

egoblog.net

Transcript (par Margot MF) en anglais du podcast de Philip Zimmermann
30/06/06

Tristan Mendès France: Philip, first of all hello!

Philip Zimmermann: Hello Tristan.

TMF: Thanks a lot for accepting this small chat with me from Paris. So you are at the center of an incredible debate concerning freedom of speech, cryptographic and security issues. All started in 1991 when you created the PGP, a programme that enables everybody to have secured and encrypted communication. Today you're coming back to us with a new programme that secures audio chatting. So here is my first question to you Philip. First of all, what do you say to the people who fear your technology and believe that it could be used by bad guys or terrorists?

PZ: Of course they're right, it certainly can be used by bad guys and terrorists, but that's true for many other technologies, in fact one example is the highjackers of September 11th purchased GPS receivers, we know that because of later investigations and they intended to use these GPS receivers to guide them to their targets. Well that is actually the original purpose for GPS. It was originally a military technology. Of course we use GPS for many civilian purposes now, but the highjackers used it for its originally intended military purposes to direct where their target gets to. So this raises an interesting question : should we stop selling GPS receivers? Because we'd want to keep it out of the hands of highjackers or terrorists Imagine the effects on the rest of the civilian economy if we were to deny every one access to GPS technology. Cryptography is a technology that has been used by the military over the centuries but in the information age the rest of us need it, the same way we need other technologies like GPS as a fuel for the economy, e-commerce depends on strong cryptography. I can't think of a way of denying access to modern technology or to cryptology in general without denying every one access to it.

TMF: Do you understand all the debate that's arousing around those questions?

PZ: Of course I do, I've been engaged in that debate for almost 15 years. I think it's a good debate, it's a valuable debate, but I think it's a debate we've all been through in the 1990s, it's a debate that we all fully took into account the idea of terrorists using this technology. In fact that subject the idea of the terrorist using this technology was actually at the focal point of the debate, during the 1990s in the United States and in Europe.

TMF: Who was precisely your support at that time?

PZ: Well the entire computer industry and not only the computer industry, the civil libertarian, civil academia, other cryptographers, parts of the US government, parts of the French government, parts of many other governments, you know the government is not monolithic. There are some people in government that like this technology. They think it's good for society and other parts that are concerned about criminals using it and terrorists using it. I am concerned about criminals and terrorists using it, and I know the bad guys are using this technology, but as I said, they use all manners of technologies that the rest of us would use and depend on. You can't stop them from having it without stopping everyone from having it

TMF: Do you see a difference, in America at least, between Democrats and Republicans when it comes to questions concerning encrypted communication?

PZ: Well both Democrats and Republicans are concerned about privacy and civil liberties, but I think that they tend to view it in slightly different ways depending on who is in power. During the Clinton years, the Republicans were quite active in opposing the export controls on strong cryptography [...]. And many Republicans in Congress were opposed to it at that time, including John Ashcroft who was a Senator at that time who later became attorney general. In fact I suspect that's why Ashcroft did not read, did not try to reverse the gangs that were made in cryptography after September 11th, after although he was attorney general he had previously taken the position as a Senator to liberalise the export control on strong cryptography. So although I disagree with John Ashcroft on almost everything else at least he was consistent on the assumption of people being allowed to use cryptography.

TMF: Have the cryptographic issues change since the 9/11 events?

PZ: Certainly a lot more people were concerned about terrorism and they now have a greater and closer experience with concrete examples of terrorists. But the general concept of terrorist using strong cryptography was always a central theme in the debate that took place in the 1990s. That debate had a participation of the US Congress, the computer industries, civilian academia, journalists, the Courts in the US, you know everybody in the US, it took several years and over the course of several years, we reached a near consensus, not a perfect consensus mind you, but a near consensus that strong cryptography was good for society that its benefits out-weighed its disadvantages.

TMF: Is this debate going to hit Europe, or France soon, considering that European legislation is not compatible yet or hasn't completely integrated the fact that we can use your technology?

PZ: Well you know European countries are all involved in that debate in the 1990s and as I said, that debate certainly discussed terrorism quite a bit, that was a central theme in the debate. So the question of will it hit Europe soon, I think it would be better to ask : didn't it already hit Europe many years ago, of course it did. Now whether it comes up again in Europe, I don't know, if it does come up again, I would certainly argue that why didn't you guys think of this before because the rest of us were debating it before, the rest of us engaged in the debate about cryptography, talked about terrorism all the time, this was a discussion that was all over Europe including France. France had domestic controls on cryptography for many years and they dropped those controls in the late 1990s, out of recognition of the importance of strong cryptography for promoting the internet. France wanted to promote the internet so that they could read the economic benefits that they saw the Americans were experiencing with the internet boom.

TMF: Ok Philip thanks you very much for these few minutes of insight and again sorry for my weird English and I hope to see you in Paris if you actually drop in again, it would be a pleasure to see you this time.

PZ: Alright it would be nice to visit Paris again, I hope that it will not be so hot as it was a couple of years ago. Have you had any air-conditioners installed?

TMF: Well a little bit and it's getting even hotter.

PZ: It's global warming.

TMF: Unfortunately, ok, thanks very much Phil and take care.

PZ: Thank you.

egoblog.net