Intersect, Vol 8, No 3 (2015)

The Techno-Political Collision: Preparing a New Generation of Policy-Minded Technologists

Zak Whittington
Stanford University

The worlds of computer science and policy are on a collision course, and tomorrow's technologists are not being adequately prepared for this reality. As computing systems diversify and become more intricately integrated into our lives, the creation and maintenance of ethical, practical, and fair technology policy has become manifestly critical. Policymakers and the American public are faced with a growing array of difficult decisions to make regarding what role technology will have in our lives over the coming years. How will we prioritize privacy and security? How much personal information should we share, and with whom should we share it? How tolerant should a liberal society be of cyber espionage and warfare? Is access to information a human right?

In the past, these questions may have seemed like the stuff of abstract philosophical treatises or of science fiction, but the answers we settle on are being codified by engineers and cemented in silicon right now. The demand for cross-disciplinary, ethically conscious engineers and technically savvy social scientists is currently outpacing supply. The most promising solution lies in education. College administrations, and particularly departmental administrations, have unique leverage to manipulate what students learn and how they think, and thus have great influence over the skill sets and cultural norms of the technology industry. Departments can draft experimental curricula, create new interdisciplinary classes, tweak major requirements, and generate opportunities for student groups. While some universities have recently begun to utilize this leverage, the educational landscape on the whole is leaving young technologists woefully unprepared for the complex world they are about to enter. This paper is a call to computer and social science departments across the country to invest more seriously in the intersection of technology, politics, and ethics.

The risk involved with bad tech policy and uncritical engineering is not abstract; tangible examples of controversy and catastrophe already exist. The most visible and poignant example in recent years has been the NSA surveillance practices exposed by Edward Snowden. Thanks to one man, the government and the public have been made aware of surveillance practices that are both inconceivably vast and, according to a federal appeals court, completely illegal (Greenberg, 2015; Savage and Risen, 2015). The NSA has unlawfully intercepted the communication of essentially every American and countless foreign nationals, fundamentally weakened the security of the internet as a whole by purposefully breaking popular encryption algorithms, blatantly lied multiple times to Congress and to various members of the executive branch, and essentially ensured the continuation of these practices by creating a secret (and illegal) interpretation of the Constitution and the USA Patriot Act, completely undermining the federal judiciary and thus shirking the entire system that was designed to constrain it ("NSA Spying," 2015). The saddest part of the whole story is that it took over a decade for one of the thousands of NSA employees to feel uncomfortable enough about the innumerable abuses of power to actually speak out about them. Yet this culture of apathy is not surprising when one considers that the majority of those technical employees were likely trained at engineering schools that lacked any cultural or pedagogical discussion of ethics or policy.

Less visible but highly important examples of ethical apathy and political ignorance abound. Fundamental misunderstandings by politicians of the distinction between whitehat (benevolent) and blackhat (malicious) hacking has created a system of incentives that heavily disfavors constructive probing of software, putting a security industry that is increasingly outmanned and outgunned at another disadvantage (Chickowski, 2015). Public inattention to the software patent debate has created a software world where corporate giants like Apple spend significantly more on patent litigation than the actual development of their products, and smaller companies enter the software market only to be immediately rendered unable to legally operate as they are overcome by patent trolls (Kamdar *et al.,* 2015). The failure to provide basic legal protections for companies who have been the victims of data breaches has actively put consumers at risk, and has made such breaches more common by disincentivizing coordination in the industry against such attacks (Jaycox and Tien, 2015). Moreover, as technology becomes more integrated into our lives, opportunities for policy failure are increasing in both frequency and magnitude. Will we be prepared for the first fatal accident involving a self-driving car? Will implantable technologies protect the elderly and the sick, or will they be co-opted by insurance companies to raise premiums in real time? Will the first artificially intelligent construct we create benefit humanity or completely destroy it, as Stephen Hawking and Elon Musk both fear (Luckerson, 2015)?

A common sentiment among those in the STEM fields seems to be that these policy questions should be left to the politicians. Yet it is thanks to this problematic attitude that the policy landscape in the field of technology today is so ineffective. Transcending this mindset is a question of shifting cultural norms in the tech community, an effort that can be accomplished by a shift in curricular priorities at the undergraduate level. Stanford professors like Eric Roberts and Steve Cooper have repeatedly advocated for a stronger ethical emphasis in computer science coursework. That emphasis can come in the form of a standalone, ethics-centered class such as Cooper's "Computers, Ethics, and Public Policy" class, or it can be peppered throughout preexisting coding courses. Simply periodically stopping to ask, "*Why* do we care about the project we're coding?" and "How can this technology be used or misused?" could help students build an awareness of the impact of their code.

