The US-EU Rivalry for Data Protection: Energy Sector Implications

Arnault Barichella

19 February 2019

The US-EU Rivalry for Data Protection

Energy Sector Implications

Arnault BARICHELLA

Arnault Barichella *is a PhD candidate at Sciences Po Paris and a Visiting Fellow at Harvard University, affiliated with the Department of Government. His research focuses on a comparative analysis of climate and energy policies in Europe and the United States.*

ISBN: 978-2-36567-991-6

How to quote this publication:

Arnault Barichella, "The US-EU Rivalry for Data Protection: Energy Sector Implications", *Édito Énergie*, Ifri, 19 February 2019.

Ifri
27 rue de la Procession
75740 Paris Cedex 15
Tel.: (0)1 40 61 60 00
Email: accueil@ifri.org

Website:
www.ifri.org

The General Data Protection Regulation and the energy sector

The energy sector is undergoing a 'digital revolution', whereby information and communication technologies (ICTs) are increasingly deployed throughout energy infrastructure, leading to the growing digitization of production, storage and consumption processes. With potentially hundreds of millions of smart meters to be installed in the European Union (EU) and the United States (US) in the coming years, ICTs make it possible to collect and analyze large amounts of complex data to optimize the whole energy system, while providing consumers with a number of customized services.[1] Firms in the energy sector are gradually turning into massive data collectors. As a result, the energy industry is one of the sectors that has been most impacted by the requirements outlined in the EU's new *General Data Protection Regulation* (GDPR), launched in May 2018.[2] The GDPR contains a number of strict and far-reaching requirements for firms that process EU citizens' data. The regulation is explicit that these cover not only EU-based firms, but any company anywhere in the world that processes the data of EU citizens or residents. As a result, the extra-territorial reach of the GDPR is considerable.[3] Since the EU is the first trading partner of the US, many American firms will have to abide by the new rules set out in the GDPR.

There have been a variety of conflicting accounts about the potential economic impact of the GDPR on both sides of the Atlantic. Certain reports claim that the GDPR could end up costing large firms more than $1 billion overall. This is in part due to high EU penalties for non-compliance (up to 4% of global revenues), which may negatively impact competitiveness and transatlantic trading.[4] Other studies, however, have asserted the exact opposite, namely that the GDPR contains a

number of provisions requiring firms to update and modernize their modes of operation, making them more efficient and competitive. In addition, the GDPR also creates a common set of rules for data protection, which will bring clarity and legal certainty to firms on both sides of the Atlantic, potentially boosting transatlantic trade.[5] Finally, firms that do not comply with the GDPR now risk being at a competitive disadvantage compared to companies that offer stronger data protection.[6] Overall though, the benefits from the GDPR in terms of privacy protection are unequivocally positive.[7]

Conflicts with the US *Cloud Act*

On March 23rd 2018, and perhaps in anticipation of the GDPR, the US Congress ratified the *Clarifying Lawful Overseas Use of Data Act* (or *Cloud Act*) as part of the 2018 federal omnibus spending bill.[8] Many of the potential benefits deriving from the GDPR, both from an economic viewpoint and from the perspective of privacy protection, risk being jeopardized by the *Cloud Act* and the danger of conflicting legislation. In a nutshell, the *Cloud Act* represents an extension of the *Stored Communications Act* (SCA) of 1986, which covered the disclosure of electronic communications held by Internet service providers.[9] As a result, the *Cloud Act* makes it lawful for US federal authorities, within the context of an investigation, to compel American technology companies, either through warrant or subpoena, to hand over data stored on their servers and data centers. This applies regardless of whether or not such data is stored on US soil or in a foreign country; the person(s) concerned are not notified and there is no possibility of oversight from judicial authorities in the country where the data is stored.

Such provisions enter into direct conflict with several key sections of the GDPR, in particular Articles 44 to 48, which subject the international transfer of EU citizens' data to very strict conditions. Up until now, the international transfer of personal data has been regulated by 'mutual legal assistance treaties' (MLATs), bilateral arrangements that are often slow and cumbersome. One of the stated objectives of the *Cloud Act* is to circumvent this existing system in order to establish a more rapid and efficient one, whereby certain foreign governments may enter into 'bilateral executive agreements' with the US for direct and reciprocal data transfers. This runs counter to the GDPR's insistence that the MLAT system provides the most

adequate framework to protect the international transfer of EU citizens' data. Furthermore, although the *Cloud Act* contains a number of clauses that are supposed to provide safeguards to protect personal data, these have been widely criticized for being insufficient, especially when compared to the MLAT system.[10] This means that the *Cloud Act* risks nullifying many of the privacy protections contained in the MLATs and the GDPR.

