Can the EU afford to drive out American cloud services?

by Zach Meyers, 2 March 2023

Some EU countries want to stifle foreign cloud computing services. These countries' concerns are not irrational. But disadvantaging America's cloud giants will do Europe more harm than good.

The European Commission has grand ambitions for the digital transformation of European businesses. To achieve this, the Commission wants 75 per cent of European businesses to adopt cloud computing services or similar technologies by 2030. The target is inexplicably specific, but the sentiment makes sense. Cloud services allow businesses to access computing resources like data storage remotely and on demand, using shared infrastructure – which is often more efficient, more secure and more easily scalable as businesses grow.

The only wrinkle: American tech firms like Amazon, Microsoft and Google currently dominate the European cloud computing market. Chinese firms like Alibaba and Huawei are keen to make headway. Despite some member-states' support for European champions in the sector, European cloud companies remain minnows.

Beyond some EU leaders' vague concern that Europe lacks 'digital sovereignty' because of its dearth of large technology companies, cloud computing poses specific worries. Cloud computing companies host vast amounts of Europeans' personal information and business secrets. If foreign governments can force cloud companies on their territory to give them access to data, that will violate EU legislation like the General Data Protection Regulation (GDPR), impinge on Europeans' rights, and allow industrial espionage (a concern that applies even to the EU's allies). Some European member-states therefore want to constrain foreign cloud computing firms' ability to win sensitive contracts in Europe. Their concern is not entirely ungrounded, nor is it uniquely European. But the EU needs a dose of hard-nosed pragmatism. If Europeans are too rigid, they risk harming their own security, growth and tech ambitions.

Governments largely seek user data from cloud computing companies for two reasons: national security and intelligence gathering; and law enforcement. The GDPR was supposed to address concerns about national security and intelligence gathering: it prohibits companies from sending data to foreign

authorities, unless those authorities meet EU privacy standards. Given its dominance in cloud computing, the EU's main focus has been the US. The EU and US recently concluded an agreement to strengthen protection of Europeans' data in the US, in order to restore free EU-US data flows after the European Court of Justice ruled that US protections were not up to European standards.

However, the GDPR is not the end of the story. The EU is also worried about foreign laws – such as those passed in recent years by the US and China – which require cloud computing companies to hand over to law enforcement even data stored in Europe, with little or no regard to the GDPR.

Foreign law enforcement agencies currently have several choices when they want to obtain data held in the EU for criminal investigations. These agencies can seek the co-operation of EU authorities under a mutual legal assistance treaty (MLAT). The EU has no gripe with this approach. However, the EU would never agree such a treaty with China out of human rights concerns, and the EU-US treaty has proven inadequate: requests for data typically take ten months to process. Instead, foreign authorities often prefer to demand data directly from businesses. In the US, for example, this process was codified in the CLOUD Act of 2018. This law requires cloud computing firms to hand over data held offshore, as long as the firm has some minimal connection to the US (although in practice the largest cloud computing companies are all headquartered there). This option bypasses EU authorities, undermines MLATs and does not provide European-style protections. The EU has pushed back. The GDPR generally prohibits firms in Europe complying with unilateral requests for personal data. The EU Data Act – a proposed law which tries to solve a number of different problems with dataflows in Europe – will, in many cases, prohibit cloud computing firms from complying with foreign authorities' unilateral demands for non-personal data. Some EU member-states also have their own similar 'blocking statutes'. As a result, cloud computing firms are often in an invidious position when faced with a direct request from foreign authorities for data held in Europe: either breach European law by disclosing the data, or risk breaching the foreign law by withholding it.

Although requests for data by foreign law enforcement agencies are relatively rare, the Commission claims they undermine European business confidence in using cloud computing services. Whether or not this is true, some member-states – including Italy, France and Spain – want to intervene. The EU's cybersecurity agency is currently developing a security certification scheme for cloud computing services, called EUCS. These member-states want cloud computing firms to be eligible for the highest level of certification only if they are 'immune' from foreign law – which, reportedly, might require firms to have their headquarters within the EU, to store European data within the EU, and to only allow personnel in the EU to access that data. News reports suggest that not all EU member-states agree. But any compromise will probably still include the concept of 'foreign law immunity' in one shape or form. The scheme will be voluntary, but it will make a difference: EU businesses and governments will think twice before buying a service that lacks the highest security certification. A recent EU law will also allow the Commission to make the scheme mandatory for companies like telecommunications and energy firms when they buy cloud services.

The 'immunity' requirements would be a significant departure from the EU's swathe of recent cybersecurity initiatives, which have generally been non-discriminatory and widely welcomed. The EU's plans for 'foreign law immunity' have transformed a relatively obscure technical document into a hot political matter, with EU capitals at loggerheads. American cloud firms are in despair. The UK has even raised concerns in the EU-UK Trade Partnership Committee.

Despite these protests, the EU is unlikely to fully back down.

First, the EU's 'digital sovereignty' concerns are not idiosyncratically European. The US also prohibits firms from disclosing data held in the US to foreign law enforcement authorities, except when Washington has an agreement with the foreign government concerned. China's Data Security Law similarly limits the transfer of important data outside China.

Second, a suggestion by business that the EU should more actively discriminate between the US and China is a non-starter, at least for now. The EU ought to be much more concerned about China than the US. But the EU has always opposed restrictions which specifically single out China – both because of the Union's commitment to international trade law principles and because of its more mercantilist approach to China. If the EU insists that foreign law enforcement agencies' data requests must provide European-style safeguards, then both the US and China fall short.

