How to Talk so Policymakers Will Listen

Susan Landau[1[0000−0003−4826−6134]]

Tufts University, Medford, MA 02155, USA
susan.landau@privacyink.org

Abstract. Policymakers and computer scientists speak different languages. Getting tech policy right requires technologists to learn how to communicate so policymakers can understand the issues and make reasonable judgements. In this keynote, I present lessons learned from twenty-five years of policy work in cybersecurity.

Keywords: cybersecurity policy · policymakers · tech policy.

My title is a bit facetious, so let me explain the purpose of my talk. Policymakers have very different jobs from scientists and engineers. As researchers, we have the luxury of time to get things right. By contrast, policymakers are often pulled from one issue of import to another; they rarely have the time to focus deeply on any one of them. So if you want to talk so policymakers will listen, you have to think how to make your words effective for their world. What I intend to do today is explain the lessons that my colleagues and I have learned about successfully conveying technology and tech policy to legislators and policymakers.

Those of you who attended the Rossfest yesterday already heard about a number of ways to talk to policymakers. You can write technical papers and show that proposed government plans, whether it's chip and PIN [17] or intrusion-detection systems designed for U.S. government systems [3], won't work as advertised. You can do blog posts, op-eds, interviews. You can testify at hearings, participate in work with non-governmental organizations (NGOs). You can do some of those things, and you can do all of those things. In this talk, I'm focusing on my experience. But in preparing this talk, I've also spoken with a number of others. The opinions I'm offering, though, are my own.

Most of my work for the last twenty-five years has been in cybersecurity policy, I came to this somewhat accidentally. I started off as a theoretical computer scientist doing algebraic algorithms. At one point in my career, I hit a bump. My husband didn't get tenure, and when we moved, my position did not come through as expected. I ended up on an ACM committee on encryption policy with Whit Diffie and others (this was the time of the Clipper Chip).

I'd been hired as the staff member, but I was overqualified for that role. I started off as the staff person on that committee and ended up writing most of the report [11]. From there I went to writing a book with Whit on encryption policy, *Privacy on the Line: The Politics of Wiretapping and Encryption* [9], after which I was hired by Sun Microsystems as a Senior Staff Engineer.

My role there was to do one-third technical work of interest to me, one-third technical work of interest to Sun, and one-third policy work. This role was an unusual one, including the fact that it involved remote work at a time when that was also quite rare. The working situation was not a normal route for one to switch research fields, but that's what ended up happening. I'd been at Sun about five years when I realized that I had become a policy wonk. I realized that Sun and I were happy. And so I kept on going in this unusual path.

At that point, there weren't many venues for writing about cybersecurity policy, at least in an academic way. I had been writing for *IEEE Security and Privacy* (the magazine), sometimes on my own, sometimes with my frequent coauthors, Matt Blaze and Steve Bellovin. But even though one of our *IEEE Security and Privacy* papers was referred to in a *New York Times* editorial [21], the magazine was not really an effective way to reach policymakers. So I embarked on writing law review articles.

Writing for law reviews is very different than writing for computer science conferences. In computer science, the reviews come back and you're told this is wrong, this is wrong, fix this, this, and this, and then we'll decide about accepting the paper. In law, things work the other way.

First, you send the paper to multiple venues—multiple in as many as twenty law reviews. Yes, you do this *simultaneously*. You also prepare a partial order of the law reviews to which you've submitted a paper. When you receive an acceptance, you write to the law reviews higher in your partial order, "I need an expedited review." Sometimes a law review will want to know which other law review made an offer to you. Then if you receive another acceptance, you say, bye, bye to the lower-ranked review, and you accept the next. You then do this again. As there are only finitely many law reviews to which you can send a paper, at some point, this process ends.

