Interview with Martin Hellman

Interviewer: Henry Corrigan-Gibbs
6 March 2014, 2:00pm
Stanford, California, U.S.A.

QUESTION To save yourself the effort of repeating over and over the stories that you have told before, I looked up some of your old interviews with people and read through the transcripts, so I might ask you about some old, old stories. I saw some of the interviews—there was one from '91 even, from IEEE.

The project I am working on is for this seminar on classification, more specifically about journalism and leaks to the press and ...

HELLMAN Is it okay out here for your recorder or is the wind creating too much noise?

QUESTION I think it will be fine, the microphone on this thing is okay.

HELLMAN Well then I will move a little closer.

QUESTION Spoken like a true engineer.

What was the story you were thinking of?

HELLMAN *The Falcon and the Snowman*, which you probably haven't heard about... When was that? It must have been the early 80s.

There was a book called the Falcon, or the Falconer and the Snowman. It was [about] two guys who were arrested in Los Angeles. One guy was a falconer and the other guy was his drug dealer—the Snowman. The falconer was the adopted son of a former FBI agent who got him a job working in the coderoom at TRW sending back encrypted highly classified communications to the CIA.

QUESTION TRW was an electronics...

HELLMAN Yeah, but (*sigh*) a lot of the electronics companies were also involved in the intelligence community. I had friends who were working for the

CIA who had cover at one or another of the Silicon Valley companies, and Silicon Valley is also called "Spook Valley" sometimes. So there is a lot more intelligence work going on here than you know.

Anyway, so he became disillusioned—he saw stuff about how we were helping subvert democratically elected governments in Australia because they were Labour instead of Conservative. The Vietnam War. This goes back before the 80s—I think the Vietnam War was part of it.

Anyway, he and his drug dealer decide to sell secrets to the Russians and they're caught. They're tried separately. I ended up—not wanting to but ended up becoming an expert for the defense in this trial. Because I was already pissing off NSA I didn't want to piss off the CIA needlessly, but no one else wanted to do it and people I kept saying would be better for it kept saying no, I was the right person.

But in that trial, they had given up on proving they were innocent—the defense at this point was trying to show that the documents they passed were not that important to national security.

And so I got one of the documents, which was a TRW study on how long a spy could operate in a city like Moscow transmitting clandestinely before he could be detected and radiolocated and captured. And they have all of these incriminating-looking diagrams in them—very sensitive—you know, antennas at one kilometer, three kilometers, five kilometers, every 60 degrees, fairly fancy equations about how long it would take at various signal levels before the KGB could home in on the guy.

So I was able to find the exact same diagram, the exact same equations lifted out of the *IEEE Transactions on Vehicular Technology* for radiolocation of police cars. And that was classified "Top Secret."

So, I mean, there is over-classification.

Why don't you stop that [recorder] for a second. I'm going to get a glass of water, do you want one too?

Break in recording.

HELLMAN Do you want to start it? Using voice memo?

QUESTION Yes.

HELLMAN I use that a lot.

QUESTION The other ones apparently would crash half-way through, which would be unfortunate.

HELLMAN Well, the other thing you can do is just stop every once and a while and save it. I don't mind.

In the trial, the guy at the CIA who had classified the documents was a witness and the defense got the judge to allow me to sit there and help them, because it was highly technical. At one point, the defense attorney is having the CIA guy who classified—the deputy director who had signed off on the classification—read from a document that had something about PCM.

And the defense attorney didn't know what PCM was so he just said "What's PCM?" and he said—I forget what the CIA guy said, but it wasn't "pulse-code modulation." And he came up with some other PCM acronym, which was wrong. And so I passed a little note to the defense attorney, and he says "Oh, doesn't PCM stand for pulse-code modulation, not that other three words you just gave me?" And the CIA guy said "yes," so he obviously didn't really understand what was in it.

But, you know, this is how things... Of course someone below him may have said, may have known more, may have said it should have been classified.

QUESTION Right. It was interesting that you mention that because we were just looking at the Pentagon Papers case and it turned that huge portions of the Pentagon Papers were just news clippings. The collection was classified Top Secret, so all of the news clippings were.

I was curious—It seemed like part of the thing that was at issue with the incident back in the late 70s was whether crypto research should be "born classified."

HELLMAN Yes.

QUESTION Or born unclassified. As I started reading about it, I learned that there is this bifurcated system in the U.S., where certain types of nuclear science can be born classified and everything else is not. I am wondering if you think that that distinction makes sense. That research on nuclear physics that is so close to bomb-making should be born classified and everything else should not be. Or maybe pieces of crypto could be born classified? Or it all should be out in the open?

HELLMAN Well, clearly there is. Let's see. Well, first of all, does it do any good for it to be "born classified?" Because people can talk about it. There are a bunch of questions.

But just forgetting about all of the practical side to it. Is there certain information that I would rather never saw the light of day if someone came up with it even though he or she didnâ't have any benefit of classified knowledge in coming up with it? Absolutely.

I just had lunch with someone who said that if someone came up with a way

to make something with the explosive force of a nuclear weapon in their basement out of baking soda, vinegar, and other household chemicals, I wouldn't want that being, you know, publicized widely and I actually think we often put way too much information out there. So there is a—there is a line but I don't know that classification really solves the problem.

When Inman was trying to—Admiral Inman—was trying to get Congress to pass legislation that would clarify, from his point of view, clarify that cryptography was "born classified," I pointed out to him that... (*Pause.*)

We [Admiral Inman and I] went from being adversaries to being cautious, talking cautiously, to really, I would say, being friends. And so, for example, he is one of the people that signed a statement of support for my bringing quantitative risk analysis to nuclear deterrence an saying to a potential failure of nuclear deterrence. I don't know if you have seen that.

QUESTION Yeah, I did.

HELLMAN Anyway, when we were about midway through that process, I pointed out to him that getting the legislation wouldn't do him any good, at least I didn't think it would. First of all, there was a question of whether it was constitutional. It might be invalidated in the courts. But secondly, I said even if you get the legislation and it's upheld, you're going to really piss off the academic community and so they may not publish their papers but they'll give 100 talks before they submit it for publication.

I argued that he really needed, and I think anyone in this, needs the cooperation of the researchers—the authors—on their side, because you have to want them to help you.

QUESTION It's interesting though that that hasn't happened with nuclear secrets. I imagine that, for the most part, the people who are working on those issues don't give 100 talks in public before they publish their papers. There is sort of a sense that it does belong classified—that it shouldn't be out in the open.

HELLMAN Well, part of it is it's hard to see... I was working on cryptography from an unclassified point of view because I could see—even in the mid-70s—the growing marriage of computers and communication and the need therefore for unclassified knowledge of cryptography. It's hard to argue that there's an unclassified need—a need for unclassified knowledge of nuclear weapons. How to make nuclear weapons.

