Courses for understanding the impact of privacy and security choices

Emily McReynolds
Program Director, Tech Policy Lab
University of Washington

Launched in September 2013, the Tech Policy Lab aims to strengthen and inform technology policy through research and education. The Lab brings together experts from the University of Washington School of Law, Information School, and Department of Computer Science and Engineering and other units on campus. We research complex policy issues such as augmented reality, big data, and the Internet of Things. Our goal is to help bridge the gap between rapidly emerging technologies and the policies that historically have lagged behind and to foster conversation between technologists and policymakers. We also work to improve the pipeline of technologists into policy, as part of our work we have developed courses for undergraduate and graduate students.

Discussing privacy with students reflects the number of different interpretations of privacy. For many of them, privacy is an abstract term and it is only when asked if they would want certain types of conversations, photos etc. available to the public that privacy becomes tangible. I have found that immersive opportunities where students can experience the technology and discuss its implications with those who focus on policy, leads to significant interest in further usable privacy and security projects.

The Tech Policy Lab has organized two courses thus far to help students, at both a graduate and undergraduate level, interact with policy.

Interdisciplinary Tech Policy Seminar

In winter quarter this year I organized a seminar that included both law and engineering graduate students. The goal was to attract computer scientists with an interest in law and policy, and law or policy students with an interest in technology. The course was organized such that each week a combination of a law student and engineering student presented on a topic of interest to them. They were required to meet with the seminar lead in advance to assure they represented both the policy and the technology. Topics included mobile privacy, drones, online harassment and cell site simulators. At one point or another in all the presentations privacy came up and led to significant discussion.

Drones and privacy

(adapted from Prof. David Hendry's description of the course)

Working in teams, the 28 students, about half enrolled in the Informatics program at The Information School, were positioned to learn about value sensitive design by investigating the design space and value implications of *personal drones* – an emerging category of personal technology.

The Tech Policy Lab provided Prof. Hendry with funds to purchase some drones for the class project. These were toy drones, equipped with video cameras, which can be flown with a special-purpose controller or smart phone. Students used these toy drones to create videos of value scenarios, stories which envision future uses of personal drones, value implications, and policy challenges. Students, in turn, asked stakeholders to view their videos and conducted interviews. This design and empirical work, along with initial conceptual investigations of direct and indirect stakeholders, led to a careful assessments of the of potential value implications of personal drones.

Value implications included privacy, safety, personhood, solitude, and creative expression. Students produced work which explored a wide range of scenarios of the future – drone use for child safety and security, how drones might be used by the visually impaired, a digital photo assistant drone for taking family photographs, the use of personal drones to attack home-based wireless communication systems, and using drones for home security.

Unit in Introduction to Computer Security

In an undergraduate computer security course this quarter, one of the classes was dedicated to policy issues in security. I worked with the professor on the topics had come up during the first six weeks of the class, and then I did a four-part presentation that broadly covered encryption, the Computer Fraud & Abuse Act, surveillance laws, and biometric passwords. The purpose of the presentation was to cover issues the students were interested in but also to encourage discussion of usable security and real-life impact of technical choices.