The *Cloud Act* has a direct impact on the energy sector, because energy firms on both sides of the Atlantic have expanded their reliance on Cloud computing technologies to store the large quantity of data they are processing. It is becoming highly problematic for companies to store all the data being collected through new ICTs (such as smart meters) in their own data centers. Cloud computing technologies offer clear economic benefits; the global market for Cloud storage in the energy sector was estimated at $1.786 billion in 2017, and is predicted to grow at a compound annual growth rate of 25.68% over the next few years, reaching $7.037 billion by 2023.[11] European energy firms often rely on American Cloud providers to store their data, given that US companies are world leaders in this sector.[12] Even when they do not, any EU-based Cloud computing company that has a branch of activity in the US risks falling under the jurisdiction of the *Cloud Act*; given the extent of transatlantic trading, this includes the majority of European Cloud providers.

As a result, there is an imminent risk that the *Cloud Act* could bypass the GDPR and render millions of EU citizens' personal data vulnerable to interception and surveillance from US federal authorities in most sectors, including the energy sector. In addition to national security concerns, industrial espionage is likely to become more widespread with the adoption of the *Cloud Act*. Moreover, energy companies and many other sectors that engage in extensive transatlantic trading could become trapped in contradictory legal obligations between the *Cloud Act* and the GDPR. This potentially exposes them to simultaneous sanctions from both the EU and US federal authorities.

Although it is true that many European energy firms rely on US Cloud providers and have an American market presence, they only become vulnerable to Cloud warrants in the case of a judicial inquiry in the US, which is not a common occurrence. Therefore, most European energy companies are still more concerned about the issue of non-

compliance with the GDPR than with the *Cloud Act*, especially since their main base of operations is in the EU. Nevertheless, the fact remains that if a US judicial inquiry is forthcoming, there is currently no apparent way to avoid a conflict between the legal requirements of a Cloud warrant and the exigencies of the GDPR, which may expose firms to very high sanctions on both sides of the Atlantic.

Different responses to the *Cloud Act*

There is no easy solution for the EU to respond to the *Cloud Act* while safeguarding the GDPR. One possibility would be for EU authorities to try and negotiate a bilateral executive agreement with the US, as outlined by the *Cloud Act*. This might help to contain some of the damage to privacy rights by setting clear and reciprocal conditions for US access to EU citizens' data and vice versa, including in the energy sector. Nevertheless, it will likely be very challenging for the EU to negotiate such a bilateral executive agreement with the US without violating key provisions of the GDPR. Another solution could be for the EU and member states to rely exclusively on EU-based Cloud providers and achieve 'digital sovereignty'. In response to the *Cloud Act*, a number of European energy firms have tried to decrease their reliance on US Cloud providers by privileging 'local' Cloud solutions. Yet, the majority of European Cloud providers and energy firms have some form of commercial activities in the US, rendering them vulnerable to Cloud Warrants. Only a small number of European-based providers are totally insulated from the American market, and they would probably not be capable of storing on their own the large amounts of data processed through smart metering.

As a result, the EU should first respond by reinforcing the transatlantic Privacy Shield to ensure that the data of EU citizens transferred to US firms under this agreement is still protected after passage of the *Cloud Act*. The Privacy Shield Framework aims to replace the former Safe Harbor Agreement, which was struck down by the European Court of Justice in October 2015 for inadequate protection of privacy rights. The new Privacy Shield aims to provide stronger guarantees during transatlantic data exchanges for commercial purposes, including in the energy sector. Although experts agree that the Privacy Shield represents an improvement over its predecessor, advocacy groups still criticize it as insufficient, and it currently faces a number of legal challenges that are likely to increase

due to the *Cloud Act*. In particular, the *Cloud Act* calls into question the European Commission (EC)'s 'adequacy determination' of July 2016. The latter deemed that the Privacy Shield provided an equivalent level of data protection compared to EU law and was therefore adequate for the transfer of EU citizens' data to the US. Consequently, there is an urgent need for the EU to demand additional guarantees from US federal authorities to ensure that the adequacy determination remains viable.[13] Since President Trump has shown little interest in promoting greater privacy protection however, the *Cloud Act* could well mark the final demise of the Privacy Shield Framework, absent a clear shift in the policies of the current US administration.[14]

Against this background, it appears that the EU has responded with a *realpolitik* approach by developing what has been described as a '*European Cloud Act*'. In April 2018, less than one month after the *US Cloud Act* was ratified, the EC published a legislative proposal outlining new rules in the form of a Directive[15] and a Regulation,[16] dubbed the '*e-Evidence Initiative*'. Like the *Cloud Act*, the *e-Evidence Initiative* would provide law enforcement institutions with stronger tools to obtain data stored across national borders, within the context of an investigation. More significantly, it would provide EU authorities with greater powers to obtain data directly from providers, even if they are based outside the EU and irrespective of which entity has custody or possession of the data. Once again, this would directly impact firms in the energy sector, given their increasing reliance on Cloud computing technologies. While the *e-Evidence Initiative* still needs to be approved by EU legislators in the coming months, it has already sparked significant outcry from advocacy groups.