QUESTION Are there pieces of cryptography that you think should never be out in the open or it all should be out in the open?

HELLMAN Oh! I think it's complicated. Kind of like Facebook where you can

say your status is complicated. In the mid-90s, I served on the NRC committee that came out with a report called CRISIS, cryptography's role in securing the information society, I think it stands for. And when I was asked to serve on that committee, I went through a little mental exercise before I did—it's something that I've found... actually I'll give you a little background.

My wife and I used to find ourselves polarizing over certain issues. Whatever position she took, I would gravitate to the other pole and vice versa. And one of the counselors we saw pointed out that that was a very natural process. So, for example, if a couple is talking about where to go on vacation and let's say that the wife says "Oh, wouldn't it be great to go to Tahiti?" And the husband shoots back immediately "But we canâ't afford it!" He has now provided a safety anchor where she can now explore how wonderful it would be without worrying that they're going to go bankrupt. Do you see what I'm saying?

QUESTION I do.

HELLMAN So now if he's anchored that position, she can now, it's natural that she will go "But it would be so much fun to go, wouldn't it?" She's not even saying that they *should* go, but it's freeing her up to think more that way than she would otherwise.

And so what I did when I agreed to serve on the NRC committee I said "let me pretend." I realized first of all that NSA and the FBI had been anchoring a position for me. It was easy for me to argue in favor of free export or freer export, freer publication, because they were anchoring the position, they were protecting my physical security from terrorists and criminals by arguing you know, "But wait a minute! We have to worry about terrorists and criminals."

And so I went through a little exercise where I said, "Let me pretend that I had"—I was actually sitting out here—I said "Let me pretend that I have dictatorial control. Whatever I say about export goes. Would I take all export restrictions off cryptographic devices?"

And all of a sudden I got worried about terrorists and criminals much more so than I had been before, because NSA and FBI were not anchoring those positions for me.

I concluded that there still should be freer export and I also thought back maybe at another point in time...

This is related: Let's see, the big fight with NSA was '76 to '78, '79, something like that. Actually it was starting in '78 that Inman paid me a visit and started to improve relations. In the early '80s my wife and I worked—went through a process which is probably one reason why we're still married after over 47 years—where we really came to understand each

other's perspectives much better and get out of this tunnel vision where, when she said something that sounded crazy, I'd treat her like she was crazy.

It turns out that some of those things are very wise, they were just outside of my field of view. And as I went through this process, I realized that when I fought with NSA in the 70s, I had done what they had done and what most people in that situation would have done. So I'm not faulting myself as a human being for having done it but I decided it's not what I wanted to do in the future.

And what I did, and what they were doing, was trying to win the argument. Every argument that buttressed their position, they amplified. Every argument, no matter how valid, that would hurt their position, they disclaimed. And I did the same thing.

That is, I used a magnifying glass for arguments that supported my position, and I tried to discredit arguments, even if they were valid, that discredited my position.

Today, I would do it differently. I would say "Yes, they have some valid points. Here are my points." And I would lay it out, and I would say "You decide. I've decided that it should be here. You decide for yourself."

And so, when I did that, I remember thinking "What would I have done differently?"

And I concluded that I still would have argued that we needed to develop unclassified knowledge of cryptography. That, even from a national security point of view, was important. Because if American business don't have good encryption, then foreign intelligence services will be able to rip us off. And that's a big concern to the country.

And so I concluded that I still would have done pretty much what I did but I would not have painted NSA as the "bad guy" and me as the "good guy." To some extent, I was a lot younger then, I was—1976—I was 30, 31 years old. I saw myself as Luke Skywalker—you may have seen I use that sometimes in these interviews—and NSA was Darth Vader. Yeah, they've got some people who do things I'd rather they didn't do but they have a lot of really good people there too who watch out for our interests.

And so that's what I would have done differently. I would have been more honest. Even though they were not being honest. They were being horribly dishonest in the debate. They told me I was wrong when I was right.

QUESTION So was there anything... I mean, sometimes when the media, when the New York Times, say, gets ahold of a classified documents, they will have the president call up the publisher of the New York Times and say "These terrible things are going to happen if you publish this." And I'm wondering if there's anything that the director of the NSA or Gerald Ford or Jimmy Carter could have said to you that would have made you say

"No, I'm going put this paper in the bottom drawer of my desk and pretend it never existed," or "I'm going to rip out all of the important details and I'm going to publish it stripped down?"

HELLMAN No. Public-key cryptography, the DES key-size issue... The DES key-size issue is the tougher one because that's telling people what key sizes to use and, you know, 56 bits—100,000 million million keys just seems horrendously large. To put it in perspective, most of the commercial systems of that era were using 40-bit keys—you know a trillion possibilities is just ridiculously small but it sounds big.

So what was your question?

QUESTION So is there anything they could have told you that would have made you not publish?

HELLMAN I think... Let's put it a little differently...

In hindsight, was it a good thing that I published or a bad thing that I published? I think it was a good thing that we published. It's even helped the military in a lot of ways.

I guess, part of the other thing is: it's a question of whether we want our military to have an unequaled advantage... an unquestioned advantage over all other militaries. And from the normal perspective, you'd say, "Of course we want that."

But having studied it, I conclude that that's not what we want. When we have the biggest hammer around, when someone needs a nail knocked in, they come to us. Or even if they don't come to us, we say "Hey! We've got the biggest hammer." We've gotten ourselves in a lot of trouble by having as powerful a military as we do.

And so... Also nuclear weapons have fundamentally changed the equations of national security and the equations of national survival. And so we need to—it's in our national security interests to have—it's not in our national security interests to have unquestioned military superiority. It's in our national security interests to have the greatest probability that our national will survive and not be destroyed by nuclear weapons. And it takes different assets to do one versus the other.

QUESTION Do you think that that argument carries over to, say, cryptography?

HELLMAN The point is that other countries having good cryptography hurts us.

In fact, one thing I've said to Inman when he was here on a visit—in fact, in that room in there—I said "In time of war, it's really important to keep things secret." If you're trying to win a war, secrecy is really important. If you're trying to avoid a war, secrecy can be really dangerous.

I mean, look at World War I and how secrecy about alliances and who is mobilizing and how far along and what their intentions were. It created a feedback process that produced a war that nobody wanted, to a large extent.

And so, I said to him, and this was at the height of the Cold War—probably 1983, 1984—I said "Given that our paramount goal with the Soviet Union," which it was in those days, "has to be to avoid war." If we get into a war with them it would be horrible for us. There is a question of whether we'd survive in any meaningful sense, or even physically. I said, "So given that our goal is to avoid war, maybe we need less secrecy. Maybe we need more openness. Maybe we should actually grant the Soviets permission to sit in on all national security council meetings—you know, top-secret meetings—in return for our getting some more privileges over there."