The good news: examples of interdisciplinary education at the intersection of tech, politics, and ethics already exist, though they are primarily at the graduate level. Citizen Lab at the University of Toronto brings together incredibly skilled network security experts, lawyers, and social scientists not only to study online human rights abuses from an academic perspective, but also to actively create technological solutions for them. Likewise, the Liberation Technology department at Stanford brings together academics from multiple fields to study how technology can be used to improve governance and pursue a variety of other social goods. Similar groups exist at schools such as Harvard, MIT, the UW, and UC Berkeley, but a commonality among them is that they focus on post-graduate projects and fail to provide sufficient resources for undergraduate students to meaningfully change student norms or culture, as would be needed to change the tech industry. Moreover, as separate interdisciplinary programs, they have limited influence over departmental rules. Nonetheless, these programs may serve as valuable models for parallel undergraduate programs, or at least provide inspiration for potential topics of study as well as access to experts in those topics.

The end goal should be threefold. First, train all programmers to develop an intuitive sense for the possible ethical ramifications of their work, in a similar manner to the way that we currently train programmers to constantly consider potential security flaws in their code. By making this an integrated part of the coding process and an ever-present question on programmers' minds, fiascos like the abuses at the NSA will hopefully be mitigated in the future.

Second, emphasize the importance of acquiring basic coding proficiency among social science students who choose to study technology. Sadly, this seemingly commonsense idea is shockingly progressive. As an undergraduate who studied political science at both Stanford and the Oxford Internet Institute, I have come across an exceedingly large amount of literature written by social scientists that clearly had no technical understanding of the technology they were studying. Literature written in this manner is prone to false conclusions, incomplete or misinterpreted evidence, and oftentimes unrealistic, impractical, or inane policy recommendations. While the field seems to be somewhat improving on this front, most of the research in "Internet studies" from the mid-2000s is now completely obsolete. This problem also exists at the policymaking level, as Congress has in multiple cases passed technology legislation mandating practices that are practically unimplementable, such as the SOPA/PIPA antipiracy bills of 2011, and David Cameron's recent push to censor pornography in the UK.

The third and final goal should be to encourage more students to directly study technology policy. Demand for tech policy experts is unmet at every level—in the federal government, local governments, NGO think tanks, non-profits and advocacy groups, and the private sector. Clearly, tech policy is a somewhat niche field, and it would be unrealistic (and probably counterproductive) to expect every technologist to also be an expert in policy. However, steps can still be taken to encourage more students to enter this field, and speaking from personal experience—corroborated with the experiences of colleagues from other schools—not much is currently being done towards that end. Computer science students are constantly and lavishly wooed by software development firms that vie for their attention by coordinating advertising campaigns on campuses, giving away free merchandise, and above all, offering unheard-of salaries and benefits to interns. Firms operating in the technology policy space often cannot compete with the financial resources of tech giants like Apple or Google, and so deserve some assistance from university faculty and programs.

By encouraging computer scientists to think more critically about the political and ethical ramifications of their work, universities would be improving the policy frameworks that constrain and steer technological innovation. In doing so, they will be helping ensure the continued peaceful and beneficial integration of technology into our society and culture. The worlds of technology and policy inevitably will grow more entwined; the question is whether we can be prepared enough to keep good policy one step ahead of bad technology.

References

Chickowski, Ericka. (2015). President's Plan To Crack Down On Hacking Could Hurt Good Hackers. *Dark Reading*. InformationWeek, 21 Jan. 2015. Web.

Greenberg, Andy. (2015) Court Rules NSA Bulk Data Collection Was Never Authorized By Congress. *Wired.com*. Conde Nast Digital, 7 May 2015. Web.

Jaycox, Mark, and Lee Tien. (2015). EFF Statement on President Obama's Cybersecurity Legislative Proposal. *Electronic Frontier Foundation*. The Electronic Frontier Foundation, 13 Jan. 2015. Web.

Kamdar, Adi, Daniel Nazer, and Vera Ranieri. (2015) Defend Innovation: How to Fix Our Broken Patent System. *Electronic Frontier Foundation White Papers* (2015). The Electronic Frontier Foundation, Feb. 2015. Retrieved from https://www.eff.org/files/2015/02/24/eff-defend-innovation

Luckerson, Victor. (2015). 5 Very Smart People Who Think Artificial Intelligence Could Bring the Apocalypse. *Time*. Time, 2 Dec. 2014. Web.

"NSA Spying." (2015). *Electronic Frontier Foundation*. The Electronic Frontier Foundation, n.d. Retrieved from https://www.eff.org/nsa-spying

Savage, Charlie, and James Risen. (2015). Federal Judge Finds N.S.A. Wiretaps Were Illegal. The New York Times. The New York Times, 31 Mar. 2010. Web.