Digital Life Seminar Series
Spring 2018

Guest Speakers
Nicki Dell & Tom Ristenpart
Cornell Tech
&
Karen Levy
Cornell University

Digital Safety & Security for Victims of Intimate Partner Violence
www.dll.tech.cornell.edu

Nicki Dell is an assistant professor focused on Human-Computer Interaction and Information and Communication Technologies for Development, with a focus on designing, building, and evaluating novel computing systems that improve the lives of underserved populations in low-income regions.

Karen Levy is an assistant professor with expertise in law, sociology, and information science. She researches how law and technology interact to regulate social life, with particular focus on social and organizational aspects of surveillance. She is also interested in how data collection uniquely impacts, and is contested by, marginalized populations.

Tom Ristenpart is an associate professor in computer science. His research spans a wide range of computer security topics, with recent focuses including digital privacy and safety in intimate partner violence, new threats to, and improved opportunities for, cloud computing security, confidentiality and privacy in machine learning, and topics in applied and theoretical cryptography.

Abstract: Digital technologies, including mobile devices, cloud computing services, and social networks, play a nuanced role in intimate partner violence (IPV) settings, including domestic abuse, stalking, and surveillance of victims by abusive partners. This talk will survey recent and ongoing work in understanding technology’s role in IPV and improving technologies to increase privacy and safety for victims. A recent qualitative study will be discussed that was conducted in collaboration with the New York City Office to Combat Domestic Violence. Findings from semi-structured interviews with 40 IPV professionals and nine focus groups with 32 survivors of IPV reveal a complex set of socio-technical challenges. The intimate nature of the relationships involved undermine the threat models underlying common security and privacy tools, which allow even technically unsophisticated abusers to install spyware on victim devices, compromise social media accounts, and post abusive Facebook messages that remain undetected by the platform. Exploration of the current support infrastructure and procedures used in this context find that professionals and victims alike feel overwhelmed by tech-born threats and that there are no best practices for tech safety in IPV. The work performing a technical measurement study of smartphone spyware, which is easily obtained by abusers from the Google play store or the web, will be discussed. A complexity here is “dual-use” software such as Find My Phone type apps, which are being repurposed by abusers to work as spyware. The work regarding evaluating existing anti-spyware tools, which prove to currently be unsuitable for the IPV context, and an outline citing ongoing and future work on improving victim safety and privacy will be discussed.

This talk will cover joint work by: Nicola Dell, Peri Doerfler, Rahul Chatterjee, Diana Freed, Sam Havron, Karen Levy, Damon McCoy, Diana Minchala, Hadas Orgad, Jackeline Palmer, and Thomas Ristenpart.