Now this of course was a wild idea and it wasn't practical at the time. And he saw it as impractical at the time. But within a couple of years, when Gorbachev was in power, it might have flown.

So that comes back to your question: is there anything they could have said to me? There's nothing they could have said to me at the time because I was too ego-involved at the time. And now, even though I still have an ego—I'm a human being—I'm less ego involved and I'm really trying to go for what's right rather than for what I think I want.

I still think it's in—overall it's good for the world and good for our country that this technology exists. I don't see that it's causing any great harm. Plus, I've heard from people within NSA—not recently, but 30 years ago—that these papers didn't cause the grave harm to national security that thought it would. People still make stupid—I'm filling in here—people still make a lot of mistakes: use wrong, bad keys, or whatever else.

QUESTION So does that extend, I mean... I was interested to see that they've actually crafted clever weaknesses—more clever than having short keys—other sorts of clever weaknesses into systems. Do you think that...

HELLMAN Let's see, the only one I'm aware of is the elliptic curve random number generator. Is that the one you're talking about?

QUESTION Yes, exactly.

HELLMAN Now, of course... Caveat: We don't know for sure that they've inserted a trapdoor. We know that if they wanted to insert a trapdoor, they could easily have done it.

QUESTION Well, one of the leaked documents—the Snowden documents—suggested that there was a standard around the same time that they had tampered with. It's not definite proof, but it begins to look pretty...

HELLMAN Okay. So what's the question?

QUESTION The question is: Say you're a newspaper reporter and that drops on your desk. Or you're a computer scientist and you find out that there might be this hole in this algorithm. Is that something that you publish or that you sit on? When really you can believe that the only people who will ever know the secret key are people who designed the algorithm who are presumably keeping it secret.

HELLMAN That's a tough one. I don't have a simple answer to that. In a way, I guess I'm grateful that I don't have to make that decision because it would take a lot of my time and I have more important things to work on, like making sure we don't blow ourselves—trying to decrease the risk of our blowing ourselves up.

QUESTION So, what would you... What would be... Do you have a sense of even how you would begin to make that decision?

HELLMAN Okay. So let's take a hypothetical situation: I look at the Advanced Encryption Standard, which is very widely used and there's almost no alternative to it in a sense. I discover that there is definitely a trapdoor—I find a technical trapdoor and then I'm told... I learn somehow that it was deliberate. It wasn't just an accident and that NSA is the one who knows the trapdoor information. Would I publish that?

What I would hope. I mean, in an ideal world—I mean this is all a very hypothetical situation—I would hope that I could go to them and (*pause*) Oh god, that's a tough one. I mean, I'm thinking aloud here. Could I go to them and say "Hey look! This is a bad thing. I mean a very dangerous thing that you've done. Because in good hands, it could not be a problem but used wrongly—and you have been used for wrong ends before by presidents—you do report to the president—this could be very dangerous." Try to ensure that there were... safeguards in place.

But on the other hand, it's just... that would be so egregious that it might just be that you'd have to go public with it. Of course, you have to be careful then: what do you go public with? Because you don't want to publish the trapdoor.

Oh! Unless the trapdoor—publishing the trapdoor would not necessarily allow other people to break it because they might need the trapdoor information.

QUESTION Sure, like in this case.

HELLMAN Yeah, yeah. (*Pause*) Good question. I don't have a...

QUESTION It's okay, of course you don't need to have the final answer.

I thought that this was a particularly clever trapdoor though, as far as they go. And actually as I was reading about it last month, I found that there is a patent application by Certicom that was published late last year about a random number generator with key escrow. And it was the same design.

HELLMAN Oh!

QUESTION Yeah, so I guess the patent application hadn't been published.

HELLMAN When was the patent? It was only published after Snowden's revelations? And when was it filed?

QUESTION Something like 2004, 2005.

HELLMAN And when was that elliptic curve random number generator?

QUESTION Around 2006.

HELLMAN Oh! So...

QUESTION It looks like it was...

HELLMAN I was not aware of that.

QUESTION Yeah, there's some technical design ideas that look very much like the Certicom style. Do you know that algorithm much?

HELLMAN Sorry, which algorithm?

QUESTION The elliptic curve random number generator, or the EC-DSA?

HELLMAN I know elliptic curve DSA a little better. I know the elliptic curve random number generator enough to understand how they could have put the trapdoor into it if you know the relation.

You know, basically I think it has to do—if my memory is serving me—it has to do with knowing that you, if you generate x and then generate α^x, or in this case $x \cdot \alpha$ on the elliptic curve and then making that y public but keeping x secret you can then...you can then from one output predict the other outputs. Is that right?

QUESTION Right.

HELLMAN Future outputs.

QUESTION Right, there are two generators and if you know the discrete log of one base the other...

Yeah, so what about even a more general thing. If you found an algorithm that you could totally break some system that everyone was using, do you go to the government first?

HELLMAN Well you don't go to the...

QUESTION If you find a way to... say, factoring or discrete log in certain cases?

HELLMAN Oh, that's a good one. Well it certainly would be unethical to just publish. If you came up with a polynomial—really fast factoring algorithm that could break everything out there that's using RSA and especially if it carried over to discrete logs. I would not—I would see it as unethical, as dangerous... as unethical, or wrong to publish it because you'd then expose everybody's information.

I think the thing to do there is more what people—what responsible people have done very often which is to go to the... That's so broad, I don't know if you can go to the people involved and get them to change their system and then eventually publish it.

QUESTION There are a lot of people involved.

HELLMAN No good answer.

QUESTION Again, no good answer.

So do you think yourself in 1975 or 1977—I guess no one was using those systems, so it would have been moot—but do you think your attitude towards those sort of questions has changed over time?

HELLMAN Well let me tell you something else that happened, which is kind of a partial answer. When Whit and I were criticizing DES as having too short a key size, we initially thought it was a technical problem and we wrote to NBS, now NIST, pointing out a couple of problems, with the biggest one being the 56-bit key size.

They answered all of our other objections and on the key size they just said "It's adequate for the purposes." You know, "We have no problem with the key size."

I then refined our estimate. You know, initially it was a back-of-the-envelope calculation. Because, especially with Moore's law, you know a factor of 10 every five years, we'd have to be off by orders of magnitude

for this not to be a problem in the long run. And we knew we weren't off by orders of magnitude. We might have been off by a factor of two, three, four, five, but not even a factor of 10.

But they... I refined the estimate. I talked to people in the integrated circuits lab here in EE at Stanford. We actually did a rough layout of what a chip would be. Although we actually used silicon-on-sapphire technology because pure silicon technology did not have a low enough speed-power product—it took too much energy to flip a flop. And it wasn't projected that it would be within a few years. Silicon technology just did a lot better than we thought it would do—or anyone thought it would do.

