Why US Clouds Are Creating Data Problems for Europeans

By David Roe | *Aug 24, 2020*

PHOTO: SHUTTERSTOCK

It will be months before the real impact of the recent decision by the EU to strike downthe US Privacy Shield is known but there are other clouds on the horizon that could upset the relationship between Europe and the US where technology is concerned.

Data Problems Ahead

In fact, the cloud could well be the next problem and it all comes down to data. It is no secret that Europe is sitting a on huge amount of personal data, which has long been considered the real wealth of any company that uses data, or the insights from data, to drive their business.

However, a recent paper under the auspices of the Germany-based National Academy of Science and Engineering (acatech), led by the former head of German software firm SAP, Henning Kagermann, argues that Europe is losing its influence in the digital economy because companies are rushing to store their data in clouds built and managed by U.S. technology companies. "The majority of European data is stocked outside of Europe, or, if stocked in Europe, is on servers that belong to non-European firms," the paper reads.

This is no vendor-driven research. Acatech, based in Berlin, has the ear of governments and was created to provide independent, science-based advice in the public interest and to outline the opportunities and risks of technological developments. Ultimately its goal is to pull science and technology, and industry together across Europe in order to give Europe a competitive edge. This 28-page paper will no doubt cause concern among US tech

companies that are providing storage services and digital workplace platforms to European organizations. It reads:

> *"From search engines and social networks to shopping platforms and cloud services, almost all the digital platforms used by citizens, the public authorities, institutions and businesses in Europe are provided by non-European private-sector companies. "*

It adds that, as a result, Europe has no influence over its governance. It argues that many established platforms "now act as de facto regulators, stipulating the rules governing interactions between their users. "In the main, this happens without democratic governance and with no reference to European values, thereby also calling into question the effectiveness of current (data protection) legislation."

It concludes by suggesting that Europe should "strengthen its digital sovereignty by building a sovereign European digital ecosystem that is democratically accountable to its citizens."

Data Sovereignty Concerns

The paper has already caused some concern across Europe, particularly in the powerhouse economies of Germany and France both of which have a trove of data thanks to their powerful industrial sector.

One French official, quoted by the French news agency AFP was even more pessimistic. "We have an enormous security and sovereignty issue with clouds. In many cases it is convenience or a sellout…because it is simple to sign up with US tech giants than find European options. However, we have very good firms offering cloud and data services."

While it is probably a coincidence, the paper was published at the end of July just after the announcement that the U.S. Privacy Shield was no longer valid and data privacy was high on the list of issues to be addressed by technology companies on both sides of the Atlantic, keeping in mind that many European companies have breached GDPR too.

However, it also needs to be kept in mind that many companies that have signed contracts with big cloud providers are guaranteed that their data will be stored in the nearest data facility to the address that is provided by the customer in the contract. While those contracts are confidential, Microsoft like Amazon and Google guarantee that all data is stored by

default in the country where the business operates, or, in the case where there is no center, the nearest center to the business.

Focus On Data

Doug Barbin, principal and cybersecurity leader of Tampa, Fla.-based Schellman & Company, a global independent security and privacy compliance assessor, points to the fact that with most data this is the case. “The reality is colocation and cloud computing companies — many US based — built data centers in countries like Germany due to data residency requirements and to service local customers,” he said. “Those customers also replicate their data to other cloud nodes due to even more critical availability requirements.”

He added that focusing on where the data resides or the domicile of the company managing the physical data center, reflects a less-than modern way of thinking about the problem. “The focus should be on the data. Through use of virtual private cloud technology and customer-controlled encryption keys, cloud tenants can create an environment where the underlying provider(s) have no access to the data,” he said.

Monitoring Data

It is true that data is becoming an invaluable commodity, and it is also true that US businesses dominate the cloud storage landscape. However, the rules introduced by GDPR and CCPA help to protect European citizens' data, in particular the ability to see what these companies hold on you. More importantly, you have the legal right to get this data corrected or deleted, Chase Higbee, lead IT Strategist for Orlando-based Atlantic.Net, which provides a web hosting solution, said. “There is much more global scrutiny of how U.S. tech firms handle and process personal information since the Cambridge Analytica scandal, and users are much more aware of how their data is collected. U.S. Congress have also shown concern recently regarding growing power of tech companies,” he said.

It should be kept in mind too, he said, that hybrid cloud technology is also booming, allowing companies to keep sensitive data locally, often in their own data centers while at the same time offloading regular workloads to U.S. cloud companies. This is a practice regularly seen in financial and government agencies.

Digging for Profit in Data

Ultimately, the bad news from a users’ perspective is that business' search for profit is an unrelenting force of nature, Kon Leong, CEO and co-founder of Malipitas, Calif.-based data management company, ZL Technologies, told us.

Consequently, the mining of the digital gold will always tend to happen regardless of which flag is flying over the mining equipment. The good news is that government always has the prerogative to trump any move by business, as demonstrated by the recent US move on

TikTok. “However, the baddest news is that government holds all the digital cards and the assumption that it will always exercise responsible self-governance has been disproven time and again by history,” he said.