I believe the biggest challenge facing computing and computer science today is privacy and security. I combine these two because they're mutually dependent. Privacy requires security and the existence of security implies the existence of privacy. Essentially you can't have privacy without security and security creates privacy no matter what.

Luckily, most people in the computer science community and especially the security seem to agree that security is a good thing. The problem here isn't on our end. It is, however, our responsibility to fix it. It takes a degree of understanding of the concepts behind encryption to understand *why* we can't, for example, build a back door that only one party can use, and it can't reasonably be expected of everybody to have that understanding. Especially for people whose jobs are in no way related to math or computer science.

The first half of this issue is, for me, the more morally based of the two. Privacy allows for new ideas to breed and thrive, where the lack of privacy would see those ideas crushed at the first sign of challenging the way things are. Without the ability for form and grow new ideas, culture and civilization can't evolve and thrive to the point that they have today and could tomorrow. Of course, that is both the argument for and against privacy, because those new ideas can also be genuinely morally horrible. I believe that is a smaller harm than the good that comes from allowing the rest. The greatest common good comes from facilitating privacy.

More than that, however, I believe privacy is a human right. We have the right to live our lives without the fear of someone, somewhere constantly watching over our shoulders to catch any mistakes we make. That kind of surveillance is crippling on every level.

The other half of the issue, security, is more of an issue with the fact that good encryption is just an implementation of certain maths. The security comes from the math, not the programming. It isn't possible to have a secure system with a backdoor because that backdoor has to be a weakness in the encryption itself, which means anybody can use it. Good guys and bad guys. Even if it were morally right to give an individual or organization a way to invade other people's privacy, it's not technically possible.

The problem, then, is the people designing legislation for this issue. Groups of people who can't be rightly expected to understand the technical issues are demanding morally wrong and actually impossible things, and the computer science and security communities need to push back with full force. So far, we've done pretty well for the most part. Some companies participate in the invasion of our privacy, but most of them are unwilling and push back to the full capability of the law. Recently Apple successfully lobbied against the FBI and were not forced to provide a way to break in to the San Bernardino shooter's phone. Hopefully they'll also be able to fix whatever method the FBI exploited to do it without Apple's help, but that's not the focus of this paper.

Unfortunately, there's only so much we can expect large companies to do to fight the government's invasion of our privacy. We can expect them to do everything possible within the law and not one step more. Anything beyond that, including noncompliance with morally black demands, falls to individual programmers, security experts, and computer scientists. The ability to say “no” is a characteristic of someone in a profession, which we are.