After a law-review accepts your paper and you agree to publish with them, you sign a contract. Then, at some point, you receive a set of proposed changes to your paper. You're given about ten days to respond (the short time frame is an aspect of training you to be a lawyer). And then you get another set of changes, completely orthogonal to the first set of changes. And again, it's ten days to respond. It's a weird system with most of the US law reviews being edited by second and third year law students (it's different in Europe). But if you're intending to influence policymakers, you have to write where they read—and that isn't publications in computer science conferences.[1]

Now Ross Anderson didn't follow this route. Ross was, as we all know, amazing in his impact and influence, not just in computer science, but in multiple other endeavors, including policy. But we all do policy work in different ways. Steve Bellovin and Matt Blaze, with whom I've collaborated a lot, have both written a number of law-review articles. Matt and I have done op-eds. Steve, Matt, and I have also participated in a number of US National Academies studies. Bart Preneel has briefed the EU Parliament and the European Commission many times. He is an Advisory Group member for ENISA and has participated

[1] Steve Bellovin has a blog post contrasting the two publication styles; see [4].

in their studies. Bart and Carmela Troncoso have put together a number of group letters to policymakers (some of you have probably signed these). Carmela pulled together the group that developed decentralized exposure-notification apps that were deployed across Europe and much of the US during Covid. Steven Murdoch has explained to lawyers how to collect electronic evidence. Elissa Redmiles has written for *Scientific American* and *Wired*. Most of us blog; some of us tweet. The point is that we provide our ideas to policymakers in different ways.

So what have we learned as we do this work?

First lesson: Policymakers are smart. They may not be conversant with technology—they speak a different language than we do—but that doesn't mean that they are not smart. They are simply smart in different ways than we are. Don't underestimate them just because they don't know a bit from a byte.

Policymakers have their finger on the pulse of how people think *and* feel. Dealing with a public whose interests and opinions can change quickly, they have to be astute in reading what people want and what is achievable when. Policymakers need other skills too. A critical one is framing an argument so that it is a winning one for their constituency. Similarly, they have to know which aspects of an issue are negotiable and which ones absolutely are not. The capabilities that successful policymakers have are different from ours—and crucial for success in their world.

One example at a briefing I gave really brought that home for me. The 2007 *Protect America Act,* which made explicit that there was no warrant requirement for wiretapping communications for US persons with people who were "reasonably believed to be outside the US." The law was passed in the wake of the discovery that the US government had been doing that post the terrorist actions of 9/11. (For the purpose of wiretap law, the US government defines a US person as a US citizen; an alien who has been lawfully admitted for permanent residence; an association of people of whom a substantial number are citizens of the US or aliens who have been lawfully admitted for permanent residence, or a corportation incorporated in the US [7].) I had written an op-ed about the security risks steming from the law in the *Washington Post* [12].[2]

I was asked to brief Congressional staffers on the issue. Two House of Representatives members were also present at the briefing. When a third one arrived, I noticed people moved so that he could sit right opposite me, he was busy with his email and didn't seem to be paying attention. But when I noted that the surveillance architecture as designed could mix purely domestic communications with ones with a foreign endpoint, the Congressman looked up and said, "Guys, this is really important." And yes, that was absolutely the most important message of my briefing. That was not the most important security risk, but it was the most important political issue. The Congressman had seen that immediately.

Lesson two: Facts are 10% of the equation. On the day I realized this, I tried to tell my husband. He is a theoretical computer scientist, in fact, a

[2] Later, Steve Bellovin, Matt Blaze, Whit Diffie, Peter Neumann, Jen Rexford, and I would write about this for *IEEE Security and Privacy,* the magazine [1].

complexity theorist. His job is to prove things; to him, facts are facts, solid and immutable. When he came home from work, I said, "I figured out Washington." He was quite interested to hear. "Facts are 10% of the equation," I said. He looked at me skeptically, and so I repeated my statement. And he looked at me as if I'd lost all my marbles. So I dropped the point.

Shortly afterwards I attended an Intelligence Advanced Research Projects Administration workshop whose purpose was developing civil-liberties protections in the wake of increased collection by the Intelligence Community (IC). I shared my observation about facts being 10% of the equation in Washington. A theoretician at the meeting looked at me, sputtered and turn red with great irritation. The researcher made it clear they thought I was spouting nonsense. But the IC policy person who was also part of the discussion strongly nodded in agreement. "Absolutely right," he said.

Some event happens—a terrorist attack occurs, a leading member of the security establishment is found using an insecure form of communication—and the political context of an issue can completely change. In policy settings, facts are 10% of the equation. We technologists forget that at our peril.