Anyway, I refined the estimate. We sent refined estimates to NBS and it was really going to two guys who had come over from NSA to NBS so they were really representing NSA's interests rather than NBS's—at least that's how it seemed to me.

And after about six months it became clear, and I was even told by some people on IEEE standards committees, you know the chair of the committee: "You don't have a technical problem. You've got a political problem. If you want to change the key size of DES, you're going to have to fight it as a political problem. You're going to have to go to the newspapers and get, you know, newspapers to cover this. You're going to have to go to Congress and get hearings. Arguing from a technical point of view is not going to get you anywhere. We're not going to have any more success than you did."

And so, one night I... Oh, then, so the first thing I did was, Paul Baran, who you may have heard of—far-reaching paper about 1964 on encryption written at RAND. Also, there's some disagreement, but he certainly deserves at least some, if not all, of the credit for inventing packet switching. B-A-R-A-N. Paul Baran died about a year-and-a-half ago.

Paul Baran was having a small group meeting here in, I think it was Menlo Park there just across—an industrial park north, so to speak. He'd been asked by someone in Congress to have a meeting to give technical input on a bill. It was not related to DES, but he agreed that it was close enough that they could add it to the agenda.

This was January '76. I think that the—I taped that meeting and I think that tape is online somewhere. I think EFF put it online. John Gilmore.

And I get a call from Paul maybe a few days, or a week, before the meeting saying that two guys from NSA would like to attend, is that okay with me? And I said "That would be great with me!" because we'd been fighting this fight, you know, a shadow fight, so to speak, it would be nice to actually talk with them.

And they came and they said—the short version of what they said is: "You're wrong on the key size being too small. You're wrong, but please be quiet. If you keep talking the way you're talking, you'll cause grave harm

to national security." Which didn't compute.

So, what I believe they were saying and what one of them later kind of admitted to me was that they had been saying is "You're right but please shut up. If you keep saying what you're saying you're going to cause great harm to national security."

I went home, it was soon after that meeting one night I was trying to debate what the right thing to—I was trying to figure out the right thing to do. Was it to go public or was it to do what they were asking me to do? And while I was trying to figure out the right thing to do, the thought just popped into my head: "Forget about what's right. Go with this, you've got a tiger by the tail. You'll never have more of an impact on society. You'll never have more chance to. . . "

I don't know. It would be an ego—I mean it's a real ego trip to run with it. And this was my ego—one part of my ego talking. It's kind of like in the movies when you have a devil on one shoulder and an angel on the other. This was the devil. And at the time, I thought that I had dealt with that idea that just popped into my head—you know, the devil whispering in my ear.

And I concluded the arguments I had were: the United States is the world's most computerized nation and the Soviet Union was the least—one of the least computerized nations of sort of the major powers. We stand, of course, to lose the most from insecure encryption. It was in our national security interest for me to go forth with what I was doing.

That was 1976. Five years later, 1981, I'm going through this process which I think I said is why I'm still married. Did I mention? Yeah okay.

You know, learning to see things other than—taking other perspectives—things like that and part of that process was, I watched a film called "Day After Trinity" about the guys who were involved in the Manhattan Project.

And in this video, this documentary, they ask each of the Manhattan Project scientists who they interviewed "What was your motivation for working on the atom bomb—this horribly destructive weapon?"

And each of them gets excited, his face lights up and they say "Nazi Germany!" Fission had been discovered by Hahn, you know, in Germany. If the Nazis got the bomb before we did, it would be a 1,000 years of dark ages. We had to get it first.

In the documentary later, they come around to each one of them, and say, "Well, when Germany was defeated and Japan was our only adversary, did you stop and reconsider?" They don't have to say "with your original motivation gone." And their faces fall. One guy, Robert Wilson, actually develops a tick in his shoulder as he's answering the question. A nervous tick.

And they all basically said, "I don't know why, but I didn't reconsider."

It's a little more complicated than that but that's the short version.

And watching that video in the summer of 1981, five years after I'd gone through this process, I recognized what they were doing. I can't be 100 percent certain about them but I was 100 percent certain about myself. They had figured out what they wanted to do and had then come up with a rationalization for doing it rather that figuring out the right thing to do and doing it whether or not it was what they wanted to do.

And I saw that I had fooled myself back in 1976; that I had not really—I couldn't be sure that I had done it for the right—I mean the arguments I had come up with—had I—I hadn't adequately considered counter-arguments. I had biased things so that I would reach the decision that the devil on my shoulder had told me to reach.

QUESTION So looking back then, do you still think that the decision you made was the right one? Just that you hadn't considered the right arguments?

HELLMAN Well, I told you before, the answer is: I still would have done what I did, but I would have done it with a better spirit. I wouldn't have posed the NSA as the "bad guy" and me as the "good guy." They had some legitimate interests. I would have not tried to shoot down all their arguments.

But there's a little post-script to this. I vowed I would never do that again. I vowed—fortunately the consequences of my fooling myself had not been as negative as—in fact, they may have been positive—I mean because I still think I—thinking it through even now I think I still would have done most of what I did. But it could have been something as bad as inventing nuclear weapons, and so I vowed I would never do that again. I then had a real problem maybe 10 years later.

Stanford had patents on public-key cryptography and MIT had patents on RSA, which is an implementation of public-key cryptography. If the patents were well-written, then they should pay royalties to Stanford and to me, because the inventors at Stanford in those days—I don't know about now—got part of the royalties.

But RSA Data Security told us "Your patents," even though in their paper, RSA had said that Diffie and Hellman had invented public-key cryptography, when it came time to pay royalties, which admittedly is a different thing than academic credit, their company told us that—the three of them sitting there with Jim Bidzos, who was the president of the company at the time—said "You're patents are invalid, sue us if you want."

It was a bluff. I think they would have caved if Stanford had mounted a case against them. They didn't have the wherewithal to defend themselves. But Stanford understandably didn't want—it's a rabbit hole that you can fall down, and the amount of money you can spend is just ridiculous. Stanford rolled over and played dead.

So I was really pissed with RSA. They sold their company for $250 million. We made almost nothing off of our patents.

Probably 10 years after my 1981 "Day After Trinity" experience, Jim Omura—have you seen his name?

QUESTION No.

HELLMAN He was a professor at UCLA, information theorist, and then worked in cryptography.

Jim Omura had left UCLA and had started a company called Cylink, C-Y-L-I-N-K, with a little combative Jewish guy from Philadelphia, Lew Morris, who has since died. And, Jim is still a very good friend of mine, just a prince of a man.

