Toward Digital Solidarity

Tom Uren ⋮ 25-31 minutes

The coronavirus crisis laid bare governments' dependence on actors beyond their control for vaccines, medical equipment, microchips, and other essential goods. Russia's invasion of Ukraine exacerbated these concerns due to Europe's heavy reliance on Russian energy. In turn, the pandemic and Russia's war have helped accelerate many countries' growing embrace of a form of technological self-sufficiency known as digital sovereignty. Rather than shifting to closed technological ecosystems, policymakers have the opportunity to move toward what could be called digital solidarity, a new policy framework for enhancing economic progress, national security, and other societal interests among open, democratic, and rule-bound societies.

The concept of digital sovereignty started to take root in the 2000s and spread quickly in digital policymaking and business circles over the next several years. Though it is more a malleable political slogan than a policy strategy, digital sovereignty's meaning can be derived from the concerns expressed by its proponents. They assert the belief that digital technology shapes in fundamental ways an ever-increasing number of significant political, economic, military, and societal trends and outcomes. Therefore, they argue, controlling such technology is critical to defending and promoting the national interest.

Digital sovereignty has been a rallying cry for and driver of various industrial policy initiatives and technology regulations in the European Union, India, Australia, Canada, and other democratic societies. The Chinese and Russian governments have also used digital sovereignty and similar terms like cyber sovereignty, in their case to argue for and establish barriers between their domestic digital environments and the outside world and to promote abroad internet governance models designed to create closed and restricted ecosystems.

In contrast, digital solidarity is an alternative path to achieving technological self-determination through partnerships and alliances among open, democratic, and rule-bound societies. The goal of digital solidarity is to enable technological cooperation and interaction that advance collective national interests. Its implementation also ensures competition among technology providers to help safeguard any participating country from being locked into a dependent technology relationship with any other nation. Though some European countries have nominally supported this alternative path in public statements, recent events in France and elsewhere in the EU suggest that the direction of travel of many democratic societies' technological self-determination may veer to a more closed and ultimately unsuccessful ecosystem.

Cloud computing is where a shift away from digital sovereignty and toward digital solidarity presents some of the most compelling opportunities for cooperation and innovation among open and democratic societies. The cloud is an abstract term, but at its core it is an on-demand network of supercomputers that an organization or an individual can rent to store and analyze vast quantities of data, build advanced digital tools, and use online services managed by third parties. The cloud's scalable, flexible, on-demand, and ubiquitous nature makes it fundamental to advancing critical technologies like artificial intelligence, quantum computing, and 5G networks.

Industry, government, and individuals worldwide are moving their activities to the cloud at a pace that has quickened during the coronavirus years. On the supply side, few companies provide advanced cloud services on a global scale. The U.S.-headquartered companies Amazon Web Services, Microsoft, and Google offer a full suite of cloud services from infrastructure as a service (IaaS)—storage, processing, networking, and other basic computing resources—up to software as a service (SaaS)—webmail, word processing, videoconferencing, and other digital services. China also has large-scale cloud providers, including AliCloud (a.k.a. AliYun), Huawei Cloud, Tencent Cloud, and Baidu Cloud. Europe itself has home-grown cloud providers, but they are significantly smaller in scale and scope than their American and Chinese competitors: Deutsche Telekom, OVHcloud, SAP, and Orange, primarily.

In the cloud, digital sovereignty involves both the data that travels through the cloud and the hardware and software that make up the cloud's infrastructure—large data centers distributed globally and the cables that connect them to each other and to other resources. Here, policymakers aim to address three core components of cloud digital sovereignty: control over data, whether very sensitive data such as a government's top-secret information or broader categories of data that can be useful for machine learning, for example; control and choice over the hardware and other physical infrastructure in which data is stored and processed; and control and choice over the software on which workloads—such as a mobile app—are run.