Lesson three: Speak so policymakers understand. This one, which is crucial, has many aspects to it. The most important issue is clarity. You need to **find ways to explain technical ideas so that they make sense to non-technical people.**

Don't explain RSA encryption in terms of modular arithmetic to a Member of Parliament. That's far too much mathematics to get to the point they care about, which is that public-key cryptography enables sharing private keys over an insecure channel. Explain the idea behind RSA in terms of the time it takes to multiply two large primes together versus the time it takes to factor their product. That's an idea that policymakers can quickly grasp. Then explain that this is the idea behind public-key cryptography though the mathematics for RSA is slightly different than what you just described.

Clear explanation about technologies can make a huge difference. I started my policy work with the encryption issue. So, of course, Alice and Bob have an appearance in this keynote. For this I need to introduce the 1994 *Communications Assistance for Law Enforcement Act* (CALEA), which requires that digitally switched telephone networks be built "wiretap enabled." This poorly thought-out law has led to many problems, including providing the Chinese government with information on which of their agents within the US are under electronic surveillance [19].

In its original formulation, CALEA explicitly excluded "information services." At the time of the bill's passage, this was understood to be the Internet. But in 2004, the FBI sought to have CALEA interpreted so that the law included Voice over IP (VoIP). A group of us swung into action to explain the complexities this proposal would introduce to a CALEA architecture and the insecurities that would result if such a change were introduced.

We wrote a whitepaper with a diagram that illustrated this. Bob and Alice are both VoIP customers, with Alice using VoIP Service Provider 1 (SP1), Bob, VoIP Service Provider 2 (SP2). SP1 uses Transport ISP A (TISP A), SP2 uses Transport ISP B (TISP B). Bob and Alice are on the go, so Alice is currently at a coffeehouse using Transport ISP C (TISP C), Bob, in a hotel lobby Tranport ISP D (TISP D).

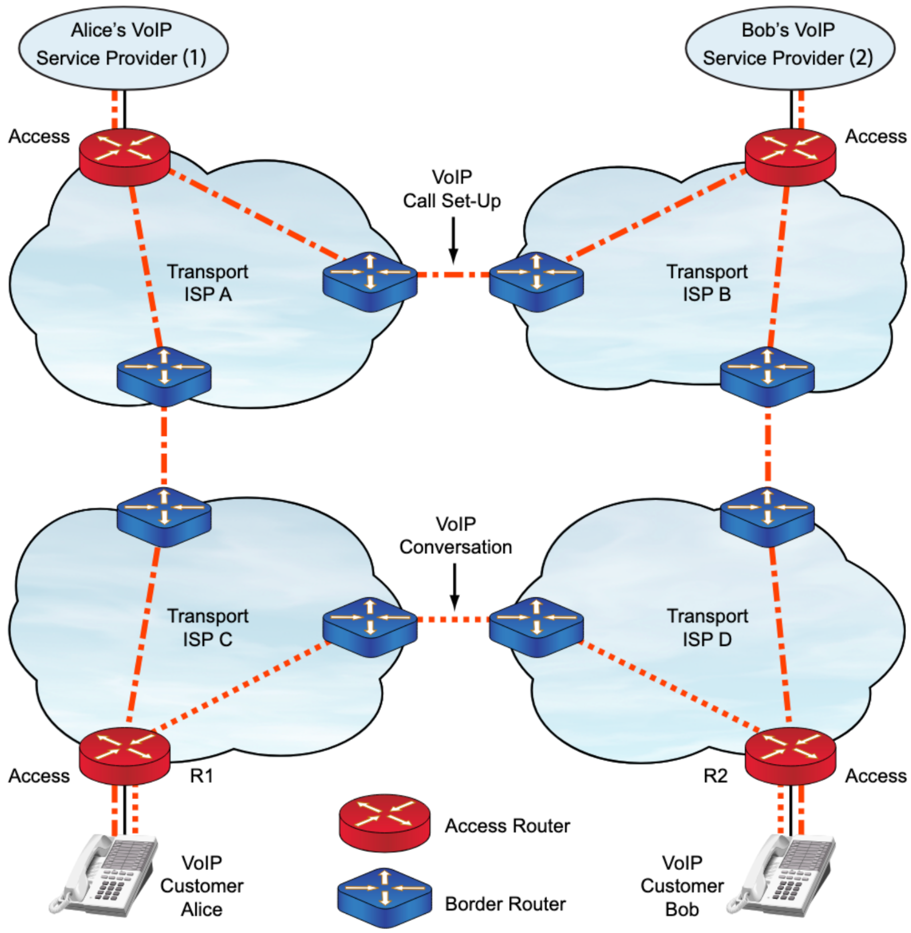

Figure 1: Alice and Bob using VoIP[3]

[3] Reproduced, with permission, from [2].

