The Moral Failure of Computer Scientists

In the 1950s, a group of scientists spoke out against the dangers of nuclear weapons. Should cryptographers take on the surveillance state?

Brian Snyder / Reuters

KAVEH WADDELL

DEC 11, 2015 | TECHNOLOGY

TEXT SIZE − +

Computer scientists and cryptographers occupy some of the ivory tower's highest floors. Among academics, their work is prestigious and celebrated. To the average observer, much of it is too technical to comprehend. The field's problems can sometimes seem remote from reality.

But computer science has quite a bit to do with reality. Its practitioners devise the surveillance systems that watch over nearly every space, public or otherwise—and they design the tools that allow for privacy in the digital realm. Computer science is political, by its very nature.

That's at least according to Phillip Rogaway, a professor of computer science at the

University of California, Davis, who has helped create some of the most important tools that secure the Internet today. Last week, Rogaway took his case directly to a roomful of cryptographers at a conference in Auckland, New Zealand. He accused them of a moral failure: By allowing the government to construct a massive surveillance apparatus, the field had abused the public trust. Rogaway said the scientists had a duty to pursue social good in their work.

He likened the danger posed by modern governments' growing surveillance capabilities to the threat of nuclear warfare in the 1950s, and called upon scientists to step up and speak out today, as they did then.

I spoke to Rogaway about why cryptographers fail to see their work in moral terms, and the emerging link between encryption and terrorism in the national conversation. A transcript of our conversation appears below, lightly edited for concision and clarity.

Kaveh Waddell: Why should we think of computer science as political—and why have many considered it to be apolitical, for so long?

Phillip Rogaway: I think that science and technology are inherently political, and whether we want to think about it that way or not, it's the nature of the beast. Our training as scientists and engineers tends to deemphasize the social positioning of what we do, and most of us scientists don't give a whole lot of thought to how our work impacts society. But it obviously does.

It's not something easily taught, either. I've taught an ethics and technology course myself, for several years, and the students are not predisposed to get the message that things technological are also political. We tend to analyze what we're working on from a very self-directed perspective. [We focus on] how it impacts us and how it impacts the small group or the company with which we're dealing, and the broader social influences of what we do aren't usually on the horizon.

Waddell: What led you to understand the political implications of your own work?

Rogaway: I myself had been thinking increasingly in these terms when the Snowden revelations came out. Those revelations made me confront more directly our failings as a community to have done anything effectual about stemming this transition of the Internet to this amazing tool for surveilling entire populations.

"With the transition to a state of total surveillance, what we have is a slow forfeiture of democracy."

Waddell: In your paper, you compare the debate over nuclear science in the 1950s to the current debate over cryptography. Nuclear weapons are one of the most obvious threats to humanity today—do you think surveillance presents a similar type of danger?

Rogaway: I do. It's of a different nature, obviously. The threat is more indirect and more subtle. So with nuclear warfare, there was this visually compelling and frightening risk of going up in a mushroom cloud. And with the transition to a state of total surveillance, what we have is just the slow forfeiture of democracy.

Waddell: Who else in the wider class of scientists—besides nuclear scientists, besides computer scientists—has this level of political responsibility?

Rogaway: I think this holds for all scientists and engineers. Very few of us are doing something so esoteric that it's unlikely to end up connected to the social well-being. If you're going to exclude people, maybe pure mathematicians, for example. But we live in an age of technology, and what scientists and other technologists do reshapes the character of our world.

Waddell: Are there any other historical examples of scientists acting according to moral principles rather than pursuing pure academic inquiry?

Rogaway: I allude to a couple of others in the paper. Rachel Carson [a scientist and environmental activist] is a nice example. There are activist scientists; they're not a popular breed, but they exist. The Indian activist-physicist—Vandana Shiva, the seed activist—is one of the most prominent activist-physicists, frankly.

There is a tradition, especially in physics, of activism. But computer scientists have not tended to be active in the political sphere. I do think there were some during the "Star Wars" debates—some computer scientists who were questioning the viability of building the kind of system that Reagan was envisioning, and saying that this was really far beyond the capabilities of contemporary computer science. So it's certainly not unheard of for scientists to be playing a role here.

