SM255 | 11.1.2025
Re-engineering Tokenization | Episode 3
Phil Zimmermann, Creator, Pretty Good Privacy (PGP)

We continue our *Re-engineering Tokenization* series this week by welcoming Phil Zimmermann, Creator of Pretty Good Privacy (PGP), into the SmarterMarkets™ studio. David Greely sits down with Phil to discuss his work in cryptography and its role in establishing trust and preserving privacy online. Phil shares his thoughts on what we need to be doing to make sure our technology is helping – not hindering – us in building the type of society we want to live in.

Phil Zimmermann (00s):
I am sort of typecast as Mr. PGP, or I am known best for my work in cryptography. But the big picture that I am seeing now is the rise of autocracies and how they get into power, how they maintain power, how do they eventually get removed from power? And surveillance plays a part of that. And secure communications is of some considerable benefit to being able to resist them. But it's not the only thing you need. It requires a lot of vigilance.

Announcer (27s):
Welcome to SmarterMarkets, a weekly podcast featuring the icons and entrepreneurs of technology, commodities, and finance ranting on the inadequacies of our systems and riffing on ideas for how to solve them. Together we examine the questions: are we facing a crisis of information or a crisis of trust, and will building Smarter Markets be the antidote?
This episode is brought to you in part by Abaxx Exchange, bringing better price discovery and risk management tools to navigate today's commodities markets through centrally cleared, physically deliverable futures contracts in energy, environmental, battery materials, and precious metals markets. Smarter Markets are here.

David Greely (01m 16s):
Welcome back to Re-engineering Tokenization on SmarterMarkets. I am Dave Greely, Chief Economist at Abaxx Technologies. Our guest today is Phil Zimmermann, Creator of Pretty Good Privacy or PGP. We will be discussing his work in cryptography and its role in establishing trust and preserving privacy online, and his thoughts on what we need to be doing to make sure that our technology is helping, not hindering us in building the type of society in which we want to live. Hello Phil, welcome to SmarterMarkets.

Phil Zimmermann (01m 50s):
Hello Dave.

David Greely (01m 51s):
It's a real honor to have you here with us today. When you published Pretty Good Privacy or PGP in 1991, it was the first mainstream encryption software empowering people to safeguard their privacy online and PGP went on to become the most widely used email encryption software in the world and I would like to get started by asking you, Phil, what got you interested in privacy and cryptography?

Phil Zimmermann (02m 18s):
Well, I released this in 1991, but during the 1980s I was active in the nuclear weapons freeze campaign and so there was an adversarial relationship between the White House and the peace movement during the 1980s and so it seemed like grassroots political organizers would need some way to protect their communications and also I was interested in the human rights angle in other countries where the adversarial relationship is deadly and so they needed it even more. It was originally a human rights tool.

David Greely (02m 54s):
And how did you get into the cryptography end of it?

Phil Zimmermann (02m 58s):
I have been interested in cryptography since I was a kid. You know how kids get a little telescope because they are interested in astronomy? Well, this is kind of like that. It's something that appeals to kids and you don't need a telescope. I read a children's book

when I was 10 years old called Codes and Secret Writing, and it's for kids teaching them, I think it was written in the 1940s or early fifties and it's teaching kids about substitution ciphers, transposition ciphers, making invisible ink out of lemon juice, that sort of thing and so I just thought it was so cool. It's obviously not serious cryptography, but for a kid it's entertaining. Kids like to send secret messages, they don't want their teachers to see what they are writing in notes.

David Greely (03m 42s):
And then you got interested in more serious cryptography, which was public key cryptography, which I think was first implemented for public use in PGP. How did you get interested in public key cryptography or how did you begin working with it?

Phil Zimmermann (03m 56s):
When I started at Florida Atlantic University in 1972, that dates me. You can see that I have a lot of gray hair. I wrote a program in basic that encrypts things. That was several years before public key cryptography came out and so I was interested in cryptography at that time, but I mean, nobody knew anything about public key cryptography. So fast forward a few years and the paper New Directions in Cryptography came out and so did the RSA paper. So those two papers really energized the whole field. In fact, it was so exciting that a lot of mathematicians that specialized in other things switch their specialty over to cryptography. It was those two papers were the most significant papers published, well, particularly New Directions in Cryptography by Whit Diffie and Martin Hellman. That was the most significant paper in the field published since World War II, maybe one other paper before that. So the field became quite energetic after that and I couldn't do anything. I couldn't implement it because you know, you needed a big computer to do anything with it and at that time there were A-bit microprocessors and those were not capable of doing the kinds of calculations you need to do.