A New Push for Digital Sovereignty

The French government has been one of the most active advocates of and actors in establishing cloud digital sovereignty in Europe. Its policy initiatives in this space are critical to understanding how digital sovereignty may evolve in Europe and other regions, given that Europe's technology policy has significant influence worldwide. Importantly, while digital sovereignty aligns with autocratic states' overall policy objectives, the French example raises the question of whether and how democratic and open societies should adopt digital policies that potentially balkanize the internet and encourage other nations to do the same.

France has promoted cloud digital sovereignty initiatives since the early 2010s. Its cloud sovereignty efforts intensified in 2018 after the United States passed the Clarifying Lawful Overseas Use of Data Act (Cloud Act), setting the stage for policy changes during the coronavirus crisis. Some observers characterized the legislation as an effective and privacy-sensitive mechanism for open, democratic, and rule-bound foreign governments to seek data from U.S. tech companies directly rather than via the U.S. government under mutual legal assistance treaties. However, critics—many still deeply concerned about the Snowden revelations in 2013—focused on the provisions in the Cloud Act that gave U.S. law enforcement explicit authority to compel U.S. technology companies to disclose the contents of electronic communications stored in the companies' data centers overseas.

Though U.S. government officials and others argued that this authority existed before the Cloud Act, government officials and private-sector actors in Europe and elsewhere claimed that the act provided a new authority that threatened the privacy of individuals and organizations outside of the U.S., and ultimately Europeans' control over their data. Some French policymakers strongly suggested that

the only way to make Europeans' data "Cloud Act-proof" is to avoid using U.S. software and infrastructure to store and process European data, even if the infrastructure were physically located in Europe. These views were sharpened by the Court of Justice of the European Union's (CJEU's) ruling in *Schrems* II, which essentially held that U.S. surveillance and procedural laws and rules do not adequately protect Europeans' data privacy and led to arguments that simply storing and processing data on U.S. cloud providers' infrastructure violated the EU's General Data Protection Regulation.

Other concerns that drive cloud digital sovereignty efforts include the perceived detrimental impact of foreign cloud providers on France's and Europe's economic development and growth, and the broader strategic consequences of becoming overly reliant on American and Chinese cloud technology. Moreover, in some cases, this overreliance is concentrated in the hands of a small number of corporations—a worry that has only grown during the coronavirus years. One hypothetical discussed often among policymakers is the possibility of European entities—for example, European commercial banks—getting cut off from American cloud services due to U.S.-imposed sanctions relating to unfavored nations. The severing of Russia from various digital services and networks like the SWIFT system in the wake of Russia's invasion of Ukraine has provided real-world examples of the consequences of disconnection, and the EU itself reportedly is now considering its own ban on providing cloud services to Russia.

France's cloud sovereignty efforts—led by Finance and Economic Minister Bruno Le Maire, Digital Minister Cédric O, and Minister of Transformation and Public Service Amélie de Montchalin—were driven by many of these concerns and, at times, contemplated policy proposals that veered toward a closed French cloud ecosystem. France's path, for now, has also been influenced by its government's analysis and ultimate conclusion that France and Europe more broadly have an interest in partnering with rather than excluding American cloud providers, given the perceived significant advantages of U.S. technology—including in the security space—and the broad adoption in Europe of American cloud services.

The National(ist) Cloud Strategy

The French government took two significant policy actions. First, Le Maire (now France's economics, finance, and industrial and digital sovereignty minister), O (now retired from government), and Montchalin (who lost her parliamentary seat in June to a member of the Socialist Party) unveiled in May 2021 a new three-part National Cloud Strategy. The strategy consists of a "Cloud de Confiance" or "Trusted Cloud" label, a "Cloud at the Center" policy that establishes a cloud-first approach for digital government projects (essentially privileging cloud computing for new information technology projects), and the launch of an industrial strategy to support financially European cloud providers with the ultimate goal of strengthening European sovereignty. The Trusted Cloud label initiative is particularly important to the transatlantic relationship because of its operational impact on American cloud providers, data transfers between the U.S. and France, and future Europe-wide cloud policies that might draw from and build on France's new initiative.

