Editors: Bob Blakley, bob.blakley@gmail.com | Lorrie Cranor, lorrie@cmu.edu

A Discussion of Public Health, Trust, and Privacy With Susan Landau

Bob Blakley: Welcome to *Over the Rainbow*, the IEEE podcast about 21st-century security and privacy. I'm Bob Blakley; I'm an operating partner at Team8 and also past general chair of the IEEE Symposium on Security and Privacy.

Lorrie Cranor: And I'm Lorrie Cranor. I'm a professor of computer science and engineering and public policy at Carnegie Mellon University, where I direct the CyLab Security and Privacy Institute, and I codirect the privacy engineering master's degree program. I recently became codirector of the new Collaboratory Against Hate: Research and Action Center at Carnegie Mellon and the University of Pittsburgh.

Blakley: This is our inaugural edition of the *Over the Rainbow* podcast, and I couldn't be more pleased to have as our first guest Susan Landau. Susan, welcome to the show. Thank you very much for joining us, and would you like to introduce yourself?

Susan Landau: Thank you very much for having me! I'm Susan Landau. I'm the Bridge Professor of Cybersecurity and Policy at the Fletcher School and at the School of Engineering's Department of Computer Science, both of them at Tufts University. I direct our new master's degree in cybersecurity and public policy.

Blakley: You've recently published a new book; it's called *People Count: Contact Tracing Apps and Public Health*, and I think it's fair to say that one of the major themes in the book is that public trust is an essential element of public health campaigns. It struck me, reading the book, that not only is public trust at sort of a historic low point but that that's not an accident—that public trust is being undermined deliberately, both as a matter of political conflict and as a matter of international and ideological conflict. Maybe you could reflect, for a minute, on the broader problem of disinformation in matters where public discourse is important.

Bob Blakley.

Lorrie Cranor.

The Problem of Disinformation

Landau: It's become even harder, of course, during the pandemic, where we don't see each other. I think, in the United States, a lot of this stems from the withdrawal of the fairness doctrine that happened under President Reagan. Prior to that, television programs had to run fair and balanced coverage. And that's no longer true, and what we've seen, of course, is support—almost all on the right—for what I would call very unbalanced coverage. And people who get their news from FOX and so on are not seeing balanced stories, and they don't have an ability to understand that they're not seeing balanced stories.

Other countries, in particular Russia, have certainly taken advantage of that for the United States. China does disinformation, but it does it largely internally, though it does some of it to countries in the South China Sea, where it's having political battles. But, mostly, the control that China exercises is internal, whereas Russia's is both internal and external.

It's very dangerous—and we don't know how to combat it well. The Baltic countries, which have dealt with Russian disinformation for decades, have been educating their public about how to think analytically about what they hear. We have largely done away with civics for students, and that's something that we probably need to bring back so that students understand the balance of powers, separation of powers, and how to think analytically.

Digital Object Identifier 10.1109/MSEC.2021.3092956
Date of current version: 3 September 2021

The Example of Fort Apache

Blakley: One of the things that I really liked about the book was that it's not all bad news, and that you have a couple of stories in the book that are actually really positive. I thought that some of your stories about public health systems that responded well to the pandemic by building on social understanding and social trust were really pretty hopeful, and I enjoyed them a lot. Do you want to say a few words about the case of Fort Apache?

Landau: You and I and Lorrie are all computer scientists, and Lorrie is the best of us at actually reaching out to people and thinking about the people side of security and privacy. We tend to work with technology, and it was a real education to talk to people working in public health and doing contact tracing and see the extent to which they needed to understand the people that they were working with.

The contact tracers, as opposed to the public health people, when they start contact tracing, they don't ask, "Who have you been with?" They ask, "How are you doing? What do you need? Do you need help if you're isolating at home?" The contact tracers working on Ebola in Liberia would ask if people needed food brought in, and they would arrange it. The ones that I talked to had funding from Partners in Health to pay for the food; they didn't bring the food themselves, but the neighbors did—to prevent the family who had potentially been exposed to Ebola from going out.

The contact tracers whom I've talked with who dealt with syphilis, some of them would actually take patients to testing and so on. And, in one case, somebody was driving some 140 mi back and forth to pick up this woman, take her to get tested, and bring her back home. And so that was really interesting to me; it was a different view of science and health than I had.