David Greely (05m 10s):
And so by the time you get to the 1990s, the computers are getting better and you are able to implement it. At the core of PGP is the concept of a decentralized trust model. And I was hoping you might be able to explain that to our audience. What does a trust model? What does a decentralized trust model and how does it work in PGP?

Phil Zimmermann (05m 32s):
When public key cryptography was invented, everybody thought it was a real breakthrough in how to manage cryptographic keys. Because before that, if you wanted to communicate with someone who was far away, you would have to figure out a way to get both of you to agree on the common key and governments could easily do that. They could put a guy on an airplane to Moscow with a briefcase handcuffed to his wrist, and then get to the American Embassy in Moscow in a special room, unlock the briefcase and pull out the key material and now they can communicate with Washington, but that's not practical for ordinary people. Not, you would quickly run out of money buying all the plane tickets. And so public key cryptography, we thought that that would solve the problem because you could publish one of the keys and keep the other one private, and then anyone could send you an encrypted message by using the key that you publish.

Phil Zimmermann (06m 21s):
You could put it on your business cards or put it in the New York Times or something like that. But it turns out that it's not quite as simple as that because you still have some complexities in key management because when you get someone's public key and want to encrypt a message to them, how do you know that public key really belongs to them? Maybe some bad guy was tricking you into using a different public key, maybe his public key, the bad guy's public key, in which case you might encrypt a message to, you think you are encrypting it to your friend who is very far away, but you are actually encrypting it to the public key of the bad guy and you try to send it to your friend and the bad guy intercepts it. He crypts it with his private key and then re-encrypt it again with the real public key that you intended to use and sends it to your friend.

Phil Zimmermann (07m 10s):
And nobody knows this happened except the bad guy and so that was the remaining problem in public key cryptography, the dancing in the streets that everybody felt, oh, this is such a breakthrough, we don't need to worry about managing keys. Well, yeah, you have a different problem to solve. It's called the man in the middle attack. The bad guy can sit in between Alice and Bob and he can pretend to be Alice from Bob's point of view. He can pretend to be Bob from Alice's point of view, and he can, without having any crypt analytic skills, he can just simply pass messages around. It reminds me of when I was in high school, my modern European history teacher had fought in World War II as a naval. He stood up on deck with those flashing lights and they would flash Morse code messages to each other in foggy nights, you know, and his ship had somehow stumbled into the middle of a Japanese convoy and he told great stories about World War II, but this was one of the most interesting.

Phil Zimmermann (08m 10s):
And so the ship in front of him, which was a Japanese ship, flashed a challenge response message to him, which he had no idea what it meant and if he didn't give the correct response, then everybody on his ship would die. So he turned around and flashed the same message to the ship behind him, which was another Japanese ship, and then got the response from that one and turned around and flashed that one to the ship in front of him, thereby saving everyone's lives and so I just thought that was such a compelling story. It's not really about cryptography, but it is pretty similar to the man in the middle attack that I described earlier and so that's where most of the complexity is. You're trying to solve the man in the middle problem and so how do you know if you get, let's say if you, you get your hands on someone else's PGP key and you want to encrypt a message not so fast.

Phil Zimmermann (09m 00s):
How do you know that PGP key public key belongs to that person? Maybe it doesn't. Maybe it's got their name on it, but maybe a bad guy put his own public key there with someone else's name on it to trick you into using the wrong public key and so how do you solve that? Well, maybe you need a trusted introducer, someone who's a mutual friend of the two parties and that person can do a digital signature on the public key of the other person and introduce you to them through this properly notarized and signed public key and the guy who signed it is saying, well, I vouch for this. I know that this key goes with this name that's attached to the key and so the question is, who is the guy that signs the keys? Is it a mutual friend? Everybody's got a network of friends, right?

Phil Zimmermann (09m 49s):
Or is it some certificate authority at the top of the food chain that everybody is forced to trust? You are forced from on high dictating that you have to trust this institutional entity that how do you know what, they are not going to make a mistake, sign the wrong key or more maliciously, deliberately sign the wrong key. Maybe it's the Chinese government. Should a Chinese dissident rely on getting the public key of say, a human rights organization that's been properly signed by the Chinese government, well maybe that's not such a good idea. So having a centralized trust model with a an authority at the top, like that little pyramid on the back of a $1 bill with the I at the top, maybe that's not the only way to do things. Maybe it's better to have a decentralized approach where everybody is free to sign anyone else's key.

