Data Free Flow with Trust and international data spaces: sustainable and successful frameworks require a focus on fundamental rights and data minimisation

Speech delivered by Estelle Massé, Europe Legislative Manager and Global Data Protection Lead at Access Now, at the G7-DPA Roundtable in Bonn, Germany, on 6 September 2022. Check against delivery.

Dear Commissioners,

On behalf of Access Now, an international organisation working to defend and extend the digital civil rights of people around the world, thank you for inviting me to contribute to today's meeting and to highlight the importance of digital rights in the context of international data transfers and data spaces. I will focus in particular on three key issues: data minimisation, international convergence of data protection rules, and your role as regulators.

Data flows with trust are critical, not only for a free and open internet but also for the realisation of human rights online. But without robust and comprehensive data protection, data security, privacy safeguards, and human rights frameworks that protect people's information, none of these benefits can be achieved. As privacy and data protection commissioners of the G7 countries, you are all acutely aware of the global convergence and progress made in the last decade to protect personal data. You are also aware of the gaps that remain and are preventing people from being able to fully exercise their data protection and privacy rights.

The largest outstanding gap relates to data harvesting, which underpins the current digital economic model – despite many of us having doubts about its economical and social benefits or even its legality. Most tech companies and many governments take a "collect it all" approach, which is directly at odds with basic data protection principles such as data minimisation and purpose limitation. To be sustainable, the digital economy requires public and private organisations alike move from data harvesting to data detoxing; prioritising quality over quantity.

For international data transfers to be sustainable, data minimisation is key. After all, the less data collected, the less data to be secured or moved around.

The nature of the internet and the online economy demands that data can flow easily, to ensure services are delivered across borders. However, this is not and should not be a free pass for ignoring or lowering data protection principles.

In today's world, protecting personal data is not a luxury, it is a necessity. We are encouraged by the global trend towards the convergence of privacy and data protection rights, and we call on all G7 states to confirm their commitment to both.

Most countries have recognised that privacy is a human right and many of them have adopted, modernised or started developing data protection frameworks which include tools for data transfers.

Yet, despite this progress, many companies have yet to change their practices and business models in a way that would make them respect and promote data protection and privacy.

A 2015 study of more than 300 ICT companies in the UK, France, and Germany showed that 72% of data gathered by these companies did not end up being used. Other studies from the US and around the world suggest that anywhere between 60 and 80% of the data collected by companies goes unused. With the rise of artificial intelligence and profiling, companies are often trying to figure out how to make money from this unused data. Instead, companies would do well to ask themselves, or be pushed to do by regulators: why was this data collected in the first place?

Online entities have largely been collecting any and all data they want about any person. This can harm people considerably and lead to data-driven discrimination that can, among others, affect employment, health, housing, and educational opportunities. Data minimisation and purpose limitation principles, which have existed for quite a long time, should apply to stop this from happening – but they are largely ignored.

If these principles are not binding or not enforced, companies and entities will continue to collect more data than they need – despite not knowing what to do with it – and the potential for people being harmed will continue to increase.

Because every minute this unused data remains stored unnecessarily, everytime it is transferred across jurisdiction without needing to be, people's rights are placed at risk and companies are potentially liable if the data is leaked, misused, or accessed without proper authorisation. Some companies would justify the continuation of the "collect it all" practices by promising transparency and strong security. These promises are important but insufficient if they don't go with a reduction of the amount of data collected. The best way to prevent data breaches is not to have the data in the first place.

We must incentivise companies to only collect data they need to deliver their products or services, to do so transparently, and to store it securely. Collecting data that might be "useful" in the future for a theoretical undefined purpose is not in line with data protection principles. Data minimisation, purpose limitation, data security and transparency are not interchangeable; each principle is as important as the other, yet they overlap and complement one another, allowing businesses to operate with confidence and reassure people that they and their information are safe.

I know that many of you here today are looking into data minimisation. Access Now was pleased to hear that the FTC plans to crack down on harmful commercial surveillance and lax data security, particularly given the relationship between the data harvesting business model and the way algorithms are currently being built. Often, troves of data are injected into opaque

AI and automated systems to place ads, sell products, and even generate text or image content. Some surveillance technologies are so dangerous that they cause more problems than the ones they are commissioned to solve. The use of facial recognition and remote biometric technologies in publicly accessible spaces enables mass surveillance and discriminatory targeted surveillance that ruin lives and communities. The consequences are severe. It is critical that regulators around the world address the misconception that for the digital economy and AI to succeed, as much data as possible is needed – when what is actually needed is the best possible quality of data - which is more limited.

