Financial Privacy and the Fight Against Financial Crime

As more and more activities occur online, with more participants than ever, the importance of privacy and data protection is increasingly apparent, with the UN reporting that 128 out of 194 countries now include legal protections, for processing personal and other data. At the same time financial crime professionals are increasingly proposing extending personal data sharing to more effectively combat financial crime, both with and between those in the private sector and with and between those in the public sector as well as between each other.

This increased data sharing, requires in many cases a new legal basis, beyond where existing norms permit. The rationale for such proposals have been shared with leading policy makers and a dialogue is underway which includes privacy advocates and data protection guardians.

Where in some quarters these proposals and discussions have been characterised in terms of more information sharing means less privacy protection, and maintaining restrictions on information sharing as perpetuating weaknesses in fighting financial crime programmes, this is a misread. In fact whilst it may at first appear counter intuitive I believe that information sharing done differently, can improve overall privacy and financial crime outcomes.

There is increasingly a consensus by Financial Crime experts who believe, that the new frontier in fighting financial crime successfully has to be through modernising the approach, from single siloed activity, huge false positives to work through and mass reporting of low quality reports to law enforcement, to a much richer set of reports, that have much higher confidence levels of involved criminality and much greater actionable intelligence, targeting those areas that are priorities for law enforcement.

That new frontier also includes new ways of working, for example in collaboration and partnership that by necessity brings data together with individual organisations bringing their own piece of the jigsaw which can be combined in aggregate to see the bigger picture. That bigger picture may well be to better identify and target the bad guys but it is also about dealing with the unintended consequences, removing the significant friction that has been built up in the system and reducing the significant bycatch that affects far too many innocent people.

From pilots and proof of concepts the evidence shows that there is a strong argument that these new methods could significantly improve the fight against financial crime AND reduce high levels of false positives that plague the system. These two outcomes, in my opinion, is where we need to focus, but we need some help in providing a clearer legal basis in order to achieve these outcomes, and that legal basis includes persuading privacy and data protection guardians that this not only makes sense from a fighting financial crime perspective but also from a privacy and data protection perspective.

Rights to privacy are cornerstones of our way of life, and encompass the right to be left alone and they increasingly include the right to know and to have a say in how our personal information is used and for what purpose, both by the State but also by None state actors, including commercial organisations. These rights to privacy are not absolute rights though. They stand together with other rights that also seek to protect the individual and wider society, which include protection from criminality, where harms come in many forms, and are not limited to accumulating illicit funds, from individual victims, but can also impact personal health outcomes and broader economic prosperity.

Finding this balance is what we must strive for. I believe we need to evolve our thinking in terms of privacy and data protection, but we are also obligated to make a case that includes assessing impacts on privacy and data protection And that we should only ask for support where a case can be made that makes sense.

Such a case cannot be made simply to allow Law Enforcement to outsource their responsibilities, or for the private sector to save on costs, or for a new RegTech solution to generate income for investors.

A case may not even be made if it resulted in the arrest of a small number of additional criminals, or even if it prevented a single terrorist event, though we may have a heavy conscience after such an event and the victims and their relatives may ask searching questions of us all.

For a case to be made the benefits should be substantial, AND safeguards need to be in place to mitigate any risks to privacy and in all cases we need to continue to apply reasonable and proportionate data protection measures. This should all be done transparently and subject to relevant oversight and assurance.

I believe a case can be made and safeguards included.

For example in the US information sharing between FIs strictly for the purpose of investigating financial crime has been legal since 2001, following 9/11, and is being used sparingly under controlled conditions.

Internationally, over the last few years due to closer working partnerships between the public and private sectors in many countries new but limited information sharing has led to increased law enforcement outcomes, through dedicated public private partnerships. In all these cases, information that is shared is either none personal information or where it is personal information it's limited in terms of volume and it's purpose clearly understood, which has also meant that whilst these initiatives are considered successful, they are not of themselves going to have a major impact overall.

What they have done though is prove the case and point to new ways we should be considering in order to be much more effective.

But is different types of information sharing for example between private sector organisations to fight financial crime and with law enforcement also good for our privacy and data protection rights?

I believe it is. To me this is not about doing more it's about doing things differently and achieving a much better balance than we have today.

We shouldn't still be trawling using huge dragnets and then sifting through the huge daily catch, which is made up largely of innocent bycatch. That applies as much to transaction monitoring as it does to name and sanctions screening. That is not good for our privacy rights.

We shouldn't still be filing far too many low quality reports, that are of no material interest or use, that suggest suspicion but all too often represent unusuality or are the product of gaps in information that exist and can't be reasonably explained because of a lack of data and or information that is available and could be used to remove any lingering suspicions. That is not good for our privacy rights.

We shouldn't be letting those that cause significant harm, harvest our data in places like the dark web, and then use that data against us, and even when we find out who these people are, are unable to warn others to protect more of us from Financial fraud especially but not just against the vulnerable. That is not good for our privacy rights.

And lastly

We shouldn't be letting important anonymous shell companies avoid disclosure of those with material interests, particularly as we know the corrupt and the criminal are users of these companies.That is an excessive level of privacy we can't afford, though legitimate rights to privacy even here can be better balanced.

By modernising the fight against financial crime, we are focussing on being more effective. In order to be more effective we need to do information sharing differently. As we do more of what makes sense, we also need to do less of what doesn't.

I believe those that advocate for reforming the fight against financial crime also need to be privacy advocates. There are too many calls for reform that simply haven't thought through the implications that for example data pooling proposals or mass information sharing suggestions would have on the privacy and data protection landscape. For those that have and suggest a right balance will make more progress.

Remember these are not opposing positions. I also believe that Privacy guardians should also consider joining the chorus for fighting financial crime Reform, that includes adjustments to privacy rights with safeguards that make sense.

What works best is when we find the right balance. We don't have it right now and it's good to have this conversation and this opportunity to contribute to this debate.

Thank You.

John Cusack
Chair, Global Coalition to Fight Financial Crime
April 21st, 2021