Phil Zimmermann (10m 40s):
And you might get download a key from a key server with 20 or 30 or 40 signatures on it from all kinds of people, most of whom you don't know. But one or two of those people might you recognize as your friends and say, okay, I believe that this key belongs to who it appears to belong to because these two people that I know and trust signed it. I don't know about all those other people that signed it, but I don't care because these two people signed it. And that's the decentralized trust model that PGP uses. It's more resilient, it's fault tolerant, it's grassroots. It's from the bottom up rather than the top down and it more reflects the way in which human society works. We have friends that we meet directly and talk to directly and trust directly. We don't have friends that are handed to us by the apex of the government who says, here, you should be friends with this person. You should trust this person. Well, no, human societies are quite decentralized. So that was my actual decision in PGP.

David Greely (11m 41s):
And it is fascinating, right because there could be 20 people who say this key belongs to Alice and you might trust that that key belongs to Alice because you know a different four people than I know. So we will both trust the key, but for different reasons.

Phil Zimmermann (12m 01s):
If both of us downloaded Alice's public key from a key server and it's got the same 20 signatures on it, when you downloaded it as when I downloaded it, we both look at that key with 20 signatures and we trust that the key was properly vouched for, but for different reasons. You are the people that you regarded as trusted introducers are different people than I regard as trusted introducers. But it still gets the job done because it's a redundant fault tolerant design. Even if somebody wasn't paying attention when they sign Alice's key, who cares? There is 19 more people that sign Alice's key.

David Greely (12m 37s):
And then you and I could both sign Alice's key if we wanted to. And then more people might trust it because they might recognize and trust me or trust you.

Phil Zimmermann (12m 48s):
I used to get a lot of emails from people asking me to sign their public key and I had to turn them down because I was drowning in requests like that.

David Greely (12m 57s):
That feels like that could open up a another vector of attack.

Phil Zimmermann (13m 00s):
Right, yes.

David Greely (13m 02s):
And so you have kind of talked about the decentralized model and then there is I have heard you talk about the centralized model as a subset or a special case of decentralized trust.

Phil Zimmermann (13m 14s):
So you could have somebody who specializes it in being an introducer in the other trust model, the centralized one, we have certificate authorities and they typically sign fees for websites and so you might need only one signature on a website's public key if it's signed by a highly trusted certificate authority. But you could have somebody who is highly trusted, who is very, very careful and meticulous about signing people's public keys. You know, maybe he looks at their passport and makes absolutely certain that they are who they say they are and they give them their public key and he signs it and gives it back, maybe charges money for it because It's a lot of work that would be an introducer that is trusted by a lot of people and so he is kind of like the certificate authority in the, in the centralized way and so the centralized trust model is a proper subset of my trust model. Or another way is to say that my trust model is a proper super set of the centralized trust model.

David Greely (14m 18s):
And what trust model is right for which situations in your experience?

Phil Zimmermann (14m 24s):
I think that quite often the centralized trust model works just fine. When I was living in the Netherlands, the healthcare system there used these smart cards that doctors and hospitals used for signing, I don't know, signing things, you know, like prescriptions or who knows, ordering tests or something. And it's all a single monolithic healthcare system in that country and so it kind of makes sense to have a centralized certificate authority signed the public keys that's locked up inside the chips on the smart cards or maybe a military organization. They tend to be monolithic. And so you can have a centralized trust model for those kinds of situations where the institution that's using it is centralized, but in a heterogeneous society of people with different agendas perhaps competing with each other, perhaps rivals, it's better if they used a decentralized trust model to make it work in a disorganized, chaotic society where people are friends for a while and maybe not friends and they sign keys that they, that they did their due diligence on. And it's more organic, it's more fault tolerant, it's more decentralized and it works well for a larger non-centralized society.

David Greely (15m 42s):
Yeah. And you had mentioned that the decentralized trust model seems much more analogous to how we operate in real life. You have friends, you introduce people, and much more aligned with how we interact and establish trust in real life. So why are centralized trust models so dominant in the online sphere right now?

Phil Zimmermann (16m 04s):
Well, as I said there are places where it's okay to use them in a monolithic centralized bureaucracy or something like that. Government employees just saw this movie a couple days ago, A House of Dynamite directed by Catherine Bigelow. It's about a nuclear attack on the US and it shows how everybody in the, you know, in Stratcom, the strategic command, the White House situation room, the radar stations and all this, how they talk to each other in an authenticated way and they insert their government issued smart card into their computer terminal that shows the video conference and so, you know, everybody is legitimate that there's no Russian spies there and so that's a perfect example of a place where a centralized trust model works just fine

David Greely (16m 53s):
But we see it in a lot of other places as well. Are there market forces or government pressures that have been pushing us towards using these centralized models more than decentralized?