The case of the Fort Apache Reservation was really interesting. As we know, health on the Native American reservations in the United States is poor. People are poor. There are diseases of various sorts, and people are also often quite far from emergency help.

And so the contact tracers and public health thought hard about how they were going to handle this problem, and they did two things that were really important in keeping fatality rates down. The first was that, when they went to a family, if there was any incidence of COVID in the family (people on the reservation live in multigenerational homes), they would have everybody measure their oxygen levels through the little oxygen meters that you can stick on a finger.

The reason for that is COVID has what's called *happy hypoxia*, which is that you can be walking around and look like you're fine: talking with people and so on, but your oxygen levels are low—in fact, low enough that, 15 min later, you can be dead. On the reservation, if you're a half hour or an hour from the hospital, that's terrible, of course. So what the public health people and contact tracers were doing was seeing if anybody in the family was infected and had a low oxygen level, so they could bring them in to the hospital early.

The other thing they did was that they took advantage of the fact that they knew that children in Apache families would often go and visit with their other grandparents for an extended period—a week or two—so, if anybody was sick in a family, the contact tracers would turn and ask, "Who are the other grandparents?" They would immediately go and check the health of that other family. That way, the contact tracers could track the situation before it got to a dangerous point. What that talks about, of course, is understanding the culture of the people for whom you're doing public health and contact tracing.

Gaps in Trust

Cranor: That's great that they were able to actually bridge that cultural gap and to do it in a trusting way. You wrote about some of the gaps in trust, especially due to some of the structural racism that we've seen in the United States. I'm wondering if you can comment a bit about how race, and even some of the immigration issues in the United States, made it more difficult to respond to COVID in some communities.

Landau: I'll start, actually, with the immigration issues. There was a study done in Massachusetts about what factors seem to cause higher rates of COVID in communities, and among the factors that were uncovered were a high rate of immigration, working in food service industries, and families living in multigenerational and close settings.

Now, the last one is obvious as to why it would be a problem, especially given the difficulty that older people have with COVID—the higher rate of death there. But the first one, the issue of immigration, stems from the problem that, of course, under the Trump administration, legal immigrants were quite concerned that anybody they knew or any family member who was undocumented—their existence should not be known to the government, including public health.

There was also something called the *Public Charge Rule* that got instituted in early 2020, which said that, if an immigrant or a person in the United States used government services, then he or she would be less likely to get a Green Card and citizenship. So that was a force pushing people away from going for public health help.

And the third thing—working in the food service industry—well, many low-income people do that, and, of course, that creates higher exposure. So when you consider all three factors, it explains why the city of Chelsea had a rate of six times the exposure of the rest of the state early, in April 2020. And it also, of course, explains the death rates in Chelsea and other immigrant communities.

The situation for black Americans is somewhat different. Of course, structural racism has led to black Americans living in communities that are subject to more pollution and, in particular, more respiratory pollution as well as in communities that are what we call *food deserts*, with much less good access to healthy foods, and so on.

There's also been a historic distrust of both the government and public health. The reason for distrust in public health includes the experience in Tuskegee, in which 400 black Americans who had syphilis were left untreated and made the subjects of a study for decades by U.S. public health to see what would happen if they were untreated. This happened even as we discovered that penicillin would cure syphilis.

And then there's the use of black bodies for medical purposes, without the permission of the patients. For example, Henrietta Lacks had ovarian cancer. It turned out that the cells in her particular cancer divided very quickly and kept growing. She died young, but her cells were used in multiple studies over decades. Her family never knew, and she never knew; it was only after Rebecca Skloot started studying the issue while writing *The Immortal Life of Henrietta Lacks* that the family discovered all of this. (Skloot talked with the family as she was writing.) So that creates a historic distrust, not only of the government, but also of public health.

And so now you have a situation in which both of these communities are less likely to interact with contact-tracing apps, which is how I got there in the first place. In the case of communities where people are working jobs at low pay, they often can't afford to stay home from work, and so, unless they are really sick and forced to stay home, many of them don't want to.