Let's suppose the wiretap order is on Alice, and thus is at SP1. Alice initiates a VoIP call to Bob. This request goes from TISP C, where Alice is currently, to her VoIP provider at TISP A, which checks with Bob's VoIP provider, SP2, whether Bob is online. If the response is yes, SP2 obtains Bob's current IP address from TISP A, which has received it from TISP B, which in turn, has obtained it from TISP D. This information is provided to the VoIP call set-up, which involves SP1 and SP2.

Once the call set-up has occurred, TISP A *then drops out of the picture.* From that point on, TISP A has no further involvement with the VoIP communication between Alice and Bob. This IP-based communication takes an efficient route on the Internet between TISP C and TISP D. But TISP C does not know about the wiretap order. SP1 is not authorized to inform providers about the order—that would be a security breach—and law enforcement cannot sufficiently quickly supply a surveilance order to TISP C, Alice's current ISP.

(The fundamental reason for the problem lies in the difference between the telephone network, which supplies both transport and communication service, while an IP-based network, separates transport, which it supplies, from service, which is what the VoIP carrier provides. "Facilities-based" VoIP communications, is a telephone communication from a fixed location using the phone network to a telephone central office; after which it can be transitted as a VoIP call, doesn't suffer this problem. Somewhat controversially, facilities-based VoIP was judged to fall under CALEA jurisdiction [13, pp. 23-24]).

In September 2006, I met with a Senate staff member; his Senator was interested in putting forth a bill to support the FBI's effort. The staffer noted that, "My senator wanted to put this bill forward. But we realized from that diagram, it's more complicated than we thought. So we're going to put off introducing this bill until after the election."

What happened next was that the Senator lost the election. The bill never came up. Explaining the techncial difficulties behind the FBI ask killed the bill's chances, with our diagram playing a crucial role in that [2].

Lesson four: Give examples that are meaningful to your audience. Nine years ago I testified before Congress in the Apple/FBI case about whether Apple should be required to undo the security protections it had developed in order to enable law enforcement to open the terrorists's phone [14]. I needed to discuss how important it was to secure the data on the phone, and so I needed to make the issue real to the members of Congress. While I could have talked about corporate email or classified documents residing on the phone, that wouldn't have worked. That's because members had secure phones for such issues—and my topic was consumer devices, not secured ones.

I needed to get the legislators to think about securing information on their personal devices. At that time, members of Congress largely didn't think of the data on their personal phones as needing such security protections. The right example to use was photos. Why photos? Because Congresspeople all have photos of their grandchildren on the phone.[4] You tell the legislators about photos, and

[4] Yes, the younger ones have photos of their children.

they say, oh, photos of my grandchildren, photos of this, photos of that. Suddenly the issue of data on the phone became personal to them. They then understood the need to protect the data on consumer devices in a visceral way. That's important in conveying your message.

Lesson five: Analogies make a big difference (be sure to get the analogy right). One of my favorite examples comes from Matt Blaze. During the Apple/FBI case that I just mentioned, FBI Director James Comey kept saying, "Oh, those smart people in Silicon Valley, surely they can come up with a solution that protects communications but still allows law enforcement in when they have a warrant." And we kept saying, "No, there is no such thing as the legal bit and the illegal bit." But law enforcement kept on making the argument that if technologists just thought hard enough, we would come up with a solution. Then Matt said, "Look, landing a man on the sun isn't hard. It's getting him back that's hard." Beautiful.

One of the great analogies for talking about client-side scanning is imagining someone looking over your shoulder and reading your letter before you put it in an envelope. Everybody gets that picture immediately. Now they have a mental model of what client-side scanning is even if they don't understand the technicalities. That's the type of analogy you want.

Lesson six: Focus on what resonates. This is again a lesson illustrated during the time of the controversy of extending CALEA to VoIP. I wanted to work on the issue, but first I needed permission from senior people at Sun Microsystems to do so. When I met with senior leadership at Sun, we discussed how complying with the law would be complex and expensive for our telcommunications customers. That was a Sun issue. Funds spent complying with CALEA were funds that the telcos wouldn't be spending on buying Sun equipment.