Phil Zimmermann (17m 05s):
Like I said, sometimes it works okay, but I think for a heterogeneous society with possible rivals and competitors all trying to communicate, even competing companies might still need to talk to each other. In fact, even in military environments, I said that the military was a good example where a centralized trust model would work well. But what if the military has to work with other militaries in other countries in a coalition environment? Well, if each one has its own centralized trust model, then now you've got some added complexity that you have to sort out and so not everything can be perfectly centralized. But you mentioned about the usefulness of mimicking human society. Well, human beings evolved over millions of years and our, I'm not talking about trust models right now, but I am talking about encryption in private communications, private conversations before all this technology arrived for a million years before that, since human speech got started, our brains evolved with the expectations that you could have private conversations with people even before we were homo sapiens.

Phil Zimmermann (18m 13s):
And all the way up until the invention of the telegraph or radio communications, you expect that every conversation you have with somebody is going to be private. If there is somebody standing nearby listening to your conversation, overhearing it, well then go out behind the barn and talk there and you can expect to have a private conversation with the arrival of all these communication technologies, the invention of the telegraph, the radio telephones, all these things started to make greater opportunities for somebody to covertly listen to your conversation and so the way in which we conduct our social interactions has evolved over the millennium, many millennia to even our, the organic construction of our brains is feeling like when we talk to somebody, it's private because it always was for a million years and yet today it's not because, I mean, we're talking through an electronic channel right now and most of the conversations we have today are through electronic channels.

Phil Zimmermann (19m 18s):
And yet our brains have this sort of unconscious expectation that when you talk to someone, it's just between you and me to remedy that we need encryption, especially end-to-end encryption. And so in 1991 when I developed this, there needed to be an end-to-end encryption tool and that was strong and so that was the motivation for PGP. It was just for ordinary people to talk to each other, but it was also for human rights. When human rights workers are talking, they don't want the autocracy to listen in because they're trying to help the human rights situation in a country that has an abusive autocracy. So there is a need for strong encryption. Now, we all know this today, but you know, in 1991 there were no good tools around. Even the best tools at the time used small keys like 56 pit data encryption standard, which can be broken by anyone with a reasonably powerful computer. That was the purpose of PGP, is to try to restore things to the way they were before the invention of telecommunications.

David Greely (20m 30s):
And do you think people have adapted or do we still lack discretion? Do we still assume that we're having private conversations when we're not?

Phil Zimmermann (20:40):
Yeah, well, so strong is this evolutionary adaptation that we have for talking and with the expectation that it's a private conversation that the majority of people that are talking to each other through electronic channels, whether those be phone calls or internet conferencing or something like that, they all still, the majority of them still think that it's a private conversation. And so people that have a career in cryptography are more careful about that. But your mom probably isn't.

David Greely (21m 13s):
And I am probably not many times now that I think about it. Well, I wanted to fast forward because you know, today for most people when they hear crypto, they think Blockchain and cryptocurrencies and given your long experience with cryptographic tools, do you think we need to be rethinking about how we use cryptographic tools and, and using them differently than the way they're getting employed in say, Blockchain and cryptocurrency?

Phil Zimmermann (21m 42s):
We have been using cryptographic tools before the invention of Blockchains and cryptocurrencies. In fact, the word crypto itself is the shortened form of the word cryptography. Unlike people that come to cryptography from the point of view of just cryptocurrencies, they tend to think that when they hear the word crypto or when they say the word crypto, they mean cryptocurrency. But real cryptographers don't like that. They, for professional career cryptographers, the word crypto means cryptography. I have a sticker on the back of my laptop and also the back of my iPad that says, it's a sticker that says crypto means cryptography. That's a struggle that's hard to overcome because for so many people, their understanding of what, of how cryptography is used is just cryptocurrencies. So yeah, for them crypto means cryptocurrencies.

David Greely (22m 33s):
And what gets you excited in cryptography today?

Phil Zimmermann (22m 37s):
You know, when I did PGP, I did it for email because that was the low hanging fruit. I really wanted to do it for telephone calls. Telephony is the natural way that human beings speak to each other. I mean, non-telephony, I mean face-to-face conversations and telephony kind of extends that through a mediating technology. But verbal communications is easier than composing an email and sending it. It's quicker, it's smoother, it's faster and so I was always interested in encrypted telephony, but I had to do encrypted email first because the enabling technologies weren't available yet. Nobody had broadband. If you don't have broadband, it's harder to do secure telephony or any telephony. Well, other than the old fashioned kind, you know, analog copper wires and analog signals. So I have always been interested in that kind of use of cryptography, but I am better known for my work in PGP just because of the strange situation that we had in 1991 when nobody could do any kind of end-to-end encryption.

