Dear Center for Long-Term Cybersecurity Committee,

In an environment marked by monitoring and data retention, simple actions like making an online purchase can carry implications into the future. Technological advances let merchants track our behavior with increasing granularity, link personal data from different sources, and make predictions about our future actions. The list of actors that are interested in our personal data is long: Companies buy it in the hopes of targeting us with the best products at prices tailored to maximize profit. Governments collect it in the hopes of identifying threats to our security and theirs. Criminals steal it in the hopes of extorting money, using our identity, or attacking our financial accounts. Not surprisingly, a recent survey by the Pew Research Center found that 91% of adults believe that consumers have lost control over how personal information is collected and used by companies.

In the course of my research I have seen how tools for data collection are already changing the relationship between citizens, corporations, and the state. In a recent study, I explore how governments might react to improvements in surveillance technology [1]. Certainly, surveillance is used for many beneficial ends and is not abusive in itself. Yet the analysis shows that with stronger monitoring technology, governments face increasing incentives to abuse their power. In another study, I examine the sharing of purchase data among merchants [2]. According to a game theoretic model, consumers do not properly account for the future consequences of each purchase, reducing their resulting surplus. Both examples highlight how threats to citizens may emerge from the combination of many individual behaviors.

Building on these previous studies, this research initiative aims at two sweeping questions: How does personal data affect the balance of power between citizens, governments, corporations, and criminals? Furthermore, what technologies and policies can maintain a playing field that protects individuals? To answer these questions, my team will blend tools from economics with analysis of network architecture. We will use models to predict future trends, identify effects, and highlight key takeaways that may benefit future architectures and policies. Support from CLTC will allow me to hire student researchers, while providing an environment of peers to help focus our work in fruitful directions.

I thank you for your consideration.

Paul Laskowski

Visiting Assistant Professor

UC Berkeley School of Information

[1] P. Laskowski, B. Johnson, T. Maillart, and J. Chuang. Government Surveillance and Incentives to Abuse Power. In Proceedings of the 13th Workshop on Economics of Information Security (WEIS). June 2014.

[2] B. Johnson, P. Laskowski, T. Maillart, J. Chuang, and N. Christin. Caviar and Yachts: How your Purchase Data May come back to Haunt You. In Proceedings of the 14th Workshop on Economics of Information Security (WEIS). June 2015.

What is the real-world relevance of this project? (1-2 sentences maximum)

This initiative aims to identify ways in which technologies for collecting personal data lead to abuses of power against individual citizens. It also seeks to develop recommendations for technology suppliers and policy makers to maintain a playing field that protects individuals.