inaugural talks for the USENIX Engima conference on emerging threats and novel attacks. Before joining the University of Cincinnati, Dr. Rozier was the founding director of the Fortinet Cybersecurity Laboratory at the University of Miami where he worked to develop and commercialize new technologies in homomorphic encryption for cloud-based systems. He earned his Ph.D. from the University of Illinois at Urbana-Champaign where he worked on applications in fault-tolerance and security with the National Center for Supercomputing Applications, and the Information Trust Institute.

The issue of Data Privacy is both a serious one, and one with consequences which are alarmingly final. Recent breaches to federal databases which have exposed social security numbers, payroll data, private health records, and credit card and banking information underscore our vulnerability, but also the finality of the damage caused by a privacy exposure or leakage. In traditional cybersecurity, a DDoS can be mitigated, privilege escalation can be removed, and holes in our defenses can be patched. Data Privacy violations, however, do permanent damage. There is no putting the genie back into the bottle. While this may seem to suggest Data Privacy is desirable above all else, the most private system is also the least usable. Data which cannot be analyzed cannot be useful, and in many cases restricted access can slow not only scientific but social progress. In 2012 we suffered a loss of access due to policy-based Data Privacy restrictions which led to a reduction in our ability to combat lead poisoning in Chicago. While it is impossible to know for sure, it is likely some children suffered permanent harm due to the reduced ability of the Chicago Department of Public Health’s ability to predict at risk populations during this loss of access.

In this talk we will examine the fundamental trade offs necessitated by Privacy and Availability, and we will challenge the necessity of this trade off through the introduction of homorphisms for search which preserve privacy through mathematical constructions which map functions of interest from the unencrypted space, to the encrypted space allowing limited computation to be conducted on ciphertext. We will examine the new trade offs necessitated by these trade offs, and discuss their application to domain problems from NASA, the FAA, public health, and civic governance.