Disclaimer: This is my personal position, I don't speak for my employer.

Given widespread Internet surveillance by an unknown number of entities all over the world, attempts to control surveillance using legislation won't work. We rather need technical solutions that make surveillance difficult or impossible.

Assured identification of communicating parties is a weak spot in secure protocols and is one of the primary problems that needs solving.

It is an obvious attack vector to manipulate entities who perform identity verifications and produce identity assertions. Centralized technologies to solve this problem should be avoided, as they can be manipulated more easily than decentralized technology.

Future communication protocols must require redundant, multi-track identity assertions from disjoint entities.

Also, it's necessary to avoid a false impression of security. While opportunistic encryption can help against casual eavesdropping, it's insufficient to protect against targeted surveillance. User facing applications should never give feedback based on opportunistic encryption used in the background, but only after having performed a multi-track identity assertion.

I've proposed the MECAI and DetecTor.io projects as potential solutions or at least inspiration how multi-track identity assertions could be provided in the context of PKI and TLS.