Waddell: What is it about physicists that makes them particularly likely to be involved in this sort of thing?

Rogaway: I do think it's a legacy of the experience of the Manhattan Project. I think we in some ways live the continuation of our histories, and that's something that's been internalized among many physicists.

And I give the example that, at my own university, how the physicists were the only group outside of the humanities to call for the chancellor's resignation in the aftermath of the pepper-spray incident. Somehow, that wasn't surprising to me. My colleagues in the physics department say that these kinds of questions are routinely discussed, and I don't think that's true in engineering departments in general.

Waddell: Is there any inherent danger in politicizing an academic discipline? I think a lot of people are drawn by the fact that academia allows this curiosity-based inquiry. Is there anything that can go wrong when politics comes in?

Rogaway: My sense is that politics is there, whether one acknowledges it or not. When you have an ostensibly apolitical department, but you scratch beneath the covers and discover that three-quarters of the faculty are funded by the Department of Defense, well, in fact that's not apolitical. That is very much working in support of a particular ethos, and one simply hasn't called it forth.

Waddell: Does tenure have a role to play here? Does tenure help academics focus on socially important goals, or does it divorce them from reality?

Rogaway: In principle, the tenure process should free academics who have already been tenured to venture out and question matters in a way that could offend power. In practice, it doesn't seem relevant. By the time a faculty member is tenured, it's likely that his or her way of seeing the world will have already been so set that they're very unlikely to become political at that point if they haven't been already.

"When three-quarters of the faculty in a department are funded by the Department of Defense, well, that's not apolitical."

Waddell: You've criticized the typical law-enforcement framing of what the FBI director James Comey likes to call the "going-dark problem." Explaining the risks of strong encryption, he testified this week in front of the Senate Judiciary Committee, saying that "encryption is part of terrorist tradecraft now." What do you think of this sort of framing?

Rogaway: In the talk that I gave [this week], I described two utterly different framings of what surveillance is about: the law-enforcement framing, and the surveillance-studies-style framing. James Comey has come out repeatedly with these sort of talking points from the law-enforcement framing. I don't believe they ultimately stand up to close scrutiny.

It involves a whole bunch of related beliefs, starting with the fact that privacy and security are in opposition with one another, and that there are all these "bad guys" out there, and technology has been a boon to them, because now they have encryption at their disposal.

"We run the risk of going dark." That's the phrase that James Comey uses. A world of dark, locked closets. I think the entire framing is this sort of discourse in fear, to make people believe that we need this almost father figure to protect us, and that we're going to have to give up some civil liberties to do so, but that's somehow for the social good.

I don't think any of it ultimately makes sense, starting from the beginning, that privacy and security are routinely in opposition to one another, and going on through the presumed effectiveness of denying the population access to effective privacy tools, that that will somehow help in a fight against terrorism.

I don't think terrorism has much to do with the mass-surveillance issue at all. This is a convenient storyline to be weaving in the present day, but the NSA's own mission statement says that they're there to serve their customers. And while some of those customers are interested in terrorism, other NSA customers have completely unrelated interests, and I don't think that surveilling is particularly aimed at confronting terrorism. It wouldn't be effective even if it were.

Anyone who really wants to encrypt their communication is going to find a method for doing so, whether it's bundled with mass-market products or not. When you make encryption harder to get for ordinary people, you don't deny it to terrorists. You just make the population as a whole insecure in their daily communications.

Furthermore, law enforcement has an extraordinary set of tools available to them now. An unprecedented set of capabilities, both for law enforcement and intelligence services. These aren't somehow the dark times for either law enforcement or intelligence. These are the times of extraordinary information. Nowhere in history has it been so easy to learn so much about everybody. So, in some sense, we're really talking about protecting the smallest remnants of remaining privacy.

"An ideology that is not consistent with being a scientist is to say, 'What I do has no impact, and I have no responsibility.' That's just not true."

Waddell: There's no question that terrorists are using technology to their benefit. Should computer scientists be doing anything about this?