But there's also worries about whether the apps are given correct data. The issue for black Americans is the distrust. And for low-income black Americans, there's also the issue of possibly not being in a position to be able to stay home from work on the basis of only the possibility of exposure.

Information Collection and Privacy

Blakley: Obviously, there are great reasons for black Americans and undocumented immigrants to distrust government information collection mechanisms. But, more generally, the information collection practices, not only of the government but also of private businesses, are reported on in ways that expose a lot of flaws and hazards to the public.

So one of the broader themes here seems to be that there is this tradeoff between uses of data that benefit people and privacy versus uses that might operate to their detriment. It seems like an exceptionally intractable issue, both because it's technically very complicated to protect privacy in the face of inference attempts and also because systems tend to be opaque, and any sort of low level of trust is amplified by any mistake. I wonder what your thoughts are about that.

Landau: Facebook and Google continue [to collect information]; people are still using systems [like these] because they can't bear not having the convenience they've grown to depend on. There are the privacy fundamentalists who don't walk around with phones or have their phones shut off and don't use certain kinds of services.

And then there are the parents whose kids are on soccer teams, and the soccer practice announcements as well as whether or not practice will occur during a light drizzle come through a Facebook announcement, and nobody feels like calling. So you show up at the soccer field and discover that no, there isn't a game today. And your kid says, "Mom!—or Dad!—Why can't you get on Facebook, like everybody else?"

So there aren't good answers. The Europeans have tried to restrict how the data are used (but I would say not very successfully) and thrown various wrinkles in the way. We have a case where the technology has gotten way far ahead of social policy.

Now, about the contact-tracing apps: I have problems with the contact-tracing apps. But I also have praise here, and, I have to say, the cryptographers (and the epidemiologists they worked with) jumped in incredibly quickly when they saw the risk that people would carry phones that would release information about exposure.

If you and I both had an app on our phone that used Bluetooth to measure the distance between us and how long we were in that proximity and then later could tell me that you'd been diagnosed, and, therefore, I needed to isolate myself—there are various ways that data could be shared. One way is that all of the data about the exposure on your phone and the phone of everybody who is near you gets shared with public health, and then public health calls me or tells me that I've been exposed.

Alternatively, all of the [anonymized] identifiers you sent out could be shared with public health, and my phone could check with public health periodically and say to you, "Oh, this identifier is one that happens to be the same as one you picked up yesterday! You were near a person who has since been diagnosed." That's a decentralized version that prevents public health from knowing you and I were in close proximity.

Cryptographers came up with that second one: a decentralized app. They did it extremely quickly. COVID was announced to the Chinese World Health Organization office on the very last day in December; the public only became aware of it in the United States sometime in February—though epidemiologists were aware of it somewhat earlier, of course.

But Google and Apple came up with the beginnings of their infrastructure in April, and we had apps running in June. That says a lot about the cryptographers and their ability to get a working system out that protected privacy. The system has other costs, but it absolutely does protect privacy.

Contact-Tracing Apps

Cranor: Speaking of those apps, overall, we have this very privacy-protective app, which is theoretically wonderful. But we haven't really seen much in the way of widespread adoption, and you point out in the book some of the fundamental flaws as far as the human approach to those sorts of apps. This Google and Apple cryptographic approach—overall, was that a win or not? Where do you come down on this?

Landau: So, isn't the right answer, "It's complicated"? We're looking at a disease that spreads easily respiratorily and spreads when somebody is presymptomatic or even when somebody is asymptomatic.

I want to go back to something that happened in February 2020. Genentech—the biotech firm—had a meeting in Boston in February, and it turned out that that conference was a super-spreading incident. One person there (it might have been more than one person that was ill, but it was at least one person) was ill and carried a particular genetic variant of the disease. Tracking through genetic fingerprinting showed that there were 100 people at the meeting who were exposed, got ill, and spread the disease to around 245,000 people by November.

So one can imagine that, if the everybody at the Genentech meeting had had the app and then isolated upon notice of exposure, the spread would have been limited to 100 or 200 or 300 people. Other people in their households might have gotten sick, but not more. Because they all would have isolated, that would have been a tremendous win, and the app would have done it.