Jim sets up a meeting for me to meet with Lew Morris. Lew comes to me and says "You help me get an exclusive license to Stanford's patents and we'll get 'em by the balls." He would come up with the money to fight RSA.

QUESTION Yeah.

HELLMAN And I think that those were his exact words. Now this is roughly 10 years after I've committed never to fool myself again. The decision I make is I'm not going to do it out of—if it's just revenge, if it's just vengeance, that's not in keeping with how I said I'm going to live my life. If it made business sense for me and for Stanford to go with Cylink, then we should go with them.

But as hard as I tried to get my emotions out of it, I couldn't be sure that—it seemed to me like we should go with Cylink but I was so pissed with RSA at the time—I'm not anymore—Jim Bidzos is a good friend of mine. He's also signed my statement of support for bringing risk analysis to nuclear deterrence.

I came to my wife and I said "Dorothie, it seems to me like we should go with Cylink, but I'm afraid I'm fooling myself. I'm so pissed at them that I can't be sure I'm not."

And Dorothie said... came up with a wonderful solution. She said—Niels Reimers was then the directory of technology licensing—and she said "Does Niels have the same business interests you do?" Because of course he's representing Stanford.

So the obvious thing is well "Of course he does!"

And does he have the emotional investment in this that I do? "No!" In fact, he served the year before it was, as—he'd taken a year's leave from here to help MIT set up their technology licensing.

And so she said "Let Niels make the decision."

And so I got to Niels' office and I explain my problem and said "What do you think? From a business point of view, what should we do?"

And he said "Oh, we should definitely go with Cylink."

And so I can be sure that I didn't make the decision for the wrong reasons, but it's really easy to fool yourself.

Now, as it turned out, even though Cylink spent one or two million dollars, by that time, RSA had the Netscape payoff. They had licensed the RSA technology and they guaranteed them that they were immune from any other patent suits (*Laughs.*) from Stanford, and they'd gotten one percent of Netscape and Netscape went public at this, you know, huge valuation. And so they now had—they could outspend us two to one. (*Although Prof. Hellman thought this to be true at the time of the interview, new information that he discovered more recently indicates that the Netscape license may have occurred after the patent fight, or at least part of it. He also noted that his belief that RSA outspent Cylink 2:1 came from statements by Cylink personnel, who may have been mistaken about that.*)

And there were some weaknesses in Stanford's patents because the first patent was written by a summer intern who was a law student rather than a—Stanford was trying to save money. But...

So this all comes back to "Would I do things differently?" The thing I would really do differently is to try to do what's right and not do what the devil on my shoulder told me to do. Now fortunately, what he told me to do in '76 is not that different from what I would have done.

QUESTION Listening to this as a PhD student, it's funny because it seems like there is a lot of pressure to have splashy results that are...

HELLMAN Oh! Absolutely!

QUESTION And it's difficult not to... I find it sort of distasteful to call up the newspapers and say "We've found out how to do magic with computers!" and then get articles written up, but it seems like there is a lot of pressure to do that.

HELLMAN There's some pressure and it's also ego. I mean we all want to make a mark in the world. But what I see is that wanting to make a mark on the world has brought us to the brink of extinction. And, which is more important: making a mark or having things live on?

Plus if we, I mean, I didn't plan it this way, but if I'm able to ever make... if I have contributed or if I'm able to make more contributions to reduce the risk of doing ourselves in, what better mark could you make on the world, even if nobody knows it?

Break in recording.

QUESTION Are you surprised at all? Or have they changed at all?

HELLMAN Yeah, okay well, first of all the best of all possible worlds would be one where NSA is able to read anything they want. No one else knows about it and the United States' policies were what we claim they are, which is to make the world a better place, not to make us look like the king of the mountain. Unfortunately, the last one is clearly wrong so you run into some real problems there.

Comments on a personal conversation removed at Hellman's request.

And it's just one example there—one of the things that really I learned as a result of Snowden's revelations and the coverage of it—I don't think it was in his revelations particularly—was that Chief Justice Roberts appoints all of the new FISA court judges. That's a dangerous way to appoint FISA court judges.

So we hadn't been paying enough attention to this, is what I come away with. And so Snowden did a service in getting us to think about it. He may have done a disservice by creating problems we didn't need. Like the German intelligence service almost surely knew that Merkel's phone calls on her insecure cellphone were being intercepted.

Someone once asked me a long time ago because I was working—back in the 80s it was a group called "Beyond War" and the basic argument was that every war has some chance of blowing up out of control, so if we keep fighting wars it's only a matter of time before one escalates out of control and we destroy ourselves. So the solution to the nuclear threat is to move beyond war, is what we called it back then. I would put it slightly different now, but the same basic argument I still believe is true.

Which is why I don't just focus on the number of weapons, I focus on avoiding needless wars. And it turns out all of them in recent years have been. So it's better to say "avoiding needless wars."

And someone asked me back then in the Beyond War, because here I am working on cryptography, and working on Beyond War, "Wouldn't the world be a better place if there were no secrets?"

And there's a certain amount of truth to that. For example, this current crisis in Ukraine has—it's not like it has a 90 percent risk of blowing up in our faces—it's probably on the order of a one percent risk of blowing up in our faces. Order of magnitude. Maybe higher—I doubt it's 10 percent but it might be.

Discussion of conflict in Ukraine.

QUESTION I have had this argument actually with a computer science professor at Stanford about... His position is that secrecy is, that privacy is overrated. If everyone was just free to be who they are, we wouldn't have to worry about our privacy being invaded.

HELLMAN There's an argument.

QUESTION There's an argument there, but...

HELLMAN We live in an imperfect world. If we lived in a perfect would then secrecy would not be needed. We live in an imperfect world so secrecy is sometimes needed.

QUESTION Even in a perfect world, there is something nice about, say, having no one know where you are—about being able to go into the mountains and have no one know where you are. Rather than know that you're being tracked on, by...

HELLMAN Well, if I know that you're in the mountains. Let's say you told me ahead of time that you're going to the mountains. That doesn't hurt you.

QUESTION But...

HELLMAN In a perfect world. You see, we just had an "if we lived in a perfect world..."—if not true, anything follows. We don't live a perfect world.

QUESTION Right. I guess so that's not so useful. [...]

Okay, well maybe I can ask you one personal question as a PhD student. Do you have any advice for a first-year PhD student in computer science?

HELLMAN Oh yeah. Lots of advice. Let's see. Let me think how to keep it short.

The first thing is: enjoy yourself. Don't worry. Try not to get too worried.

The quals in computer science probably work differently. In EE when I took them, they may have even changed now, but they were this way for a long time, you could take...

Well, when I came here as a first-year student, I talked... The quals were a big issue but the people I talked to gave me the impression that no one passed the quals the first time around. So you had to fail them once to have some hope of passing the second time.

