Last week, Muslims around the world celebrated the end of Ramadan. Celebrations were held in many countries, including here. There was however a notable exception: China. There the authorities banned such celebrations. This is not surprising. A recent article of the New York Times from the city of Kashgar showed the extent to which the Chinese authorities are using facial recognition and snooping technologies to keep a tight control of the Muslim community.

If you think that this does not concern you because it is happening far away, you would be terribly wrong. The Chinese experiment bears a great significance for all of us. It shows to what extent the cozy relations between technology companies and state security agencies can harm us. This has become particularly acute as part of states response to terrorist threats and attacks. States around the world have increased their surveillance arsenal, not always to the benefit of our safety. On the contrary, in several occasions they used it to silence criticism, restrict free assembly, snoop into our private life, or control individuals or minorities.

An illustration of this comes from human rights defenders. If in the past human rights defenders have been ahead of states in using technological progress to expose human rights abuses, now they are facing a backlash. As we speak, states and non-state actors are intercepting their communications, intrude their personal data, trace their digital footprint. States are using technologies to learn about human rights defenders’ plans or upcoming campaigns; to find or fabricate information that can help intimidate, incriminate or destroy their reputation; or to learn about their networks and sources.

This concerns us all. At stake here is the society we want to live in and bequeath to the next generations. Technology should maximise our freedoms and rights – and keep those in power accountable.

To get there we need to strengthen the connections among us and crowdsourcing human rights protection, promotion and engagement. An important step in that direction would be to provide more support, funding and digital literacy training to human rights defenders. It is also crucial that the private sector and state authorities uphold human rights standards in the designing and implementation of all technological tools.

Living in an increasingly digital world does not mean living artificial lives with artificial liberties. Our rights must be real, all the time.

We all must resist the current backlash and persist in demanding more human rights protection, more transparency and more accountability in the digital world.