A cloud service provider is potentially eligible for the Trusted Cloud label if it meets three conditions. Notably, the provider must meet the security requirements of SecNumCloud, a stringent and evolving cloud cybersecurity certificate issued by the French National Cybersecurity Agency (known by its French acronym, ANSSI) developed to ensure the cybersecurity of organizations in critical industries like energy, transportation, and health care that are known in France as "Operators of Vital Importance" or OVIs. ANSSI's standards focus on the physical security of data centers, requirements for personnel working in SecNumCloud-certified data centers, access controls, encryption practices, and other security-focused technical and operational requirements.

Second, a cloud provider must have its servers physically in France, which was a new requirement above and beyond those of SecNumCloud and, overall, a new development in France's approach to foreign cloud providers.

Third, any company that uses and sells cloud services to the French public sector and OVIs must be European and owned by Europeans. In essence, this requirement ensures the establishment of a business relationship between any non-European cloud provider wishing to serve the French public sector and OVIs and a French corporate partner, loosely similar to Chinese regulations that require foreign cloud providers wishing to operate in China to form a joint venture with local Chinese companies.

The French government presented these security, location, and nationality requirements as key to ensuring independence from U.S. extraterritorial laws, including the Cloud Act. Given the breadth and ambiguity of some aspects of the requirements, their details have changed and will likely continue to evolve—depending in part on how these requirements are operationalized and how they work in application.

The second outcome of the French government's National Cloud Strategy was the identification during 2021 of commercial transactions and corporate structures that meet, at least in principle, the criteria of the Trusted Cloud label. Specifically, the French government approved two U.S.-French cloud partnerships that could potentially serve as models for future cooperation but might also become cautionary tales for policymakers interested in greater collaboration and economic interchange among democratic nations.

An agreement among Microsoft, Orange, and Capgemini was the first effort at a U.S.-France cloud partnership in line with the Trusted Cloud label. The companies announced their intention to meet the technical and operational security requirements of SecNumCloud. Second, the companies stated that the venture will rely on data centers located in France, "strictly separated from Microsoft's global data center infrastructure," to guarantee operational autonomy, according to the companies' announcement. Third, the companies stated that they will form a new company, Bleu, jointly owned by Capgemini and Orange—both French digital companies. Bleu, in turn, will license Microsoft cloud technology and be operated by employees in France. Whether the data centers will be owned by Microsoft or another entity, whether Microsoft will be permitted to take a minority stake in Bleu, and other details about the transaction are not yet known to the public.

Google followed suit later in 2021 with its own approach to the Trusted Cloud. In Google's case, the French partner is French multinational Thales Group, which operates in the aerospace, defense, transportation, and security markets. As with Bleu, Google and Thales state that they will comply with SecNumCloud. Also, the data centers will be operated in France, with a separate network and servers controlled and operated by the newly formed company. Like the Bleu transaction, the Google-Thales deal calls for creating and operating a French company majority-owned by Thales. The Thales-formed company will manage encryption keys, access, identities, and cyber threat monitoring, positioning Thales as the trust and security partner in the venture while Google provides the hardware and software infrastructure.

The Span Between Open and Closed

However, over time, the French government has been criticized by French industry players that expected a much more restrictive implementation of cloud digital sovereignty. President Emmanuel Macron's rivals across the political spectrum have also expressed concerns about the government's National Cloud Strategy as not strong enough in excluding foreign players, showing an alignment across a significant swath of the French political spectrum in favor of digital sovereignty.

In defense of its Trusted Cloud label, the French government tightened ANSSI's SecNumCloud requirements in two significant ways. First, ANSSI now requires that cloud providers store and process customer and technical data in the EU, which could detrimentally impact product offerings and potentially jeopardize the security of customers' cloud environments. Second, despite ANSSI's technical focus, SecNumCloud now contains corporate governance requirements including a provision that specifies that non-EU shareholders cannot own more than 39 percent of a company providing cloud services in France. The government has also highlighted more investment in the industrial policy leg of its National Cloud Strategy to further address criticism that it was not doing enough for French companies.