And since I didn't know what they were like—until you have experienced them, you have no idea what they are like, the amount of work people tell you—I figured, "Let me take them once and then I'll have a better idea of

what to study next time."

I didn't study very much. I maybe put in eight hours total reviewing some basic things, which I don't think helped me very much anyway, and I ended up being number one by a wide margin.

Now, I think the fact... I think I would have done well on the quals anyway. But I think the fact that I was at ease, that I wasn't too worried about it, made me do better. Or allowed me to do better.

And just keep in mind that no matter what happens here, you are going to have a great life, a great career, and things that seem awful at the time—oh! My first exam at Stanford I was in the lower quarter of the class. I had to learn how to take exams differently—I won't go into what happened there—the professor told us something that turned out not being true. He said he didn't expect anybody to finish the exam, so I didn't worry that I was having problems on one of the problems and I made sure I had everything else right.

And, at the time that felt pretty bad. It turned out to be a really positive thing, because when I was working with students later who were in the lower quarter of the class, I could tell them "Hey! The lower quarter of the class is still pretty smart." Because guess where I was on my first exam. If somebody from the lower quarter of the class can move to the top. It tells a lot.

Other things in terms of research: Don't wait until you know everything that you ought to know to tackle a problem. Because (A) you will never know everything you ought to know, and (B) a beginner's mind is actually useful.

So when I did my best work in cryptography, I knew much less of the relevant math than I know now. Maybe 10 or 20 percent. And so it was kind of arrogant in a way to tackle these problems but it worked out okay.

The other thing, if you've watched my "Wisdom of Foolishness" lecture[1]... have you seen that?

QUESTION Yeah, I have.

HELLMAN Most of the time, you take a swing at a foolish pitch. A wild pitch. And you don't connect but every once in a while you do hit a fool home run.

So the examples I gave there were DSL and GPS and the microprocessor.

QUESTION There's some selection bias there, right? Because there are probably lots of people who do foolish things...

[1] `http://scpdweb.stanford.edu/free-learning/webinars/stanford-engineering-hero-lectures/martin-hellman-wisdom-foolishness`

HELLMAN Oh, it's amazing though how frequently I come across someone who's really well known for having done something amazing and said "How was your work viewed when you first..." "Oh! Crazy."

No, so I think it's at least 50 percent.

QUESTION Huh.

HELLMAN So I don't think... No, I don't think it's selection bias. Because I have people like... I'm a Marconi Fellow, which they like to regard as the Nobel Prize in communications and I have asked several people there.

Oh, Vint Cerf is a Marconi Fellow. He was in my... packet switching [was initially seen as] crazy! Marconi Fellows are good examples. They weren't selected on the basis of doing foolish work, but then so how many of them—their work was viewed as foolish.

John Cioffi, DSL. He's a Marconi Fellow.

Then there's a guy who worked in an area I know nothing about—two guys, actually... The names are escaping me right now, this is embarrassing. The guy who came up with the idea of the amplifier for fiber optics. What you do is you come in and you have some kind... it's an yttrium-doped laser something. And they do broadband amplification. You don't have to go from optical to electrical and back again.

His work was regarded as crazy.

Chraplyvy, at Bell Labs, who is also a Marconi Fellow. His work was on non-linear analysis of optical signals in fiber. And his performance reviews at Bell Labs were sub-standard, his salary increases were below normal, because it was useless work! But once, actually once the amplifier came about that allowed them to pump these at higher power levels, his work became critically important in terms of optimizing the capacity of the fiber.

And so what we ought to do is go down the Marconi list and go to each one of them and ask. And Federico Faggin, the microprocessor guy that I talked about, he's also a Marconi Fellow. (*Hellman noted after the interview that Faggin also encountered disbelief about the role the microprocessor would play.*)

No, so actually it may be well over 50 percent.

Part of it is if an idea doesn't seem crazy, people have already worked on it. The real breakthroughs occur because you look at something from a totally different perspective.

QUESTION Reading Merkle's project proposal from Berkeley is just incredible. And seeing the comments that he got back from the professor...

Hellman Yeah! Well then you also ought to see the comments he got from the editor from the *CACM* [*Communications of the ACM*].

Question Yeah, it's in there—in the file.

The poor professor of computer science up at Berkeley must have...

Hellman Lance Hoffman.

Question Did you ever talk to him after that?

Hellman No, in a way it's just... he probably had 100 students in the class.

I mean, the same thing happened when Ralph submitted the paper. The editor wrote back to him saying "You don't have any references. This doesn't seem to be in the mainstream of cryptographic research." (*Laughs.*) Something along those lines.

And one of the reviewers said, "You can't do this!"

Question It's just impossible?

Hellman Yeah!

Question To be fair, it does seem sort of...

Hellman Yeah, but Ralph had the puzzles! He had a way—he had a reasonable argument. He was young. He may not have written it up as well as he could have. But it was all there if someone wanted to understand it, they could've.

Question Is it true that you finished your PhD in three years or two years?

Hellman Two years. Well, legally... So I came in September '66 and I left in September '68, having worked in the summer, so it was seven quarters. But I couldn't technically get the degree for two more quarters because you needed... I needed... I sometimes joke that I completed my residency in absentia. Because I needed more research units—more units, but they could all be research units.

I had just squeaked under the number of course units. I mean I wasn't thinking I'd finish that fast.

Oh, that's the other thing. Half an hour before I had the key result that became my thesis, I was wondering if I should drop out of the program. Because, who was I to think that I could make an original contribution to knowledge?

And then I sat down and what happened was I was carrying four courses,

you know 15 units a quarter my first year, and then I was carrying three courses—one course became research—my second year here. (*Hellman noted afterwards: "I was carrying three 3-unit academic courses and research units that second year."*)

And so over spring break I was beginning to feel like, "Who am I to think I can do this?" and "Is it ever going to go anywhere?"

But I decided that I ought to take... I was carrying a lot of course units and I didn't have that much time for research. So before I decided I should junk the degree, I don't think I really would have ended it there. "Let me take the break week and take 40 hours doing research." You know, nine to five, Monday through Friday. I would take the weekend off and I would take the second weekend off.

And within the first half hour I had proved the key lemma, I mean the key theorem. That didn't take me all the way to the result, but I knew it was a really important result. And, in fact, it was 90 percent of the way there. We were able to then take it there.

QUESTION That's pretty fast.

HELLMAN It surprised me. Very pleasantly. Yeah.

QUESTION Okay, well are there any... Do you have any favorite papers that I should check out that you think are really amazing must-see papers?

HELLMAN In cryptography?

QUESTION No, just in general.

HELLMAN Well, have you read "How risky is Nuclear Optimism?"

QUESTION I haven't.