Phil Zimmermann (23m 43s):
Every way in which you could talk to someone that are far away for the average person. I don't mean governments has the risk of interception every possible way that you can communicate back then had the risk of interception. And PGP changed that for the first time. There was a way for the average person, not some government sending keys to their embassy in a foreign capital. It was for the first time possible for ordinary people to communicate over great distances without the risk of interception. Now later on we see that there is still the risk of interception because Intel agencies, if they can't break the cryptography, they just try to insert malware on one of the endpoints. So your computer might have malware that was put there by some Intel agency and that malware will exfiltrate your cryptographic keys, enabling them to decrypt the traffic between you and the other party. And so it's not that they could crypt analyze it, it's just that they became increasingly clever in, in inserting malware on your computer.

David Greely (24m 46s):
It's even more frightening. I, I think back to using email for me in college in the early 1990s and realizing everything that was sent back and forth was an open book and then thinking of course, the late nineties, we saw the whole rise of internet commerce and really couldn't have had that without cryptography.

Phil Zimmermann (25m 10s):
Internet commerce needed strong cryptography. In fact, if you look at historically how this played out, why did governments have the attitude that they had in the nineties? It's because back in World War II, the US and the UK broke the axis powers, encryption algorithms, the German enigma, the Japanese purple cipher, they found a way to break it. They, they had to put incredible amounts of money and effort into it. I mean, a good example is Bletchley Park, which is where they broke the enigma and other high level German ciphers and Japanese ciphers. But it was top secret there. And nobody blew any whistles because everyone who worked there was morally aware. They felt that they were more doing what was morally right because London was being bombed every night by the Lu Wafa. So they had moral clarity about what they were doing. So there were no Snowdens or any other whistleblowers.

Phil Zimmermann (26m 07s):
And they shortened the war by probably a couple of years in both theaters. The Battle of Midway was decided by being able to read the Japanese encryption and also the war in Europe was shortened by a couple years for the same reason. And so it probably saved a couple million lives and so after the war, the US and the UK decided that they would do everything possible to prevent foreign governments from getting their hands on strong encryption because if another war came along, they wanted to be able to do the same thing again and so the work that they did at Bletchley Park was they destroyed the Colossus computer that they had built to read

Hitler's email. They swore everybody to secrecy and they kept that attitude about encryption for decades all the way up to the nineties and so that's why they were so aggressive about trying to keep strong cryptography out of people's hands.

Phil Zimmermann (27m 02s):
The US had export controls, the US didn't have domestic controls, but the FBI was attempting to impose domestic controls. The French had no export controls, but they did have domestic controls. The British had a little bit of both and, and so we had to fight hard through the whole 1990s to get these governments to loosen up and the US to allow strong encryption to be exported. PGP was a major part of that struggle. They tried to put me in prison for developing and distributing PGP. And so for the whole decade we had to fight hard to lift the export controls. We had to stop the FBI from imposing domestic controls. The French finally woke up and realized that they wanted the economic benefits that the US was enjoying from e-commerce. So they got rid of their domestic controls. And by the end of the nineties, things had changed. The French had dropped their domestic controls and in 2000 the US dropped their export controls and they never were able to get any traction on domestic controls. The market forces were against it. Nobody wanted to buy products that had back doors in it for the FBI much to the surprise of the FBI.

David Greely (28m 15s):
And how big was the commercial drive of internet commerce to forcing the hand of governments to loosen up?

Phil Zimmermann (28m 24s):
In the early days, it wasn't very big. And so it took a while to make that point. We had to show that this was going to grow and grow in the early days of the internet, it wasn't obvious that this was gonna turn into this behemoth driver of economic activity. But once that started to gather momentum, then it became an irresistible force.

David Greely (28m 47s):
We had the early promise of the internet was gonna be this great democratizing liberating force. But often with web two we see that it's become a powerful surveillance tool for big companies and for government. How central do you think the loss of privacy has been to the early promise of the internet not being met?