The fear is that the EU may be preparing to mimic the *Cloud Act* and the transatlantic rivalry on data protection could turn into a 'race to the bottom', with potentially dire consequences for privacy rights on both sides of the Atlantic. It is understandable that the EU is seeking to provide more effective tools for law enforcement agencies in the fight against organized crime and terrorism; likewise, it is important to demonstrate European resolve to the Trump administration. Nevertheless, this should not come at the expense of sacrificing data protection and core European values.

As the *e-Evidence Initiative* is debated and amended in the coming months, sufficient safeguards must be inserted to ensure adequate protection of privacy rights consistent with the GDPR. It should be noted that both the *Cloud Act* and the *e-Evidence Initiative* embody responses to the inefficiency of the existing MLAT system.[17] However, since the latter continues to offer the best safeguards in terms of privacy protection, the EU should seek to improve its legal framework, rather than attempt to bypass it. This means working more closely with partner countries to ensure that MLATs can offer a more rapid and effective structure for international data exchanges.

Overall, the GDPR, the *Cloud Act* and the *e-Evidence Initiative* all point to an escalation of the transatlantic rivalry for data protection, with major ramifications for the energy sector in the years to come.

1. G. Desarnaud, "Cyber Attacks and Energy Infrastructures: Anticipating Risks", *Études de l'Ifri*, Ifri, January 2017, available at: www.ifri.org.

2. For example, energy firms now collect, process and store data on how citizens consume energy, at what time and in what locations, as well as data relevant to billing.

3. T. Gomart, J. Nocetti, and C. Tonon, "Europe: Subject or Object in the Geopolitics of Data?", *Études de l'Ifri*, Ifri, July 2018, available at: www.ifri.org.

4. PricewaterhouseCoopers, "Pulse Survey: US Companies Ramping Up General Data Protection Regulation (GDPR) Budgets", 2017, available at: www.pwc.com.

5. EU Commission, "Stronger Rules on Data Protection Mean People Have More Control over their Personal Data and Businesses Benefit from a Level Playing Field", 2018. For more details, see: https://ec.europa.eu.

6. *RSA Data Privacy & Security Report*, 2018, available at: www.rsa.com.

7. For more details, see: https://eugdpr.org.

8. The manner in which the *Cloud Act* was ratified, tacked on to the end of the 2018 omnibus spending bill without any congressional debate or oversight, has been widely criticized as representing a dishonest attempt to force the law through as a 'legislative rider'.

9. The origins of the *Cloud Act* are linked to the difficulties of the Federal Bureau of Investigation in obtaining data stored abroad by US firms via SCA warrants. This was highlighted in 2013 when Microsoft refused to hand over data stored in Ireland during a drug trafficking investigation, on the grounds that the SCA did not cover data stored overseas. See: *United States vs. Microsoft Corporation* (No. 17-2); the case was declared moot after passage of the *Cloud Act*.

10. Although bilateral executive agreements require the US Secretary of State and the Attorney General to certify that the foreign government provides certain protections in terms of civil liberties, they do not necessitate congressional approval, in contrast to MLATs. Moreover, the *Cloud Act* does allow firms, within a two-week period, to oppose any request for data before a US judge on the grounds that the person targeted is not a US citizen or resident, and that such a request could contravene the laws of the foreign country. However, these are arguably inadequate safeguards since they would rely in many cases on the goodwill of US Cloud providers, whose concern for the protection of EU citizens' data is questionable.

11. *Cloud Storage Market for Energy and Power Industry – Forecasts from 2018 to 2023*, Knowledge Sourcing Intelligence LLP, 2018.

12. This includes large US-based multinational firms such as Microsoft, Amazon, IBM, Salesforce, Oracle, Google, ServiceNow, Workday and VMware, among others.

13. The EC has recently issued a deadline to US authorities to appoint a permanent Ombudsperson for managing EU citizens' complaints by the end of February 2019 at the latest. While this is a step in the right direction, with the US finally agreeing to do so in late January 2019, it remains insufficient following passage of the *Cloud Act*.

14. So far, the Privacy Shield Framework has been very successful from an economic perspective. In a little over two years, more than 4,000 companies have already certified under the Framework. Therefore, the demise of the Privacy Shield is likely to damage transatlantic trade.

15. The proposed Directive would require providers of online services, including Cloud computing technologies, to designate and maintain a permanent legal representative in the EU, who would be charged with processing and complying with orders from EU or member state authorities on preserving or producing electronic evidence used in the context of investigations.

16. The proposed Regulation aims to create two new legal tools: a 'European Production Order' and a 'European Preservation Order'. The objective is to allow EU and member state authorities to compel certain providers of online services, including Cloud computing technologies, to produce or to preserve stored electronic data on a cross-border basis.

17. Under the MLAT system, it can take up to 10 months for authorities to gain access to requested data from a service provider. By contrast, a European Production Order as outlined in the e-Evidence Initiative would compel the release of such data within 10 days, and 6 hours in cases of emergency.