That's the positive side of the of the app. Now, let me get to the negative side. Anytime you use a technology, you change how the social impact works. The three of us—I can see it from where I see Lorrie and Bob sitting—are all happily, or at least effectively, working and doing our jobs at home. And while the pandemic has been disruptive, it has been not terribly disruptive to our work—as opposed to somebody who works in the food service industry, or somebody who drives a cab, or a bus driver, or another low-income essential worker.

Now, what happens if one of the three of us gets an exposure notification is that we call our doctor or public health. We say, "I've gotten an exposure notification." They might talk to us and say, "Well, where have you been?" or they might say, "We want you to go get tested, and then we want you to go get tested again in a week," or "If it shows up negative today, we still want you to get tested in three or four days, and then, if you're still negative, we'll want you to isolate just a bit longer."

But the situation will not be terribly disruptive to us. It won't affect our income; it won't affect our lives–it will affect us only in that we don't go to the supermarket. We'll order in, and we can all afford the cost.

For somebody like the people I was describing in Chelsea, an exposure notification is very costly. They can't afford to stop working; they especially can't afford to stop working if the exposure notification is just a notification that doesn't actually end up being a case of COVID. For somebody who works from home, an exposure notification is just a little bit of interruption. You can't walk the dog; somebody has to walk the dog for you. You can't go to the market. That's all.

What you need for the system to work effectively is social interventions. In Switzerland, for example, if you get an exposure notification and public health deems that you should isolate, if you can't work from home because your job doesn't enable you to work from home, the Swiss government will pay enough of your salary for you to afford to stay at home. We don't have that kind of situation here.

There was a study done by people at Harvard that looked at how much it would cost if the state of Massachusetts did that as public policy, and I think it worked out to about US$430 per person—in other words, less than the cost that would be incurred if people went to work under an exposure notification and then turned out to be sick and got other people sick. And that's taking into account the probabilities that the exposure notification is nothing more than a notification you've been exposed, but you don't actually end up ill.

Blakley: So I wanted to go back to something you said a minute ago and give you a chance to come back to it as you said you would. You mentioned the possibility of people reporting their contact or test status inaccurately, either through apps or maybe in other ways. Do you see the potential for essentially malicious false reporting? Do you expect that to happen?

Landau: I think the apps are relatively well designed to prevent that, in the sense that it's only a public health app run by a public health department that can use the Google or Apple infrastructure. And you can only report that you've been diagnosed with COVID after you get a token from public health to do so. There are ways to fool the apps. Serge Vaudenay, a researcher at Ecole Polytechnique fédérale de Lausanne in Europe, has done several papers on this; I would characterize [malicious reports] as in the noise.

That isn't to say they can't be done; there are probably feasible attacks, but we're looking at a situation in which I think we're now at the 3 million mark in the United States;

I don't know how much above 500,000 we are in deaths. So we're not looking at a perfect mathematical situation (like "Factor a 2,048-b RSA number.") We're looking at "What are the tradeoffs?" The apps have been well developed and well designed in that way. But they've been designed in a way that doesn't take into account all of the social factors of an epidemic.

There was a National Academies of Science, Engineering, and Medicine study back in 1993 about the social impact of AIDS. It made the point that an epidemic is both a social and medical phenomenon. I was talking a little while ago about the whole idea of "The app can prevent me from spreading disease if I'm exposed, and it will do so in a way that is not particularly socially expensive for me to do."

But it'll have a different impact on a low-income wage earner who can't afford to stay home, especially if the app registers a number of true exposures, but those don't result in the people exposed becoming ill, and so a person is staying home multiple times when they're not actually ill. In those situations, there hasn't been a social infrastructure built to take care of what happens to those people, so the apps are potentially negative for those people.

Lessons and Future Challenges

Cranor: So, in thinking about some of the lessons that we've learned from this, the Fort Apache intervention seems to have worked, in part, because the contact tracers seem to really understand the social structure of their community. Are there lessons for designers of not just contact-tracing systems but other types of security systems, even corporate security systems, that that we can take from that?