And, in the wake of Russia's invasion of Ukraine, France has ramped up its efforts to promote digital sovereignty as part of a broader push for European sovereignty. For example, in March, France spearheaded the Versailles Declaration, which stated the European Council's commitment to investing in digital technologies, including cloud computing, as part of a European sovereignty agenda. On a parallel track, it has also worked to embed its SecNumCloud digital sovereignty requirements in a Europe-wide cybersecurity certification scheme being developed by ENISA, the EU's cybersecurity agency.

These trends, coupled with the lack of specificity in some aspects of the Trusted Cloud label, suggest fluidity in France's and the EU's relationship with U.S. and other non-European cloud providers. Consequently, it is important to articulate policy recommendations for European technological self-determination that steers away from the versions embraced and promoted by China and Russia and toward strong ties to open, democratic, and rule-bound societies around the world. Indeed, France and Europe have the opportunity to lead the community of open, democratic states in a broader movement toward digital solidarity and away from more restrictive notions of digital sovereignty.

Maintaining policy equilibrium in this space will be challenging. Among other things, moving away from solidarity and too far into a closed, autarkic system would have detrimental economic consequences. Already, the corporate partnerships, local infrastructure development, and technical changes required to receive the Trusted Cloud label add operating and capital expenses to the financial statements of cloud providers and their French partners. Though the French partners may ultimately profit from the additional revenue generated from these joint ventures, it is less clear whether potential increased costs will benefit the growth and success of SaaS and other companies that build their businesses on Trusted Clouds. These issues are coming into even sharper focus at a time when countries around the world, including many in the EU, are facing significant inflationary pressures and broader economic stagnation.

President Macron and other European leaders will need to be mindful of these concerns and cognizant that many companies build successful and innovative businesses on third-party cloud infrastructure because such infrastructure permits faster growth and innovation at a lower cost. To quantify the point, accounting firm KPMG estimates that the total European cloud market will be worth 560 billion euros by 2030. Roughly half of that value is projected to be in SaaS. Those SaaS companies are just as likely—if not more likely—to be based in France, Germany, or elsewhere in Europe than outside of Europe, given current incorporation, financing, valuation, and business success trends, and will be capturing that economic value even if they are built on Google, Microsoft, or Amazon Web Services infrastructure.

A corollary proposition is that successful companies built on third-party clouds often go on to build and control their own data centers and other technical infrastructure (Google, Meta, and TikTok are three examples). But without the U.S. company infrastructure, the European SaaS companies face higher barriers to building and scaling digital products and services. Too much movement toward a closed system could slow down and reduce the number of Europe's future tech success stories.

At the same time, a policy of digital solidarity in the cloud space must acknowledge that Europe has a strong interest in ensuring the integrity, security, and effectiveness of its government functions and nongovernmental critical infrastructure. The U.S. itself has many security requirements for cloud services that support government operations and military, space, and dual-use products and services. For example, the U.S. Department of Defense and the U.S. General Services Administration sometimes have stringent security and operational requirements for sensitive workloads like data location restrictions, which are similar to France's Trusted Cloud rules. In addition, the U.S. government continues to wrestle with proposals to restrict data flows to China in the interest of protecting national security. In a system of digital solidarity, these types of policies should be assessed to determine whether they are necessary and proportionate to the accomplishment of critical government objectives, while maintaining connections to and openness with other democratic, open societies.

A Policy of Digital Solidarity

Several specific policy paths can be pursued to accomplish digital solidarity. First, the U.S. government and the European Union should build on their recently announced Trans-Atlantic Data Privacy Framework (designed to address the CJEU's *Schrems* II ruling to permit data flows between the EU and the U.S.) by negotiating a U.S.-EU executive agreement under the Cloud Act as the U.S. has done with the United Kingdom and, more recently, Australia (a U.S.-Canada agreement is expected soon as well). Reasonable negotiated restrictions on the data access practices of U.S. law enforcement could go a long way to creating trust in American cloud providers and enhancing digital solidarity between the United States and Europe. Importantly, given the role of member states in law enforcement investigations and intelligence collection, a U.S.-EU agreement would need to bring the activities of France and other EU member states within its scope.

