

CARLOS MOREIRA

Founder and CEO of WISeKey

Alvise GIUSTINIANI

Talking about digital, I will pass it over to Carlos. We talk a lot today about blockchain, about cryptocurrency and Facebook launching Libra. Microchips are becoming cheaper and cheaper so you can almost print them on goods. How is all this playing into the illicit trade? Do you see it positively, is it helping? Is it helping the bad guys or the good guys?

Carlos MOREIRA

Thank you, Alvise. As was said yesterday, technology can be used as a weapon or as a tool, you can destroy, or you can construct. Just to give you a history on the technology of what we now call blockchain and how it can really enhance the fight against illicit trade. The World Wide Web, which is the invention that happened in Geneva, I was actually at the United Nations when it happened and at that time there was a lot of hope because we expected the Web to solve a lot of problems.

You now have a USD 10 trillion economy sitting on the top of the Web with companies like Apple, Facebook, Amazon and Google. All of them have been extraordinary efficient in monetizing the World Wide Web and creating a lot of wealth, but they have been extraordinarily inefficient in one specific thing, which is digital identity. The Web is blind, it does not know what it is doing. Obviously, you can transfer good things on the Web, but you can also transfer very bad things. What has happened is that illicit trade and also issues related to the underground economy are using the Web in an extraordinarily efficient way to do bad things. The reason is that the people on there are trying and there have been some very good companies like LVMH, and we have been helping many companies in WISeKey, to improve their defence systems. These companies are working in silos and when you are dealing with a USD 2.4 trillion problem, which is illicit trade, you cannot work in silos, you have to build platforms.

The platform is something that stakeholders can use one entry point to access endless amounts of data, which is not the case now. If a government or a private sector company wants to investigate illicit trade issues where do they go? They go to a database and those databases are not available to them and so they have to negotiate credentials to access the database. This has been extraordinarily inefficient. That is why Interpol and many police organizations around the world are totally in a situation of needing to centralize data. However, it is very difficult to centralize data because there are commercial and ownership, intellectual property issues.

In the last five years a new technology has arrived with the name blockchain, which could be the beginning of solving the problem. Although, I always say and I have been working on blockchain since the beginning, blockchain is only one of the components not the only one. We are creating in security, cybersecurity and technology a convergent historic point where what we call deep tech technologies are converging. You have artificial intelligence, blockchain, digital identity, the Internet of Things – IoT – and all these technologies are now talking to each other. This is creating an unprecedented power to solve critical problems for which we did not have the tools to solve before.

I was in the UN before and then I left and created a company because I wanted to solve the problem not just talk about it. We have already secured 1.2 billion objects, so those are watches in Switzerland, which are now traced with a microchip that is put inside the watches, or wines, perfumes and food products, because the traceability of a product cannot be established if you do not have a digital identity. The digital identity that is embedded in the project as I said with a microchip, is also available in a blockchain ledger. For you to understand if you do not understand it or are not confronted by blockchain technology, the beauty of blockchain is that decentralized data; you do not have to have the data in one place. If the visual identity of my object, let us say an LVMH watch is traced at the object level, the digital twin of that product is also available in a ledger and then that ledger is available for anyone to see, so no one can stop



you accessing the ledger. Let us say that a watch has a chip and it is in a ledger, when someone walks into customs, they can detect if the product is fake or has been falsified because the identity of the product has not been embedded.

This is creating a very interesting proposition. It is also a great advantage for brands, and if they do not cooperate in this it will never happen, because brands can also know where their objects are and who owns them. The ownership of the object has a very big advantage for the brand because brands no longer know their customers. Nowadays, many brands, with maybe the exception of LVMH which has a very strong digital strategy, would need to go somebody like Facebook or Amazon to know who their clients are because the client is registered with Facebook and not the platform. That creates an advantage because now at the same time, you are protecting your product and creating a KYC, know your customer, facility that allows brands to reengage with customers.

Then you have the Libras of the world. Libra is in Geneva and so am I and I am very involved with the team there and they are trying to understand how Libra can expand out of Geneva. There are good things and bad things about Libra. It has an amazing thing which is that they are creating a digital currency, which could become dominant because they have 2.5 billion active users. The other thing is that if Libra do not apply the financial regulation principles of KYC, it could also be used to move money illegally on the Internet. Putting KYC compliance into projects like Libra, on cryptocurrencies is a must, otherwise technology designed to do good can end up doing bad. One example of that is the Dark Web which now has a USD 1 trillion economy. Originally it was designed by intelligence services which wanted to enter the underworld and see where bad things were happening, and it was actually absorbed, used and manipulated by the underworld basically to create their own digital ecosystem.

The good news is that there are a lot of technologies there. The bad news is that we need conferences like this and an international multi-stakeholder approach to use those technologies in a way that satisfies regulatory requirements worldwide.

Alvise GIUSTINIANI

Thank you, Carlos. On technology you are upbeat on some parts and still doubtful about others. Libra needs to be regulated in the right way. Before going to Jean-Francois, I would like to come back to Laurent and ask his opinion. You went from 20 million in one year to 21 million takedowns, do you think we are winning the battle or is it a mountain that when you reach the top, there is an even bigger one yet to climb?

Laurent MARCADIER

We are indeed at 20 million takedowns. Now our goal is to have 20 million stay-downs because, and this is obvious, as soon as one counterfeit ad is taken down, another one pops up in its place.

Carlos talked about the technical aspect, which is very important for rights-holders, but I think standards and legislation is where progress is really needed. We have to get the big Internet companies to take more responsibility.

Strides have been made in the areas of taxation, hate speech and content of a terrorist nature. Discussions are moving forward for this kind of content to be taken down by the Internet giants upstream, not just after it is reported.

In this comprehensive approach, which I hope and pray for, I think we need to make the Internet giants responsible for all illegal content. In other words, let us stop creating micro-subjects depending the nature of the content that is spread and let us finally follow a recommendation the European Commission made in May 2018 calling for responsibility for all illegal content. Let us take this cross-sector approach.

We, public officials and rights-holders, face a common foe: hackers, counterfeiters and criminal organizations. Is our response too fragmented? A global, cross-sector approach must also apply to the Internet, and I hope our debates will be an opportunity to make headway on increasing the digital giants' responsibility. That is the technical work that must be done upstream. They have the resources to do it using tools and instruments to screen out illicit content involving counterfeiting, hate speech and terrorism. I think deeper involvement by the Internet actors will solve a good part of the problem.



Alvise GIUSTINIANI

Thank you, that's a perfect segue for Jean-François about regulation.