Landau: Of course, and it's funny, of course, for you to be asking me that because what you've been teaching and researching for years is that security and privacy technology is ultimately about people. You have to understand people to develop the technology well. I don't know that I've ever heard you say, "'Educate the user' is wrong," but I've certainly heard it from many people. If your security advice is "Educate the user," then you're approaching security and privacy the wrong way.

The Google and Apple app infrastructure, which is the basis of the COVID apps in many of the U.S. states and much of Europe, is not actually a contact-tracing app infrastructure. It's an exposure-notification app infrastructure. What Google and Apple said, right from the beginning, is that their infrastructure was not meant to replace contact tracers but to supplement their work. However, when Google and Apple came up with what's called *exposure notification express*—essentially a template for the states to use when building their apps ("I will pick a distance of 6 ft and an exposure of this amount of time, and I want this logo on my app page")—it didn't include the option of providing your phone number.

Now, if you're really interested in protecting privacy, you don't want to give the option of providing your phone number. But the Irish app, which was developed earlier using the Google and Apple infrastructure, gave users the option of providing a phone number at the time that they registered the app. And what that meant was that, when a user was exposed, a contact tracer called them.

The users who didn't give their phone number didn't get called by a contact tracer, so they just got the exposure notification on their app on their phone. But the ones who gave a phone number got called by human contact tracer, who then said, "First, how are you feeling? I think maybe you need to call your doctor and go in," or "First, how are you feeling? Okay, I'm going to check in tomorrow and see how you're doing. You need to isolate. Is getting food a problem? Are you safe at home?" Because, of course, some people are not safe at home. And an app can't do that; even if an app asks those questions, it's not the same follow-up as from a human being.

Cranor: So, taking this a step further on lessons, this will, unfortunately, not be the last infectious disease that that we're going to have this problem for, so some have said that these apps that we've built now—it's great that we already have them; we can use them for the next pandemic! But as we've discussed, they're not working that well. So what should we be doing to get ready for the next time that we need this? What should we be doing differently with these apps?

Landau: Thank you! That's in fact how I wrote the book. I wrote the book saying that, by the time the book came out, if all I provided was details on how various apps work, the book would be out of date from the moment it left my hand. What I really wanted to describe to people is how to think about these things.

The apps have to be used as part of a whole public health infrastructure. So, one: you have to provide support for people to isolate; that is, the government has to do so. Two: you have to make sure that the exposure-notification data are only used for the purpose of exposure notification. In Singapore, which uses a centralized system, the Ministry of Public Health does get the data about who's been exposed by whom. Those data have been used in arrests. You have to make sure that the exposure-notification data stay only on [public health applications].

You want to bolster the areas where people won't be using the app as much—so I described why in the book. Black and immigrant communities might be less interested in the app. What happens, when I call up my doctor and say, "I've been exposed: my app says so," and the doctor says, "Go get a test today, and, if it's negative, I still want you to go in three days and get a test again," is that we're moving medical resources to me.

It's great because I've been exposed, and we don't want me to expose anybody else; we want to cut off that risk of further contagion. But, at the same time, we're putting more resources on my health because I have the app. We want to make sure that there's also an equitable use of resources where people are less likely to have the app. So yes, I'm saying fund public health more.

The apps are useful; I described the statistics from the U.K. modeling—because the app there is like all of the Google and Apple apps: you can't tell exactly who got exposed because the data are anonymized; you can't tell if they isolated because the data are anonymized. But statistical modeling indicates that the U.K. app has prevented hundreds of thousands of cases, which is really valuable.

So the apps are valuable, but you have to build them within the context of building public health infrastructure. We haven't asked, "How does this modify public health? How do we then fix it so we have an equitable system?" And that was a failure, I would say.

Of the computer scientists and epidemiologists who were thinking about the problem, to begin with, they did a great job on privacy. They didn't go to the next level to say, "Okay, we're now modifying the public health system. What does that mean?" They wouldn't know the answer because, of course, they're not public health people.

But if they come in, and they say, "We're modifying the public health system; anybody who uses the app will get these resources," then the public health people who think about these problems will say, "Ah! What this means is…, and therefore we need to…." And that's what we should be thinking about now, of course.

Vaccine Passports

Cranor: So, as we're starting to get people vaccinated, now the talk is about vaccine passports, and people have been talking about using technology and privacy-enhancing technology there. So what do you think we should be doing about vaccine passports, and is there a role for technology there?