Another reason that data mining has become commonplace is because, until recently, data storage was cheap. But with energy prices now soaring and the reality of the climate crisis looming larger than ever, we also need to consider the environmental impact of data centers, which use up massive amounts of electricity to stay cool and keep running. Reducing the amount of data collected via enforced data minimisation can play a part in tackling the digital economy's carbon footprint.

Data minimisation and purpose limitation principles can help reduce the amount of data flowing across borders, even if it is not a silver bullet for data transfer disputes, it can reduce tensions. But there's a larger, more fundamental problem at the heart of several ongoing data transfers battles. Governments have been taking advantage of the "collect it all" approach of companies to, in turn, largely, "access it all" via their surveillance programmes. To make data flows safe and sustainable: governments must reform surveillance frameworks and develop clear rules for lawful government access to personal data.

The OECD is working to advance discussions on this issue. In December 2020, they rightly acknowledged that "disproportionate government access to data held by the companies is a crucial issue for data governance and the protection of individual rights and [...] a potential barrier to enabling the free flow of data with trust." And while talks between OECD countries may have progressed with difficulty, they are moving forward – and countries are reckoning with their own surveillance practices and disproportionate ability to access data. It is crucial that these talks embed principles of transparency, access to remedy, independent oversight, necessity, and proportionality (and when we say embed we don't mean token "name dropping", we mean make these principles the genuine foundations of a rights-respecting approach). Many of you in the room are tasked with enforcement, oversight and the protection of these principles. So we are counting on you to get this message across to your governments, both here at the G7 and at the OECD.

Beyond the OECD conversations, access to remedies and independent oversight are at the core of several ongoing battles over data transfers. The future EU-US data transfers arrangement, for instance, must comprehensively guarantee these rights and principles. We know this will require legislative changes in the US and we encourage US lawmakers to implement the needed reforms.

The recently launched APEC Cross-Border Privacy Rules also raise significant red flags in its structure and around oversight and enforcement. This framework relies on self-certification

systems that are insufficient to ensure data protection as it lacks adequate oversight and enforcement mechanisms. We understand that countries want to move data across regions and around the world, but to ensure “Data Free Flow with Trust ", this concept must be rooted in security, privacy and safeguards – which the CBPR is not. In fact, the CBPR stands at odds with the convergence we see happening between most countries in Latin America, Europe, Africa, and part of Asia who are focusing on binding and comprehensive data protection rules, including for transfers. The OECD discussion I previously mentioned is also a demonstration of this convergence, where tough questions are being put on the table, to address how national and domestic laws on surveillance may impact not only business operations, but people’s fundamental rights. Convergence, instead of interoperability of norms or self-certification, is central to ensuring data free flow with trust.

A few words on international data spaces, which seem to generate more interest and excitement everyday. Data spaces are a way to organise data so they can be used or re-used; this means that these spaces must be designed with data protection, data security, and privacy principles at their core. We’ve noticed that very often, discussions around data spaces focus on the potential benefits and undefined innovations they may deliver; but we must remember that innovation for innovation’s sake alone is both valueless and purposeless. Innovation is not always synonymous with positive progress; it can have negative consequences, particularly when reinforcing the harmful “collect it all” attitude. There are plenty of surveillance and digital oppression related innovations in the world; but I’m sure you would agree that such tools undermine democratic principles and human rights. Innovating how we organize data must not translate to lowering our data protection standards. This undos any good created by the innovation in question.

Before wrapping up, I’d like to leave you with two steps you should take to safeguard human rights in data collection. One is a commitment, and one is an invitation.
Firstly, the commitment. As you reflect, discuss, and prepare for your communiqué today and tomorrow: commit to putting human rights, privacy and data protection at the heart of data governance. In recent G7 and G20 documents such as the Carbis Bay Communiqué, G7 nations reaffirmed the principles of data free flow with trust, but then contradicted this by presenting the exploitation of data as an opportunity for businesses and portraying the protection of personal data as a challenge — ensure your discussions keep focus on what’s most important: the protection of people’s information.
Without data protection and privacy rules, we cannot have Data Free Flow with Trust. As regulators, you can shift the digital economy from thinking of personal data as a commodity, to restoring it to its rightful place as information that belongs to and is controlled by people. Data protection isn’t about never using any data; it’s about using data in a wise, secure, necessary and proportionate way.

And now the invitation. On behalf of Access Now, I would like to invite you all to our next global conference, RightsCon, which will be held in Costa Rica from 5 to 9 June 2023. We look forward to continuing this important progress with you there and to opening the debate to private, public, and civil society voices in Latin America, and beyond.

Thank you very much for your attention and for including an NGO voice in your conversation today. If I may, I highly recommend that this becomes a standard practice for all future G7 meetings, and encourage you to bring even more of our civil society partners to the table.

I look forward to the rest of the discussion.

ENDS