Neighbourhood Watch - transcript of presentation video

Nick: The next team up is Team Neighbourhood, please come in, please make them for a welcome.

Good afternoon, we are team Neighbourhood Watch, and we are dealing with privacy neighbourhood KYC data sharing.

Meet Alice, Alice is a successful entrepreneur and she wants to bank with you, from what she tells you, her business is based in a high-risk country, but there are no other red flags that you can see.

So, today you take her through your standard KYC checks, CDD checks, and EDD checks and ultimately you on-board her, but through those checks you don't uncover that she's been linked to human trafficking through another bank. Imagine if you had access to that information, imagine if you could ask the whole neighbourhood what they knew about Alice.

Introducing Neighbourhood Watch, Neighbourhood Watch is a platform that allows banks to securely and privately query data sources from other entities. Neighbourhood Watch lets you get intelligence from across the network to make better, more informed decisions. Neighbourhood Watch lets you decide about what to about Alice and people like Alice, who profit from the trafficking of over 2.4million people worldwide.

We know that in the current landscape, there are barriers to data sharing, both real and perceived, and we've put some of these up on the screen now. In particular, regulatory ambiguity, time lag and limited collaborators. The facilities that exist for data sharing at the moment do not cover the entire industry, so we know that there is a gap there and the time lag in the facilities that exist today are quite long, that gives criminals an opportunity to exploit that delay.

Neighbourhood Watch addresses these problems and the real-world impact is that we have a robust framework for intelligence sharing. Leading to richer EDD, a risk-based decision making and ultimately accelerated disruption of criminal networks.

So, how do we do it? We leverage significant advances that have happened over the last several years in the area of homomorphic encryption. Specifically looking at work that has been done, with nation states and other organisations to be able to do operations at scale. We also look at some of the other, we look at some of the other barriers that exists within organisations and data collaboration, which oftentimes require consolidation of data assets.

We want to let the data assets remain at the organisation that is helping and providing data in the neighbourhood, and sit above that and allow secure and private access, but the data owner always retain positive control of the data asset and access to it. But this enables a mechanism for us to have secure and private queries initiated by a third party and then run over environments that have been configured to have access to that. It allows a framework for us to be able to provide the Neighbourhood Watch, so as we look at, how do we deal with it.

When we are looking at the TechSprints specifically, there were number of challenges that we wanted to address. Is the software straightforward enough that organisations can actually adopt it or is it going to be something that is going to take years for them to be able to accomplish. So, the good news about this is, it's based on a software deployed model that allows organisations of all sizes to be able to participate in the Neighbourhood Watch.

So, specifically we enable a piece of software, that requesting party, that allows them to keep their queries secure and private to them and they are the only ones that knows the questions being asked, and the results being produced and they can engage with organisations that have opened up data, now the data initially maybe very small, might be one column, one row, but overtime we establish a trust network. We are able, then to be able to look at other things as regulation and policy change, that we might be able to make available to the neighbourhood, but what happens if when we have a bad neighbour? I am the data owner, and I don't want you coming into my data because you've done something to abuse the framework governance model that we've put in place with your organisations, because the data owner maintains positive control of the data assets and access to it. We don't allow you to come as a bad neighbour, so there is all kinds of mechanism in place to be able to leverage this and this is something that is deployed at scale and different scenarios today.

So, the problem we were looking at, is that Alice had come in and we were looking at information that we had internally and we were making decisions based on what was available at the time. We on-boarded her, which means we gave her significant window to do things, that were bad. If we had access to the neighbourhood, we would have then been able to detect, that there was a flag out there that we should have considered, now this isn't an automatic de-risking process, it's something that triggers a higher review and extra due diligence as part of the process.

So, with the neighbourhood, we now have access and we would have made a different decision about on-boarding Alice. So, what have we built as part of the TechSprints, to start to demonstrate the solution and bring it to life? So, we started with the data that was provided to us by the FCA, we loaded that into an industry standard KYC analysis tool and de-risking the customers, then we took the output of that and put it on a secure enclave, we then analyse the data and essentially credit 3 of the banks, each of which we put in a secure encrypted enclave.

We then designed series of questions, encrypted questions that we could leverage with homomorphic encryption to essentially query in a privacy enhanced way. We also took a look at the data and built within the institution Bank A, 3 other jurisdictions, privacy enhanced jurisdictions and designed series of questions, that we could ask to essentially anonymise aggregate and leverage the risk intelligence that we might have on any bad actor across multiple jurisdictions.

So, in terms of an encrypted query, what is it? So, you could see it from the left, you can see this is what the requesting bank will ask for, and on the right, it's what the requesting bank would see. So, this is essentially the mechanism that we can leverage to for protocols, standards and automatically understand what level of matching it supplies and in terms of an encrypted response, again the responder, the bank provides the response, can't see what's going back, but the request, do then could see the information, I could consume it.

So, in terms of quick demonstration, what you will see here is Alice has raised a red flag, so we are going through enhanced due diligence, we can see that she currently has CDD risk of 1,114 and a number of risk factors have been identified against her. We then now using Neighbourhood Watch can query external sources, what we are going to do is to ask questions to others the bank, to see does Alice's data match?

So, we can see that Bank A doesn't hold any data on Alice, Bank B and Bank C, they hold some information and we could see that the several conflicts so that might be indicative of, you know I need to put on extra due diligence against those fields. We can also check and see within our institution, cross geographies. Do we just raise Alice financial crime red flags? Is it something that we are aware of within our network about Alice that raises concerns? And then we can see Alice risks has been updated, it's been increased, and we kind of have much better, faster picture of Alice's risks, to make better more informed risk decisions.

So, this is something that is available today and you can leverage for an internal use case to get started or you can look at other crash sharing type of scenarios. The ultimate goal is that, you've got a platform that allows you to be able to embrace different types of data sources as they become available without having to read through an entire process.

So, in summary we looked at Alice and the on-boarding of her, we looked at how we can leverage this breakthrough in homomorphic encryption to help us and most importantly to put the real access flexible and adaptable privacy enhancing technology platform in place.

FCA

FINANCIAL
CONDUCT
AUTHORITY