HELLMAN Okay, so go to my publications page. It's one of the last publications. "How Risky is Nuclear Optimism?"

Because what's the point in proving theorems, doing PhDs if the world is—if no one is around to appreciate them in 10, 20, 50, 100 years?

And I'm not proposing that you shift from what you're doing to doing that but it would... If it strikes a chord, keep it as a piece of your personality rather than, as it is for me now, my prime concern.

If you like that one, look at the last publication in that list, which is about the 50th anniversary of the Cuban Missile Crisis. I've got 11 little-known risks from that timeframe and 11 little-known risks in the current world, or at least as of two years ago. And ways to reduce them.

As an example, it didn't have the Estonian Foreign Minister audio that I played for you, but I have links, which I hope are still up, and I have the original video here if they have taken them off the Web.[2] John McCain threatening Vladimir Putin's life, so the question comes up: "What could we do to reduce the risk of a confrontation that could turn nuclear?"[3] Not threatening Putin's life would be a good place to start, especially when you have been a presidential candidate of a major party in this country.

And for Americans to recognize that stuff like that is going on and demand that it stop—hopefully demand that it stop.

QUESTION So, it was so interesting to me that you started working—it went from very core theoretical—I guess practical too—crypto, but then to work that has huge social implications. I find, at least, talking to professors of computer science here, that people often treat the social effects of technology as "not my job."

HELLMAN No, I definitely made a shift and I think I mentioned what got me to make the shift—or, if I haven't—it wasn't wanting to save the world, it was wanting to make my marriage work. My marriage was falling apart around me because, among other things, I was trying to apply logic to the relationship.

I was trying to tell my wife how she... I once told her, "You can't feel that way, it doesn't make any sense!" which is one of the most illogical things you can say. I had taken enough mathematics to know about [Gödel's] Incompleteness Theorem that *proves* that logic is not adequate for proving everything, and yet I was still trying to make a false god out of logic.

Yeah, so also on my Opinions page—my Stanford home page, it's got opinions.[4] There's something you can read in under five minutes, it's called "Resist Not Evil."[5] Which fits with a lot of the things we've been saying today.

Let me think if there's anything technical that I can think of.

QUESTION It is stunning how often we invoke your name, Diffie-Hellman is attached to now so so many things in cryptography. It's amazing.

HELLMAN It impresses me. I am glad. It also gives me credibility to work on these other issues. I mean, they're different, but if you could do that... and yet, I also do bring technical into it. Like "How risky is Nuclear Optimisism?"

[2] For Hellman's analysis of this incident, see `https://nuclearrisk.wordpress.com/2014/06/19/transcript-of-estonian-fm-bombshell-revelation/` and `https://nuclearrisk.wordpress.com/2014/03/06/ukraine-why-we-need-to-stop-and-think/`.

[3] Hellman discusses this on his blog in more depth: `https://nuclearrisk.wordpress.com/2011/12/06/mccain-threatens-putin/`.

[4] `http://www-ee.stanford.edu/~hellman/opinions.html`

[5] `http://www-ee.stanford.edu/~hellman/opinion/Resist_Not.html`

is an argument for applying risk analysis to a potential failure of nuclear deterrence.

I didn't... Did I go through the order of magnitude with you? The one percent?

QUESTION No.

HELLMAN Okay, here's the elevator pitch.

Order of magnitude, how long do you think nuclear deterrence can work before it fails, on our current path? So things will change over the next 1,000 years, but imagine we kind of stay where we are, and so things like the Ukrainian Crisis occur about as often as they have—the Georgian War of 2008, the Cuban Missile Crisis—there is a certain arrival rate for each of those levels of crisis.

Order of magnitude, do you think one year is too long or too short a time horizon where we expect to roughly have 50/50 odds of it having happened? Too short, right?

QUESTION Sure.

HELLMAN Ten years? Too short. I mean, we've gone 50 or 60, right?

Let me skip over 100 to 1,000. A thousand?

QUESTION Say 1,000, sure.

HELLMAN What?

QUESTION Say 1,000.

HELLMAN Does it seem too short or too long? Do you think that if nothing changes, do you think it's more or less likely that we will survive a 1,000 years?

QUESTION We as a society?

HELLMAN Yeah, before we have a nuclear war.

QUESTION I am not qualified to say.

HELLMAN Okay, 95 percent of the people I ask say "Oh, that's ridiculously optimistic."

QUESTION Okay.

HELLMAN Because that would be like 20 repetitions of the last 50 years. Now the next 50 will be somewhat different, though we really haven't ended the Cold War, so things like the Cuban Missile Crisis can happen again. And actually it almost happened in 2008 which, if you read the 50th anniversary of the Cuban Missile crisis, that'll give you the details—are in there.

So if 1,000 years is too long and 10 years is too short, what is the only order of magnitude left in between?

QUESTION A hundred.

HELLMAN That at first sounds okay. You're not going to be around in 100 years. But that's one percent a year!

What's that over a decade? Ten percent!

What's it over your expected lifetime of about 60 years? About 50/50!

So, why aren't we doing something about this? The good news is—the positive part is that we don't have to just get rid of the problem, we actually have to make the world a lot better place.

Most people focus, when the focus on it at all, just getting rid of the weapons. But that's not going to happen in the current world, first of all. And also, if I had a magic wand that could change nothing except that all of the weapons were gone, I probably wouldn't wave it because then we would probably be more likely to get into a big war. Because we are very war-like in our current state, and we'd remember how to build them very quickly.

So we actually have to deal with some of the underlying flaws in our national security—approach to national security, our approach to foreign relations, our perceptions of ourselves as knights in shining armor, and our adversaries, whoever they may be, as Darth Vader. Luke Skywaker-Darth Vader analogy.

That's why it would horrify me to do something like that again. That's the fundamental problem.

QUESTION I haven't looked at nuclear war issues almost at all...

HELLMAN That's understandable, almost nobody does these days.

QUESTION *The Making of the Atomic Bomb* is basically the only book I have read on it.

HELLMAN Oh.

QUESTION You know Richard Rhodes' book?

HELLMAN I know the book. I haven't read that one specifically.

QUESTION Oh, it's really really good. But I imagine that there's computers controlling these things and that terrifies me. The idea that someone's buggy Fortran code, or whatever is, is running...

HELLMAN Yes! Find my blog also on my home page where I have a link to the blog. And on the blog, search for "Wyoming."[6] I think it only occurs on one blog. Or if you have trouble, I can send it to you.

About, I think it was about four years ago, there was a malfunction where 50 Minuteman ICBMs in Wyoming went offline.[7] They could not communicate with them. And the Department of Defense issued a statement saying, "Don't worry, if we had to launch them, we could."