Among other things, a U.S.-EU deal should address legitimate concerns about the extraterritorial reach of U.S. law enforcement efforts. For example, a U.S. law enforcement agency should not need to turn to a U.S. cloud provider for the data of a large and well-known corporate customer or the data of a European government agency. The U.S. Department of Justice's stated policy is to turn to cloud customers first rather than to cloud providers when seeking customers' data. In addition, large European entities are increasingly holding

their own encryption keys for data stored and processed in U.S. clouds, thus reducing the ability of cloud providers to respond to government data requests.

Second, the U.S. government should acknowledge Europeans' desire to promote their economic growth and development through digital transformation and help make a case for why such economic development is better and achieved more quickly in partnership with American technology companies. American economic security is at stake here, too, as participating in the European economy is critical to U.S. cloud providers' financial performance, research and development, employment of engineers and other personnel (largely in the U.S.), and contribution to the U.S. tax base. There is also a tremendous strategic and financial potential for a strong economic engagement track between the U.S. and Europe in the cloud. Among other things, the U.S. and Europe together present a formidable alternative to Huawei, for example, with cloud-based 5G telecommunications networks developed jointly between U.S. and European companies.

Third, European and American policymakers should engage candidly to address concerns about the U.S. government cutting European customers off of U.S. cloud services. Relatedly, concerns about overdependence on a handful of cloud providers, especially when they are largely headquartered in the U.S. or China, should be addressed. One way to respond to both issues is to align around cloud customer data portability and cloud interoperability initiatives (including the growing common use of open source software) to ensure that no country engaged in digital sovereignty partnerships can be locked into a relationship with a single country or, for that matter, a single vendor. Efforts on cloud portability and interoperability are already underway in forums like SWIPO (Switching Cloud Providers and Porting Data), a multi-stakeholder group facilitated by the European Commission, and in the EU's draft Data Act.

Fourth, U.S. and European policymakers should push toward harmonizing cloud rules with a focus on policies that are proportionate and necessary to critical issues like national security, economic security, and privacy protection. In the French case, the Trusted Cloud label requires servers to be in France. In a digital solidarity environment, the requirement would be generalized to any EU member state and broadened to apply to any country participating in the digital solidarity network because each of those countries would have agreed to security, privacy, portability, and other relevant standards. Similarly, France's SecNumCloud should evolve to a harmonized European standard managed by ENISA that is consistent with the standards of digital solidarity partners to ensure that cloud providers, regardless of where they operate, uphold strong security practices.

Finally, the U.S., the EU, and EU member states should institutionalize cloud collaboration and partnership in an ongoing program of digital solidarity. Given the profound importance of cloud computing on both sides of the Atlantic and the opportunity to create a broader cloud network of open, democratic, and rule-bound societies, the U.S. and the EU should consider a Transatlantic Cloud Partnership that promotes bilateral cloud cooperation and partnerships.

In doing so, the U.S. and the EU should build and elaborate on the recently launched Declaration for the Future of the Internet, which brings together 61 countries, including several members of the EU, in support of critical principles such as the idea that technical infrastructure should be designed to be secure, interoperable, reliable, and sustainable. Ongoing European efforts like Gaia-X (a project launched in 2019 and focused on the development of a federated data and infrastructure in Europe to promote digital sovereignty) and the European Alliance for Industrial Data, Edge and Cloud (a group focused on strengthening European cloud and edge technologies launched in 2020) should also inform such a partnership, which could quickly expand to other open, democratic, and rule-bound societies interested in the security and economic development benefits of joining the network.

Many European leaders are already embracing digital solidarity. For example, in a recent speech given at Science Po, Dutch Prime Minister Mark Rutte called for "open strategic autonomy," which would allow Europe to defend its way of life in a way that is "open with our democratic partners around the world." Policymakers in the U.S., Europe, and other open and democratic societies should work to capitalize on this sentiment and the current opportunity to establish long-term relationships, organizations, and rules to ensure digital solidarity among democracies.