But in 2005, four years after the terrorist attacks of 9/11, arguments about economic costs to telecommunications provider and to Sun would not resonate in Washington when up against a law-enforcement security issue. So in Washington, I talked about how the wiretapping requirement created a security risk. I put forth the argument that CALEA applied to VoIP was a "security versus security" issue.[5] In making it easier to wiretap IP-mediated "telephone calls"—"telephone calls" in quotes because the communications were not public switched telephone network communications but IP-mediated ones—the requirement would make it easier to allow nefarious actors to wiretap. This is a real concern. In 2004-2005, such an architecture was used to illegally wiretap one hundred senior members of the Greek government for a period of ten months [23]. As I've already said, CALEA also enabled aspects of the Salt Typhoon access to classified information [15].

Lesson seven: Tailor your information to the arguments that most resonate with the policymaker. This is a bit of a repeat of the last point, but with a slight twist. If consumer protection is part of their remit, talk about that aspect. If human rights is, add that in.

[5] This was unfortunately demonstrated by Salt Typhoon [10, 22].

When I worked for Sun, anytime I was to meet with policymakers, whether in the US or elsewhere, I would be provided with a description of what each person's interests were. That helped me tailor arguments to their interests and concerns. This is important. Politicians win elections by doing the work the constituents care about. So if you want traction on the issues you're presenting, make sure you understand the interests of the policymaker with whom you are meeting.

Lesson eight: Provide alternatives. As I mentioned earlier, Steve Bellovin, Matt Blaze, Sandy Clark, and I did a paper on the alternatives to wiretapping when law enforcement encouters end-to-end encryption.

We said that they have to be able to hack into the devices in order to wiretap. By that time, some groups, including some Mexican cartels, were employing strong forms of cryptography on their devices. At that point, Apple did not yet have end-to-end encryption on the phones, but we were saying, "Look, you're going to have to have lawful hacking for searching some set of devices." Providing an alternative is important for honesty and credibility. But it's also critical for having credibility with politicians.

Lesson nine: The EU is not the United States. This is something that has become a great deal more clear in the last several months, but in the context of this talk, it could do with a bit of explanation.

One of the ways we're different, and this is something that Bart Preneel said to me, is that in the EU, the discussions about wiretapping and encryption happen in the back rooms. That is, by the time the bill is public, the text is fixed—but no players other than the government have been given an opportunity to participate. Civil society organizations have had no input. So rather than the back and forth that often occurs as US bills are being written, all such discussion happens much later in the EU. And that means that it isn't as much of a negotation because the discussion is now fully in public. Essentially, it is so late in the process that the only alternatives are up/down votes. That makes the situation much more difficult—and with much higher stakes.

In the US, bill writing is a more public process. The draft is circulated within Congress as they're writing the bill. Because the proposed text by government agencies gets out much earlier, civil society organizations, academics, and industry have input into the final bill. It isn't a perfect system by any means, but it is an important difference to keep in mind.

There are also other ways that we're different. The US is not the UK. In the US, we are very impressed by a posh accent— Queen's English— regardless of whether the speaker actually knows a hawk from a handsaw [24][II, ii, l. 379]. Speak with such an accent in the US and you're immediately considered quite erudite. In contrast, the British are quite taken when technology is discussed by people with American accents. This is not the John Wayne American cowboy accent, but the plain American accent from the East Coast or Silicon Valley. Americans know about technology; thus, opinions about technology spoken with an American accent are considered quite knowledgeable.

Lesson ten: There is no "the government." Now, this may be an American lesson, but there are universal aspects. Different US agencies have different views on policy; just look at the different take on encryption policy between the FBI and the NSA since 2000. Sometimes within an agency, there will be different views as well. Within the EU, the Commission is very powerful and tries to steer the discussion. But member states operate behind the scenes and can change seeming already fixed decisions. Understanding who is saying what privately and who might be responsive to your arguments is very important.

Lesson eleven: Dancing with NGOs can be very valuable. But never forget they have their own agendas. Between teaching, advising students, serving on program commmittees, writing technical papers and the like, we're all very busy. NGOs track the policy issues *all the time*. That's their job after all. NGOs know policymakers, they often know what is occurring behind the scenes, they know which of your arguments will resonate most where. So they can be very useful.