Phil Zimmermann (29m 11s):
Well, I remember a friend of mine, John Perry Barlow, who was a co-founder of the Electronic Frontier Foundation. He also was a lyricist for the Grateful Dead. He was quite active in writing and speaking about the promise of the internet. He compared it to the invention of fire. He said, no, the invention of the printing press is not adequate to address the magnitude of the innovation of and effect of the internet. He said it was more like the invention of fire. He had a very optimistic view of how the internet would benefit society. But what happened over the course of the decade since then is that we have discovered that the internet has not been this sort of utopian influence. It's turned into a dystopian influence. In fact, I mean, well social networks have divided us so severely that it fractures our society and turns people against each other and facilitates the rise of autocrats. And so, I mean the internet is so, especially social networks with their algorithms to put you in a bubble have been very damaging to society.

David Greely (30m 14s):
And is there a way that we can use cryptography, some of these tools to break out of those bubbles? Like I am also thinking about, you know, now of course everyone's focused on artificial intelligence and the flood of actors on the internet that even passed the touring test going back to Bletchley Park. Do we need to think about this differently?

Phil Zimmermann (30m 37s):
There's the 'I'll be back,' spoken with a Schwarzenegger accent.

David Greely (30m 42s):
Is there another hill that has to be conquered now given the challenges that the internet didn't work out as planned and now we have got AI?

Phil Zimmermann (30m 51s):
We have to struggle against, it's not specific to AI, it's about the growth of surveillance technology. The human population does not double every 18 months, but the ability for computers to surveil us and keep track of us does because of Moore's law and so this means that the growth of surveillance power is outpacing the growth of the human population and so this leads to dystopian outcomes. If you

live in a country with a good democracy, you might not worry about that because things seem to be okay, you know? But in no matter which country you live in, it's possible that there could be an election that elects someone who wants to consolidate his power and turn it into an autocracy. We have seen that in numerous examples around the world. In Hungary, Victor Orban is a kind of an autocrat and some years earlier, Hungary was a vibrant democracy.

Phil Zimmermann (31m 48s):
Right after the Cold War, they were focused on Western Europe. They wanted to become another, another democracy like Western Europe and it looked like they were heading in that direction for a while, but now today there is an autocrat in charge and, and so whenever you live in an autocracy, you have to be concerned that the autocrat is gonna try to consolidate his control over all aspects of society. You know, getting controlling press, controlling the courts, controlling academia, controlling all kinds of things to consolidate his power and it means that speaking against the autocrat is dangerous. You could be arrested or worse and so if you want to organize any political opposition to try to win an election, to change back to a democracy, you need to be able to have private conversations to organize politically. So for that, you need strong cryptography, end-to-end cryptography, not just something that it's hop wise encryption where it's decrypted at the server and then re-encrypt and sent somewhere else.

Phil Zimmermann (32m 53s):
It's got to be end-to-end encryption. That means that, well, it's got to be something that the government, the autocracy, if you are unfortunate enough to live in a country with an autocracy, can't intercept it and see who is opposing them and go arrest them. So it's essential, it's a very political technology. It's essential for maintaining resistance to autocrats, emerging in holding onto power. So you might decide that you don't care about that so much because maybe you live in a country with a leadership that you trust in a democratic process that seems to work pretty good. But if you allow them to put back doors in and allow them to build the elements of surveillance, not just in things relating to communication or cryptography, but also video cameras to, to solve crimes. You know, Britain has so many millions of video cameras with facial recognition software behind those cameras, just like the Chinese have.

Phil Zimmermann (33m 49s):
And you might think, well, Britain is, is a democracy, so what have we got to worry about? Let them have their surveillance apparatus. The problem is, is that you are only one election cycle away from potentially somebody consolidating their power and then using that surveillance capability that they inherited from their predecessors to maintain surveillance on any political opposition that might emerge and so then they can stay in power for very, very long periods. So there is a connection between, it's not only encryption, it's also trying to resist maybe just in policy space, resisting the growth of surveillance technology.

David Greely (34m 29s):
There is back doors and then there's the front doors and before you go, and I really appreciate you taking the time to share your experience and your insights, but I wanted to ask you a question about the future of cryptography and that is the risk of people being able to come in the front door, the risk pose to current techniques, current cryptographic techniques by the development of quantum computers. How big of a risk is quantum computing to current cryptographic techniques and where would we need to go next in order to preserve privacy online?

Phil Zimmermann (35m 05s):
Many years ago, like 20 years ago, I didn't really take it seriously because in order to build a quantum computer that is capable of factoring large imagers is something that's just very difficult to build because you have to isolate it from the outside universe, which is easier said than done but then NSA announced that everybody should get ready for quantum computers and no matter how you feel about the NSA, whether you trust them or you don't trust them or whatever, if they say, if they warn you, you better get ready for quantum computers and you would better get ready for quantum computers. And so for some years everybody's been scrambling to do that. In fact, NIST started soliciting submissions for post quantum algorithms that would be resistant to quantum computers to build new of the key algorithms. It's public key algorithms that are affected most by quantum computers, well by this theoretical quantum computer that has sufficient complexity and power to attack the key sizes that we currently use.