Rogaway: Criminals are always going to use technology to their benefit, just as ordinary people are going to attempt to do so. I don't believe that anyone is going to change that basic truth. Fortunately, criminal behavior has never been such a drag on society that it's foreclosed entire areas of technological advance.

Waddell: You touch on a few recommendations for academics who are looking to be more involved, to get people to care—morally—about their role in blocking mass surveillance. Should morality be a criterion of hiring?

Rogaway: I think that when you're hiring faculty members at a public university, that it's fair game to ask them what their social views are, their views of social responsibility of scientists. I think you have to be careful in how you do this that you're not applying some kind of political test, that the candidates' political opinions match up with your own.

But part of the purpose of the public university, land-grant universities like my own, is to serve the public welfare. And if a faculty candidate doesn't believe that that's a part of the purpose of his or her work at all, then I think that that's not appropriate.

But again, I think one has to be quite careful in how this is applied, that it doesn't become some sort of political test. There's a wide range of ideologies that are perfectly consistent with being a scientist or a faculty member. But one kind of ideology that to me is not consistent is to say, "What I do has no impact, and I have no responsibilities." Because that's just not true.

Waddell: What about the issue of funding? The fact that so much of the money for the work that academics do comes from the parts of the government that are involved in surveillance—is there a way around that?

Rogaway: Faculty members can decide what funding they will or will not seek. But it's very rare for a faculty member to say, "I'm not going to accept DoD funding," for example. I think that viewpoint should be more common, actually. That some people should say, "I won't accept from this agency, I don't agree with their institutional goals."

“When you make encryption harder to get for ordinary people, you don’t deny it to terrorists. You just make the population as a whole insecure in their daily communications.”

Waddell: Is that a practical proposition?

Rogaway: It’s perfectly practical, in the sense that you can be a successful faculty member without accepting DoD funding. You won’t have as many students, you won’t be able to support as large a research group. And in some areas of computer science, and I’m sure in some areas more broadly, the vast majority of funding may be from the DoD.

I remember speaking to a computer architect, asking if there was any person in computer architecture he was aware of that wouldn’t take DoD money, and he said there was not. And he didn’t really believe that such a person could exist and be successful in the field, as there is no access to adequate resources just from the [National Science Foundation], say.

In my own area, cryptography, I think one can do fine living just on NSF money. But you won’t have a group of 10 students, or something.

Waddell: The paper and the talk you gave are pretty critical of your colleagues in the field. How have they taken the criticism since you presented the paper?

Rogaway: I’ve received a great deal of feedback, and almost all of it has been positive. Even from faculty members whose research is kind of directly impinged. So I believe the thoughts expressed in the piece exist as a kind of undercurrent in lots of people’s thinking. It’s just uncommon to give voice to them. I’ve received a great many positive emails and thanks and essentially no negative ones. Maybe those people just aren’t talking, I don’t know!

Waddell: What do you think is the moral role of journalism and the media in covering these issues?

Rogaway: First of all, I think journalism is quite threatened by the possibility of being continually surveilled. It's surprising to me that journalists aren't fighting harder to ensure that they have good and easy access to the tools for privacy.

Perhaps it's an indication of the decline of investigative journalism, the number of people that are really doing investigative journalism, that journalists aren't more up in arms about revelations, for example, that many journalists are being surveilled, and it's probably beyond the technical capabilities of most of your potential sources to actually avert modern surveillance.

And in a world in which journalists are denied access to sources that can speak up free of fear of governmental intrusion, I think this shuts down an enormously important aspect of what makes democracy work. I don't think you can have a healthy democracy without healthy journalism, and I don't think you have healthy journalism without the ability to conduct a private conversation.

And that includes not just what you're saying, but whom you're saying it to. If every contact a journalist makes—and the weight of that contact: the number of minutes, the frequency, and such—is something that hundreds of thousands of analysts can get from a Google-like search tool, I think that this makes serious investigative journalism effectively impossible.

ABOUT THE AUTHOR

KAVEH WADDELL is an associate editor at *The Atlantic*.

Twitter Facebook Email