But be careful. One NGO was quite excited about a paper I wrote with Matt and others, and urged us to get it out quickly. We arranged to have it appear in *IEEE Security and Privacy* (the magazine). The NGO offered to take us around to Congressional offices to brief on it. And then they realized that there was one aspect of the paper that might upset their funders. They wanted us to stop briefing, and they also wanted us to pull the paper. We didn't.

The point here, though, is that NGOs have their own agendas—and that might not match yours. Make sure that you hold fast to your truth.

Lesson twelve: If you want your policy ideas accepted, ignore who gets the credit. Whit Diffie taught me this. It's really critical. This is sometimes about a policymaker wanting credit for an approach, but it can also be about a policymaker **not** wanting to associate themselves with an idea that was previously floated by a civil libertarian or a member of the tech community or ...or ... If you want your policy ideas accepted, sit quietly when you hear a policy person espouse the proposal, smile if you like, but *do not try to say how pleased you are that they are following your suggestion.* Instead, just enjoy it. You've been successful even if the only people who know that are you and your best friend.

This is a really important lesson. It is quite different from how we operate in academia. This lession is crucial if you want your ideas accepted.

Lesson thirteen: Want to get to know the press? People in civil-liberties organizations? Broaden the set of meetings you attend. Go to non-academic meetings like CPDP (Computers, Privacy, and Data Protection) in Brussels. Chat with the reporters. Talk with the staffers.

You can go to learn, and you can go to connect and make contacts. If the latter, do your homework beforehand. Thoroughly know the ins and outs of issues. Then, instead of hanging out with your friends, join groups of people you don't know but whose panel presentations interested you. Two important rules when you do so:

- If you have interesting thoughts to share, do so, but be brief.

– Carry business cards with you (yes, really).

Figure out these meetings, then propose a panel or workshop for the following year.

Lesson fourteen: How do you get involved? The answer is that there is no one answer. I'll give just a brief sampling here, since each person I talked with—and there are many others I did not—will have their own pathway.

Matt, Steve, and I now do lots of writing in policy; it happened over time for each of us. I began writing policy papers—well, technical papers that had some policy in them—for the *Notices of the American Mathematical Society* when I was a graduate student. I kept on doing that, then was hired by the ACM policy committee to be the staff member on the encryption policy report in 1994, and one thing led to another. But yes, I had also taken a course in constitutional law in college and another in writing non-fiction, neither standard fare for an undergraduate math major. I was interested in history of science and science policy since high school and read widely in those. So in many ways, the shift to doing policy work was a very natural one for me.

Steve Bellovin has always had policy interests. He had already begun writing policy and law-review articles when he spent a year in Washington as the Federal Trade Commission's Chief Technologist. That gave him great contacts in government and lots of insight; since that time, most of his work has been in law related to tech policy issues.

Matt Blaze found himself immersed in policy issues when, in 1994, he found a way to spoof the Clipper chip into encrypting using keys that were *not* stored in the system [16, 5]. He handled the situation with wit, smarts, and aplomb—and has done the same ever since (see, e.g, [6] for his discussion of same).

Others of those I talked with still have one foot much more firmly planted in computer science research even while contributing significantly to policy-related activities.

Bart Preneel explained his involvement this way, "Well, you know, I teach at Leuven and it's very close to Brussels, so when they wanted an expert on encryption, they called me." That's typical Bart modesty, and it provides only a partial explanation of Bart's success in policy efforts. Proximity to EU headquarters can explain a first invite to do a briefing, but distance to Brussels doesn't get you a second invite unless your presentation worked out well the first time. Explaining tech correctly in terms non-experts can understand is really important. This is something Bart does thoughtfully and extremely well.

Steven Murdoch started doing policy work as an undergraduate at University of Glasgow. On the tech side, Steven conducts research related to privacy-enhancing technologies, censorship resistance, and security, including security problems with proposed systems [17]; on the policy and legal side, Steven has written for and educated lawyers on gathering electronic evidence [18].