Phil Zimmermann (36m 08s):
The NSA calls these cryptographically relevant quantum computers, it even has an acronym for that and so what we've seen though is that it's so difficult to get them powerful enough to do that, that it may be exponentially hard. And if it is, then we are not gonna see cryptographically relevant quantum computers in our lifetime, even if everything works perfectly, it might be like 2050 before we see this and well for my lifetime that that's a little bit right at the edge of my lifetime and so it's like nuclear fusion. You know, nuclear

fusion has been, I don't know, 20 or 30 years away in the future for the past, I don't know, 60 years. So maybe there will be quantum computers that are sufficiently powerful to do it, but it's certainly taking them a long time. So I am not quite as alarmed about it now, as I was before, I used to give talks on this.

Phil Zimmermann (37m 01s):
I kept on reminding people that, look, it's not that the messages you are sending now are gonna be broken by a quantum computer now, but in the future, Intel agencies will archive the traffic that they intercept today and they store it in these giant disc farms. I saw the NSA built this facility in the Utah desert. I saw aerial photographs of it. It looks like a Tesla gigafactory and it's just jam packed with disc drives and so they don't know how to decrypt this traffic, use strong cryptography today. So they can't decrypt it. I mean, they can insert malware and exfiltrate your keys, but if they didn't do that and they intercepted the traffic, they store it in these giant dis farms hoping that someday they'll be able to get their hands on the keys perhaps with the help of a quantum computer in the future.

Phil Zimmermann (37m 45s):
And so this is the archive today, analyzed tomorrow threat so that it means that we need to hurry up, migrate all of our public key algorithms to post quantum versions, post quantum algorithms to replace RSA Diffie home and elliptic curve with post quantum replacements.

David Greely (38m 14s):
Do we have those post quantum replacements now or do those have to be developed?

Phil Zimmermann (37m 17s):
We do. There has been a number of, I mean, all you have to do is find, you want to find a problem that is very fast to calculate in one direction, but extremely slow to calculate in the opposite direction. Like for example, you can multiply two very large prime numbers together in the blink of an eye, takes no time. But if you wanted to take that composite number result and factor it back into the original prime numbers, it takes longer than the lifetime of the universe and so that's how you build public encryption algorithms.

Phil Zimmermann (38m 37s):
Well, the problem is, is that quantum computers, if they ever get powerful enough, they will be able to do that factoring much faster within minutes. But we may never reach that because it's so difficult to build quantum computers isolated from the rest of the universe. So I would say error on the side of caution and start using public key algorithms that have nothing to do with factory. I mean, Diffie Hellman is based on discrete log rhythm, the discrete log problem, but that also is related to factoring. So if you could do fast factoring, you can break not only RSA, but Diffie humming and also elliptic curves. But we should find new algorithms that have nothing to do with factoring and that's what all these post quantum algorithms are and so NIST has recently, you know, come out with some standards about this and they are doing more work because they want some more signature algorithms, for example and so we are getting ready to transition to that. But it's going to take years of intense work because everybody's fully entrenched with software that is not easily changed because the engineers who wrote that software have retired or they don't work there anymore or something like that and so it's a difficult migration, but it will take years. So people are working hard on doing that migration.

David Greely (39m 55s):
Well, it sounds like we have still got work to do, but you sound optimistic about the future, at least in the tools, we just need to know how to use them.

Phil Zimmermann (40m 03s):
Yeah, I think that we'll be able to develop post quantum algorithms, but I am not as worried about, worried about the speed of which then happens now as I used to be because the progress in cryptographically relevant quantum computers is just slower than, it's not very alarming. Could change. I mean, at some point they could make a breakthrough and speed things up quite a bit. And then we don't want to be caught with our pants down.

David Greely (40m 29s):
I guess before we go, is there a, an area that you are focused on these days? What, if anything, makes you optimistic about the use of cryptography and being able to, to build a better online way to interact that's closer to the way we interact in real life?