Now that, to me, was really scary because it's unusual states that create a lot of risk. If you could launch them when certain safeguards aren't there, I mean, that's not how the system should work. The system should work that when anything is abnormal, you can't launch.

QUESTION Right.

HELLMAN That would be the failsafe approach. But a similar thing happened... Bruce Blair, who now heads Global Zero, or he did until recently, he may have stepped down, was a Minuteman launch control officer in the 70s. McNamara ordered then that the combination locks, PALs—permissive action links—be installed on all of them. And the Air Force installed them but set the combination to eight zeros.

QUESTION I think I have seen this, yes.

HELLMAN Again, the military was more concerned about being able to—even though they say these weapons are there never to be used, that's their sole purpose—they were more concerned about being able to use them when they wanted to than mistakenly using them when they didn't want to.

QUESTION It's a difficult type of question though. If someone came into you and said "We have this weapon that is going to destroy the world, what security setup should be used to authenticate...?" It's not clear to me that there is a good answer to that.

HELLMAN No, and we do have that weapon.

[6] `https://nuclearrisk.wordpress.com/2010/10/27/risky-nuclear-designs/`

[7] The incident took place on October 23, 2010. See `http://www.theatlantic.com/politics/archive/2010/10/failure-shuts-down-squadron-of-nuclear-missiles/65207/`.

QUESTION And there's some system that someone built.

HELLMAN Right. No, we need to become a lot more... We need to work really fast and recognize that we have been playing with god-like power with the maturity level of an irresponsible adolescent.

QUESTION I hate to keep bringing it back to cryptography, but do you feel that way about cryptography at all? The power of these tools is awesome, in the sense that a criminal or whoever can encrypt stuff in such a way that we think no one—no government—can read it. That's pretty powerful.

HELLMAN Well, if they don't... Let's see. First of all, criminals and terrorists can still talk privately. Even if there were no encryption, they could still talk securely. It's less efficient.

I don't know, in the September 11th attacks, could they have occurred without any encryption? In fact, oh! I suspect that any encryption they used was probably, I mean, I don't know for sure, but there's a good chance that any encryption they did use was broken. And yet, and even without the encrypted messages, there was plenty of information.

Jack Matlock, who was Ronald Reagan's ambassador to Moscow—I think he was a career foreign service officer—in one of his books he has written that, based on what he knows from having served on the National Security Council, or been in National Security Council meetings, the information available to the Bush Administration prior to September 11th that they did not act on constituted criminal negligence on their part. I believe those were his words, I can double-check if you want me to.[8]

So, even without encryption, we could have stopped it but we weren't paying attention. So, in some sense it's immaterial.

It's not like having secure encryption means that everything's protected and no one ever knows anything.

[8]Hellman double-checked after the interview and Matlock's words were "inexcusably negligent," not "criminally negligent." See Jack F. Matlock, Jr., *Superpower Illusions*, Yale University Press, New Haven, 2010, pages 188-189.

> The attacks on the World Trade Center in New York and the Pentagon in northern Virginia on September 11, 2001, could have been prevented. They very likely would have been prevented if a competent, alert administration had been in office in Washington.
>
> That was not the explicit conclusion of the bipartisan commission established by Congress and the president to investigate the terrorist attacks on the United States. But few people knowledgeable about the manner in which most presidents and their national security assistants react to intelligence warnings can escape the conclusion that President George W. Bush, Vice President Richard Cheney, and Assistant for National Security Condoleezza Rice were inexcusably negligent when they were warned repeatedly of an impending attack by Al-Qaeda. [...] This is a heavy charge, and I should explain why I make it.

QUESTION Right, right.

HELLMAN If there's insecure encryption, it doesn't mean that criminals...

There is evidence in both directions. That encryption isn't as important as we think it is. It doesn't prevent what we think it does, and a lack of encryption doesn't allow us to catch...

Ah, that's the point! Even if we could break, even if NSA and the FBI could break every message they wanted to, they wouldn't necessarily put two and two together. There have been plenty of examples of that.

QUESTION So you're saying that the level of encryption someone is using is independent of whether they are going to get caught or not.

HELLMAN Well, it's not as important as we think it is. As cryptographers we like to think that we provide an indispensable service.

QUESTION So if the Department of Defense—just one more whacked-out hypothetical—if they called you up and said "We have these Minuteman systems that we're trying to secure, would you come help us build a better authentication scheme for the launching of these things?" How would you feel about going and doing that?

HELLMAN Oh, it's very simple. I wouldn't do it.

But the reason I wouldn't do it is that I am not the most competent person to do it today and I am working on other things. There are plenty of people, even if I were one of the most competent people to do it today, there are plenty of other people that can help them do that as competently as I. And there are very few people working on what I'm working on, which I see as perhaps even more important than that.

QUESTION It's actually very inspiring to see someone who had a technical background who is looking at the world from a more human, social perspective also.

HELLMAN A holistic perspective. Well, it's inspiring to me too.

I mean, in the sense that if I could do it, anybody could do it. I look back on where I was 30, roughly 30 years ago when I started this process. I was a hopeless case.

I told my wife that she couldn't feel a certain way because it didn't make any sense. What I really meant was "I don't like you feeling that way and I am now using logic to try to convince you that you don't feel how you do." It was horribly abusive and a misuse of logic. Incompatible with the scientific spirit of seeking truth.

So it is inspiring to me that I went from there to where I am today. It is inspiring to me that my wife and I have a relationship that I thought was impossible. My wife, I sometimes describe as the "Princess and the Pea" of relationship conflict. She picks up this tiny shred of it, which I could be totally missing, and so she has really pushed us to not just save our marriage but take it to a place where we haven't had an argument in 15 years.

And it's not because we don't talk, we still see things differently but when we see things differently, we really try to get at what the right thing to do is rather than what each of us thought we wanted. And the right thing has usually worked out better than when we did have—not a conflict, but a conflicting perspective.

And so, that's inspiring to me. I didn't think this was possible. And if it's possible... if we could do it, then in some sense I think anybody can do it because we probably were headed for divorce. And, as I told you, I was a hopeless case. And while she's a wonderful woman, she was not exactly in a great place either when we started out the process. You know, she was hurt and angry.

QUESTION You said you've been married almost 50 years?

HELLMAN Forty-seven years. So the other part of it is we haven't had an argument in 15 years. I did a computation. If we haven't had an argument in 15 years, we've been married 47 and we started the process and we started the process [roughly 13 years into the marriage]—it was a 19-year process. It wasn't like it was horrible the whole 19 years, I mean it got progressively better.

It's the hardest thing I've ever done. Harder than doing the PhD. But even more rewarding.

QUESTION Great.

HELLMAN Okay.

QUESTION Thank you so much.

HELLMAN I enjoyed talking with you. Good questions.