Carmela Troncoso is very active, technically and politically. I'll mention just one project here—the one that had tremendous impact around the world. That's the exposure-notification smartphone applications for proximity tracing during Covid. In the very early days of the pandemic, we understood that the disease spread through exposure before symptoms were visible, and thus a proximity-tracing system would be useful. The move was towards centralized systems, but Carmela and others pulled together computer scientists, epidemiologists, industry and policy folks and quickly developed, not just a decentralized algorithm, but an actual working system—one that was widely adopted in Europe and the US [25, 26]. The pandemic was officially declared in March 2020. By early summer 2020, the Google-Apple Exposure Notification systems had been deployed—and people's lives were being saved even as their location data was kept private. This was a huge victory.

I told you that I made this switch slightly by accident. That's because in my day, there was largely a sharp divide between scientists and those who worked in policy. But now, both because technology is moving so quickly and having such impact on our lives, and because the opportunities to publish are much more varied, the rules are different. When Matt, Steve, Ross, and I started doing policy work, that was not something that computer scientists did. Now computer scientists, both because of cybersecurity, privacy, and AI are more inclined and able to do this, and the computer science departments are looking at doing so differently. Indeed, Steven Murdoch mentioned that every six years or so, UK academic departments go through an assessment that includes a section on broader impact. The kind of work I've described here fits into that.

This brings me to Elissa Redmiles, who is younger than the rest of the people I've mentioned. I want to discuss her path because she's taken a different route than us older folks. Elissa does research on human factors in security and privacy; some of her research examines security and privacy issues for threatened communities. Early she started writing not only for *Scientific American* and *Wired,* but also *The Conversation,* an independent website whose articles and news pieces are picked up by press around the world (there is no payment involved, just the requirement that the full piece be reprinted along with the author's name and "The Conversation" listed as the original source). Elissa's pieces from *The Conversation* have been reprinted by the Associated Press, the *Miami Herald, Houston Chronicle, LA Times, Newsweek,* and many others. Having policy impact means engaging the broader public in discussions about technology and its potential impact, and Elissa is doing that—early in her career. Elissa is blazing a path younger people can follow.

There's a caveat though. In academia, young faculty must exercise care as they follow this path, ensuring that they are establishing their computer science credentials even as they do their policy work. Joe Nye, an eminent political science scholar who also held multiple eminent roles in the U.S. goverment, described the situation this way, "If I were to offer a strategy for a young academic, it would be to first nail down your academic credentials: get published in refereed journals, write a book or two that is reviewed as truly first-rate, and then consider a period of policy experience. When you return, that policy experience can enrich the next phase of your academic life. However, the path between academia and policy is, in some ways, a one-way street. It's easier to move from academia into a policy position than to transition from a policy role into a first-rate academic institution. So, secure your academic credentials first, and then think about what you want to do in government or policy." [8, Q10: Answer]. Joe was a brilliant scholar with a great deal of experience in both academic and policy worlds. While his advice about writing books applies more to political scientists than computer scientists—they write books, we typically don't—his advice about pathways between academia and policy is spot on for both fields.

So in concluding, let me say that I do this work, as do my colleagues and many others, because we care deeply about tech's impact on the world and policy's impact on tech. We do this work because it's important. And we do this work because of the deep satisfaction we get from doing so. If that sounds attractive to you, I have provided a roadmap to help you get started.

Thank you.

Acknowledgements: Many thanks to Steve Bellovin, Matt Blaze, Whit Diffie, Steven Murdoch, Bart Preneel, Elissa Redmiles, and Carmela Troncoso for multiple conversations over the years as well as when I prepared this talk.

