The next generation in the field of the science of cybersecurity is to focus on security and privacy for *all* users, not just security and privacy for some. Additionally, the next generation in the field of the science of cybersecurity must engage with the fact that cybersecurity advances that are good for one stakeholder group (e.g., the government or law enforcement) may create dynamics that disadvantage (or, worse, harm) other stakeholders. In order to fully investigate these dynamics and make their consequences clear to the research community, we must bring not only a computer science perspective but also legal and sociological lenses to our work.

The 2022 paper “Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives” presented at USENIX Security is an example of the science of cybersecurity that advances the field along the axes laid out above. It studies a technology created for government (electronic monitoring technologies used by law enforcement) that, due to the complexities of the real world, result in unacceptable harms to people under probation, parole, or other legal reasons for pervasive electronic monitoring.

Owens et al. examine the understudied phenomenon of carceral technology and electronic monitoring from multiple perspectives, connecting technical, legal, and human-centered findings to expose the promise of this technology as false: While electronic monitoring is often sold as a liberatory technology that will allow more people to serve legal sentences while living freely outside incarceration, the reality is that electronic monitoring is pervasive and overreaching, prone to mistake and bugs, and ultimately introduces new privacy and security risks to an already marginalized and vulnerable population.

Through analysis of apps, privacy policies, and user reviews, this multidisciplinary paper lays a thorough groundwork for further work in this critical area. This paper presents the first systematic analysis of the electronic monitoring app ecosystem, and connects it to other known bad actors like third-party trackers and data brokers. It could have stopped there and still represented an important contribution, but extended further to understand both the experience of the users subjected to this technology and the legal context that puts parolees and probationers at a disadvantage.

This is the work the science of cybersecurity should be advancing: using novel technical analysis and findings to have an impact on the lives of real people embedded in social and legal power dynamics. Work like Owens et al.’s is how our field will create connections with other scientists and scholars to multiply our impact and advance the state of the art more rapidly and thoroughly than we as cybersecurity researchers and practitioners can alone.

Thank you for considering this nomination.