Third, a mooted EU-US agreement on obtaining cross-border data for law enforcement would help but would not be a panacea. The EU and US have started to negotiate such a deal. But the negotiations will prove difficult: after all, the EU's institutions spent years agreeing rules for cross-border access to data for law enforcement even within the EU, and agreement was only reached only in recent weeks. Even if the EU rapidly concluded a similar agreement with the US, it would simply give the US another option: it could access data under the newly agreed method (subject to whatever safeguards the EU agreed) or it could continue to make unilateral requests under the CLOUD Act. The new method would hopefully prove more efficient than using MLATs, and lead to fewer CLOUD Act requests. But it would not preclude such requests. To rule out use of its unilateral CLOUD Act powers, the US would probably need to change the CLOUD Act itself. But in today's Congress, that would face formidable hurdles. After the ECJ case which blocked seamless EU-US personal dataflows, Washington avoided new privacy legislation. Instead, it is relying on a Presidential executive order to restore the free flow of data between the EU and US – even though relying only on such an order, rather than passing new legislation, significantly increases the risk that the ECJ might once again find US protections inadequate.

EU member-states pushing to provide a 'European-only' security certification are therefore unlikely to give up – and even sceptical member-states are reportedly unlikely to ditch the idea of 'foreign law immunity' completely. The EU's concern with digital sovereignty is valid. But Europe needs a sober assessment of the economic trade-offs. Would Europe be better off without the largest cloud computing firms being able to win important European contracts? Or would excluding them carry large costs – for European security, businesses, and for its own cloud computing ambitions? If critics are right that the 'immunity' requirement is merely disguised protectionism to support European digital firms, then it is even more important that Europe consider the economic and security impacts carefully. In fact, these impacts are likely to be overwhelmingly negative.

First, the rules address one specific risk – that foreign authorities will access European data – but, overall, they would weaken Europe's cybersecurity. Firms with global scale and reach can more easily adopt some types of cybersecurity measures – such as splitting up data and spreading it across multiple global data centres, to reduce the risk of its exposure – than local or regional firms can. They can also use global data flows to spot emerging cybersecurity threats more quickly. And their ability to use and reroute traffic through multiple data centres across the globe means they can maximise their resilience to natural disasters and security incidents. The EUCS would therefore discourage European businesses

from using cloud computing services that have the most advanced security capabilities – making cloud services in Europe less resilient and secure. Data would be less exposed to US investigators, but could be more exposed to rogue states and cyber criminals with far fewer qualms. Perversely, this effect would be strongest for sensitive contracts where this security is most important.

Second, the EU would lose out economically by stifling competition between cloud computing firms. Brussels recognises that European firms need to increase their use of cloud computing to boost their productivity and competitiveness: in fact, the Commission justifies restrictions on foreign cloud firms by saying these restrictions will improve trust in cloud computing and increase Europeans' use of cloud services. Disadvantaging the largest and most attractive service offerings is a counterproductive way of achieving that. It would distort competition, give businesses fewer choices, and give European cloud firms fewer incentives to improve their services and reduce their prices.

Third, given the EU has a trade-intensive economy, member-states should not disregard claims that the EUCS would breach international trade law. The EU believes it can rely on relevant World Trade Organisation (WTO) agreements, which allow discrimination against foreign firms for national security and privacy reasons. However, the EUCS rules would need to choose the method of protecting security and privacy which imposes the least possible distortion on trade. A blanket ban on foreign-headquartered firms would not achieve this. For example, in at least some cases, cloud firms can use end-to-end encryption, which means that data stored in the cloud is only accessible to the user – it cannot be unencrypted by the cloud service provider, and so the cloud provider cannot hand any useful data over to a foreign law enforcement agency. The US has done itself no favours here. It has relied on national security requirements for far more spurious reasons, such as to impose tariffs to protect its steel and aluminium industries. But it is in the EU's broader economic interests to support WTO standards rather than to undermine them.

Finally, the EU's current proposal would not even help European cloud firms become globally successful. On the contrary, European cloud firms would have stronger incentives to stay out of the US and many other markets – or to have only a minimal presence, such as having a US subsidiary that cannot directly access data in the EU. If those firms expanded overseas, or properly integrated their US and European operations, they could become subject to the CLOUD Act, lose their European security certification, and find it harder to compete in Europe. The cloud computing market is dominated by a small handful of companies (often referred to as 'hyperscalers') because securing the greatest possible economies of scale is critical to being competitive. Forcing European firms to choose between their opportunities in Europe and their opportunities overseas is therefore defeatist. The EU would be left with an inefficient industry, in turn making it harder for European businesses to make effective use of cloud services to digitise. Competition authorities across Europe are already closely scrutinising the cloud market. If there are problems with the market which mean European competitors are not getting a fair chance to succeed, then this is best addressed through sensible pro-competitive interventions rather than by excluding foreign firms.

However this particular transatlantic tussle ends, it is unlikely to be the last. EU member-states remain concerned about the EU economy's reliance on US networks, technology companies, and financial and payment systems, and worry that Europe will face collateral damage if these systems are ever withdrawn or if Washington forces them to operate in ways harmful to Europe's interests. While EU-US dialogue on tech has improved in recent years, the EU remains concerned that US unilateralism did not end with President Trump. The US's sudden decision to impose wide-ranging sanctions against

China's tech industry came as a surprise to Europe. The US took no account of the measures' impacts on European businesses. And America's Inflation Reduction Act was a recent reminder that even Democratic presidents will not necessarily take Europeans' concerns into account.

Washington can help by deepening its dialogue with Brussels, to help assure the EU that it will take its interests into account and that there will be no more unwelcome surprises. But Europe's best leverage against US unilateralism is to help its own tech firms go global, so that European reliance on American technology will no longer be so one-sided. Stifling competition and limiting European firms' choices will do little to achieve that.

Zach Meyers is a senior research fellow at the Centre for European Reform.