Phil Zimmermann (40m 45s):
I mean, I think we have pretty mature cryptography and there is lot of different protocols that serve useful purposes. There's VPNs, there's TLS that lets us do our e-commerce and online banking. There is SSH for remote administration of servers. There's PGP, there's secure telephony products like Signal or silent phone. There is a lot of protocols that work really well for solving their particular narrowly defined problem. But my original motivation for developing PGP had to do with the preservation of democracy and to try to give us a way to organize politically should a, an auto crack come to power and consolidate his power and make it hard to dislodge him without having a political opposition, being able to organize by talking to each other securely. And so now I worry more about other things that aren't just cryptography. I worry about surveillance technology, traffic analysis, facial recognition software behind all the millions of video cameras, tracking where you go and seeing if you're doing something that is a threat to the incumbent autocrat.

Phil Zimmermann (41m 56s):
And also even other things that make it easier for autocrats to get elected. Sometimes the moderate political parties, that would be our way of protecting ourselves from autocrats. Sometimes they have widely unpopular policies that increase the probability of the other parties, the more extreme parties from they can come to power in an election and then use their power to seize control. And we see this in a number of countries in Europe, for example, alternative for Deutsche Line. It's a far right party that it's a little bit too much like Germany's painful history with that. And we see things happening in the US that are going to be hard to deal with. So I worry more about the big picture of preserving democracies all over the world. You see these democracies sliding into autocracies and autocracies like to help each other. North Korea, China, Russia, Iran, they all, they don't have any common ideology, but they like to help each other stay in power.

Phil Zimmermann (42m 58s):
And democracies also do better if they are surrounded by other democracies. And so I look at this not just about cryptography. I am sort of typecast as Mr. PGP or I am known best for my work in cryptography. But the big picture that I am seeing now is the rise of autocracies and how they get into power, how they maintain power, how do they eventually get removed from power and surveillance plays a part of that and secure communications is of some considerable benefit to being able to resist them. But it's not the only thing you need. It requires a lot of vigilance. Back in the seventies, I had a friend who took me up in his airplane. He had a small airplane and we flew out over the ocean and came back and he let me take the stick and steer the plane. And I found that something very interesting that if I let go of the stick, the plane continued flying straight. And I just thought that was pretty clever that the plane was designed to do that. Of course, I only let go of the stick for a minute or so. Probably if I didn't touch the stick for a longer period then it would gradually get worse and worse. But anyway, I just thought that was pretty cool. And not all airplanes are like that. The F 16 fighter is not like that. In order to win dog fights, they had to design it to be unstable, and they require avionics computers to actively control it, fly by wire. And if that computer ever crashes well, so does the airplane no matter how good the pilot is. And so you have these two different kinds of airplanes. One of them is stable when you take your hand off the stick and the other one, well, the F16 is kind of stable because the computer tries to make it appear to be stable. But if you take away that computer control, it quickly will crash And so I used to think for a long time, I used to think that democracies were kind of like that airplane where I could let go of the stick. That I look around and I see democracy everywhere and I say, oh, democracies must be stable.

Phil Zimmermann (45m 07s):
Well, no, they are not. They're more like the F 16 without the flight computer. It requires constant effort to keep them flying straight and so I worry about democracies because of that, and I try to do things to facilitate the preservation of democracy. For many years, it was about providing cryptographic tools, but it, we got to also fight this in policy space. We have to try to impede the deployment of pervasive surveillance technology. This is not something that could be easily solved with cryptography. You can't encrypt your face, but you have to find some way to push back in policy space, not just by deploying encryption software.

David Greely (45m 48s):
Thanks again to Phil Zimmermann, Creator of Pretty Good Privacy, or PGP. We hope you enjoyed the episode. We will be back next week with another episode of Re-engineering Tokenization. We hope you will join us.

Announcer (46m 03s):
This episode is brought to you in part by Abaxx Exchange, bringing better price discovery and risk management tools to navigate today's commodities markets through centrally cleared, physically deliverable futures contracts in energy, environmental, battery materials, and precious metals markets. Smarter Markets are here. Contact sales@abaxx.exchange to get started.

That concludes this week's episode of SmarterMarkets by Abaxx. For episode transcripts and additional episode information, including research, editorial and video content, please visit smartermarkets.media. Please help more people discover the podcast by leaving a review on Apple Podcast, Spotify, YouTube, or your favorite podcast platform. SmarterMarkets is presented for informational and entertainment purposes only. The information presented on SmarterMarkets should not be construed as investment advice. Always consult a licensed investment professional before making investment decisions. The views and opinions expressed on SmarterMarkets are those of the participants and do not necessarily reflect those of the show's hosts or producer. SmarterMarkets, its hosts, guests, employees, and producer, Abaxx Technologies, shall not be held liable for losses resulting from investment decisions based on informational viewpoints presented on SmarterMarkets. Thank you for listening and please join us again next week.