Joint Declaration of the European Police Chiefs

We, the European Police Chiefs, recognise that law enforcement and the technology industry have a shared duty to keep the public safe, especially children. We have a proud partnership of complementary actions towards that end. That partnership is at risk.

Two key capabilities are crucial to supporting online safety.

First, the ability of technology companies to reactively provide to law enforcement investigations – on the basis of a lawful authority with strong safeguards and oversight – the data of suspected criminals on their service. This is known as 'lawful access'.

Second, the ability of technology companies proactively to identify illegal and harmful activity on their platforms. This is especially true in regards to detecting users who have a sexual interest in children, exchange images of abuse and seek to commit contact sexual offences. The companies currently have the ability to alert the proper authorities – with the result that many thousands of children have been safeguarded, and perpetrators arrested and brought to justice.

These are quite different capabilities, but together they help us save many lives and protect the vulnerable in all our countries on a daily basis from the most heinous of crimes, including but not limited to terrorism, child sexual abuse, human trafficking, drugs smuggling, murder and economic crime. They also provide the evidence that leads to prosecutions and justice for victims of crime.

We are, therefore, deeply concerned that end to end encryption is being rolled out in a way that will undermine both of these capabilities. Companies will not be able to respond effectively to a lawful authority. Nor will they be able to identify or report illegal activity on their platforms. As a result, we will simply not be able to keep the public safe.

Our societies have not previously tolerated spaces that are beyond the reach of law enforcement, where criminals can communicate safely and child abuse can flourish. They should not now. We cannot let ourselves be blinded to crime. We know from the protections afforded by the darkweb how rapidly and extensively criminals exploit such anonymity.

We are committed to supporting the development of critical innovations, such as encryption, as a means of strengthening the cyber security and privacy of citizens. However, we do not accept that there need be a binary choice between cyber security or privacy on the one hand and public safety on the other. Absolutism on either side is not helpful. Our view is that technical solutions do exist; they simply require flexibility from industry as well as from governments. We recognise that the solutions will be different for each capability, and also differ between platforms.

We therefore call on the technology industry to build in security by design, to ensure they maintain the ability to both identify and report harmful and illegal activities, such as child sexual exploitation, and to lawfully and exceptionally act on a lawful authority.

We call on our democratic governments to put in place frameworks that give us the information we need to keep our publics safe.

Trends in crime are deeply concerning and show how offenders increasingly use technology to find and exploit victims and to communicate with each other within and across international boundaries. It must be our shared objective to ensure that those who seek to abuse these platforms are identified and caught, and that the platforms become more safe not less.