References

1. Bellovin, S.M. et al. 2008. Risking communications security: Potential hazards of the Protect America Act. IEEE Security & Privacy, 6(1), pp.24-33, https://doi.org/10.1109/MSP.2008.17
2. Bellovin, S. M.. et al., *Security Implications of Applying the Communications Assistance for Law Enforcement Act to Voice over IP,* 2006, https://privacyink.org/pdf/CALEAVOIPreport.pdf.
3. Bellovin, S.M., Bradner, S.O., Diffie, W. and Landau, S., 2011. Can it really work-problems with extending EINSTEIN 3 to critical infrastructure. Harv. Nat'l Sec. J., 3, p.1.
4. Bellovin, S. 2013. "Alternate Universes: Academic Publishing in Computer Science vs. Law." SMBlog. https://www.cs.columbia.edu/ smb/blog/2013-12/2013-12-06.html
5. Blaze, M., 1994, November. "Protocol failure in the escrowed encryption standard." In *Proceedings of the 2nd ACM Conference on Computer and Communications Security* (pp. 59-67). https://doi.org/10.1145/191177.191193
6. Blaze, M., 2011, December. "Key escrow from a safe distance: looking back at the clipper chip." In *Proceedings of the 27th annual computer security applications conference* (pp. 317-321). https://doi.org/10.1145/2076732.207677.
7. Central Securitiy Service, National Security Agency, "Frequently Asked Questions," https://www.nsa.gov/about/faqs/sigint-faqs/#sigint4.
8. Crisan, S.I. and Nye Jr., J.S. 2024. "How to Manage Harvard Kennedy School: Prof. Joseph S. Nye Jr. Reflects on His Marriage, Overall Career & Writing Craft." *Pervasive Discourse.* https://www.persuasivediscourse.com/post/a-life-in-the-american-century-prof-joseph-s-nye-jr-reflects-on-his-marriage-overall-career.
9. Diffie, W. and Landau, S., 1998. *Privacy on the Line. The Politics of Wiretapping and Encryption.* https://doi.org/10.7551/mitpress/5571.001.0001.
10. Krouse, Sarah et al. 2024. "U.S. Wiretap Systems Targeted in China-Linked Hack," *Wall Street Journal,* Oct. 5, 2024.

11. Landau, S. et al. 1994. *Codes. Keys, and Conflicts: Issues in US Crypto Policy, Report of a Special Panel of the ACM US Public Policy Committee (USACM).* https://doi.org/10.1145/185354.
12. Landau, S., "A Gateway for Hackers: The Security Threat in the New Wiretapping Law," *Washington Post*, August 9, 2007, p. A17.
13. Landau, S., 2013. "The large immortal machine and the ticking time bomb."*J. on Telecomm. & High Tech.* L., 11, p.1.
14. Testimony, Hearing on The Encryption Tightrope, Balancing Americans' Security and Privacy before the Judiciary Committee, House of Representatives, 114th Congress, 2nd session (2016), (Susan Landau, Professor of Cybersecurity Policy, Worcester Polytechnic Institute).
15. Landau, S. "CALEA was a National-Security Disaster Waiting to Happen," Lawfare, Nov. 13, 2024, https://www.lawfaremedia.org/article/calea-was-a-national-security-disaster-waiting-to-happen
16. Markoff, J. "Flaw discovered in federal plan for wire tapping." *New York Times.* Jun. 2, 2994.
17. Murdoch, S.J. et al., 2010, May. Chip and PIN is Broken. In 2010 IEEE Symposium on Security and Privacy (pp. 433-446). IEEE.https://doi.org/10.1109/SP.2010.33
18. Murdoch, S.J., Seng, D., Schafer, B. and Mason, S., 2021. "The sources and characteristics of electronic evidence and artificial intelligence." in Mason, S, amd Seng, D. (eds.). *Electronic Evidence and Electronic Signatures.* University of London Press. 10.14296/2108.9781911507246.
19. Nakashima, E., "Top Senator calls Salt Typhoon 'worst telecom hack in our nation's history'," *'Washington Post*, Nov. 21, 2024.
20. National Institute of Standards and Technology, *NIST Cryptographic Standards and Guidelines Development Process, 'Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology'* (NIST, July 2014) https://www.nist.gov/system/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf
21. Editorial Board. 2013. "Eavesdropping on Internet Communications," *New York Times.* https://www.nytimes.com/2013/05/20/opinion/eavesdropping-on-internet-communications.html.
22. Office of the Chairwoman Federal Communications Commission. 2024. "Implications of Salt Typhoon Attack and FCC Response." Dec. 5, 2024. https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf.
23. Prevelakis, V. and Spinellis, D., 2007. "The athens affair." *Ieee Spectrum*, 44(7), pp.26-33. DOI: 10.1109/MSPEC.2007.376605.
24. Shakespeare, W. *Hamlet* 1602.
25. Troncoso, C. et al. 2020. "Decentralized privacy-preserving proximity tracing." arXiv preprint arXiv:2005.12273.
26. Troncoso, C. et al. 2022. "Deploying decentralized, privacy-preserving proximity tracing". *Communications of the ACM* 65(9). pp.48-57. https://doi.org/10.1145/35241.