Landau: I need to be able to show you when I go into a theater or a plane or an airport or another country that I have been vaccinated. And that seems to be very much tied to me. With the exposure notification, I just need to know that I've been exposed. So it's a different kind of tying in. That is, I need to know the information that I've been exposed, but public health doesn't need to, whereas, in the vaccine passport case, the theater or the airport or the country I'm going into wants to know that it's me who has been vaccinated.

I'm old enough to remember having to carry these little yellow booklets that showed that I'd had a yellow fever vaccine when traveling to certain places. So there, technology can make it simpler. I have my little COVID vaccine card, but it's easy to make up paper cards that look just like the COVID vaccine card; you want something that is cryptographically secure that can't be tampered with.

We all know how to do all those things, and it doesn't have to be anonymous. In fact, it can't be anonymous. So the real question, I think, is a privacy question of "When should one have to show that kind of information?" And that's really a social question rather than a technical question.

Cranor: It seems there's also the related privacy issue of if I'm letting people into a building, and I just want to make sure that they're all vaccinated. I actually don't need to know their identities; I just need to know they're vaccinated. So is that a role that cryptography can help us with?

Landau: Sure, and that's the same kind of thing we've been doing with identity management since I worked on the Liberty protocols back in the early 2000s. When I want to drink in a bar, I want to prove that I'm over 18. I don't want to show when my birthday is. I don't want to show my driver's license. I just want to prove a particular attribute.

Here, I want the attribute "I'm vaccinated," and there should be a way to show that attribute. But somehow, I have to prove that this digital record belongs to me and that it isn't my husband's phone that I'm using to show that I'm vaccinated. So, perhaps in addition to the verification, a photo of me is attached (that is, the service provider provides that in providing proof I'm vaccinated).

Reflections

Blakley: I'm going to move on to our two wrap-up questions, which, I hope, are going to become a tradition. The first question is "What are the three or fewer things you've learned in a career in security and privacy (and, in your case, public policy) that you think the next generation of practitioners should remember?"

Landau: One of them I have already told you about, which is that it's really all about people and that "educate the user" is the wrong way to go about security. The other is that it's really hard to explain to people why privacy is so important.

I come from a family history that has made me very sensitive to privacy, but I'll actually tell the story of the mother of one of my good friends. Maybe 10 or 15 years ago, when her mother was in her 70s or 80s, they were in a shop together, and the clerk said, as her mother was paying, "What's your phone number?"

Her mother rattled off 10 digits, and my friend walked out of the store with her mother and said, “That’s not your phone number!” And my friend’s mother said, “Ever since I was in the internment camps, I don’t give out any data I don’t have to.” Because her mother was Japanese American. And this was the sweetest, most friendly, most pleasant woman I knew. It was hard to imagine there was that edge underneath, but the edge was there 50 years after Americans had put citizens into internment camps during the Second World War.

So explaining to people the cost of lost data—that is, the cost of giving away your data—has been surprisingly hard. I teach a course on privacy, and, by the end of the course, boy! The students really think about the world differently. But I teach 30 kids at a time. That doesn’t make a dent in 300 million Americans. Thinking about ways to get people to understand the costs of lost privacy is an important thing. And throw out “educate the user about security.”

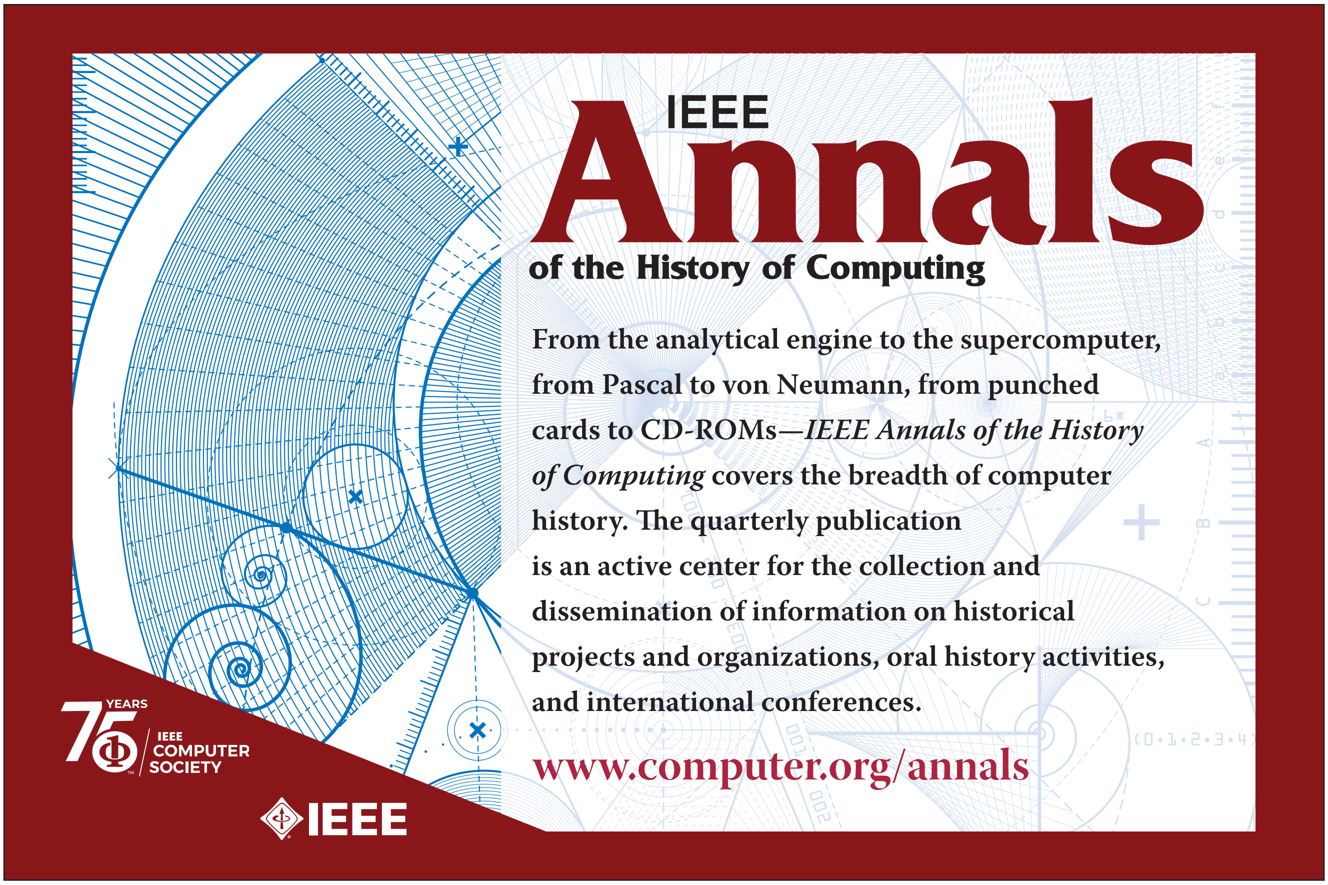
Cranor: Great! So our second wrap-up question is “What advice do you have for a young person who wants to grow up to be like you?”

Landau: Don’t do it! You’ve got to be crazy! But, if you want to be crazy in this way, if I think about what impacted me the most, I read voraciously. I still read voraciously. I have read *The New York Times* every day since I was 10 or 12. I read lots of things, like *The New Yorker* and *The Atlantic* and so on, but I also read literature.

I’m a scientist. I’m an engineer. But I’m very interested in public policy and always have been. You don’t learn how to write by reading just *The New York Times*, and you certainly don’t learn how to write by reading textbooks about security, or about differential operators, or about semisimple rings. You learn to write by reading good writing—by reading good literature. So nonfiction writing—the superb nonfiction writing in *The New Yorker* and other places. But it was really literature that educated me. Reading the sentences of Henry James.

Understanding about people, which you learn from people, but you also learn from great literature, and those have been my places of great education. I went to a great high school; I had good education otherwise, too, but reading has been the thing that shaped me more than anything else, intellectually.

Cranor: That’s wonderful. Thank you. ■



Digital Object Identifier 10.1109/MSEC.2021.3103618