Cloud services made in Europe after Snowden and Schrems

Irion, K.

Publication date
2015
Document Version
Final published version

Cloud services made in Europe after Snowden and Schrems

Kristina Irion, *Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands*

PUBLISHED ON: *23 Oct 2015*

The geolocation of server farms - where data is stored and computing is performed – has evolved into an important attribute of cloud computing. By now, clients and providers are increasingly conscious of the actual whereabouts of cloud services. As a standalone fact this sounds counter-intuitive since cloud technology is location-independent and distance should not matter anymore. However, outside of technology there are factual and legal issues which have come to force data localisation requirements into cloud computing contracts and offerings.

DATA LOCALISATION ON THE RISE

As a result of increased localisation guarantees Europe emerges as a distinct region for cloud computing. First, the demand for enterprise cloud services made in Europe triggered significant investments in local cloud infrastructure by global internet companies and native operators. Large organisational clients that can negotiate cloud service contracts increasingly insist on data localisation guarantees (Irion, 2012). But also consumer-facing cloud services relocate substantial portions of their operations to Europe. In May of this year, Dropbox and Twitter announced that they would move all operations to Ireland, with the exception of their North-American accounts.

These shifts take place mainly at the expense of US-based cloud services, arguably as a direct fallout from the Snowden revelations that have been eroding the confidence of clients and users.

Data localisation is thus the manifestation of a geopolitical rift , in particular transatlantic, over jurisdiction and protection of cloud-sourced data. Irreconcilable conflicts of laws presently persist in relation to statutory privacy protections and due process requirements in the event of disclosure authorities (Severson, 2015). It also exhibits a shortcoming in contract law which so far has proven rather capable to span jurisdictions and to address differences in the legal protections afforded to information and personal data in particular (Bygrave, 2015: 86). Data localisation is a fairly basic but effective means to influence jurisdiction, thereby reducing legal risks for providers and clients and arbitrate the lack of confidence. The cloud consequently gravitates toward the law of territory.

EU consumers using cloud services may not be fully aware of the potential risks for their personal data in a global cloud environment. Moreover, bargaining for data locations is not in the power of individuals who are most likely confined to standard terms of service which are unilaterally stipulated by the service provider (Irion, 2015: 11). Individuals' personal data is, however, protected subject-matter under EU data protection law. The regulation protects

personal data of EU citizens as users of cloud services and, when it is in the custody of a client of cloud services; And it establishes requirements for the lawful transfer of personal data to third countries.

EU LAW AND POLICY APPLICABLE TO CLOUD COMPUTING

For two decades the European Commission and the competent national data protection authorities have been pragmatic about international transfers of personal data. For example, the standard contractual clauses, the EU-US Safe Harbour framework and the binding corporate rules give evidence of the administrative practice to facilitate personal data flows instead of obstructing them. Whereas in a data–driven economy any restrictions on personal data flows are readily criticised, the revelations on the mass surveillance programmes have fundamentally uprooted the bureaucratic *laissez-faire*.

In its 2014 resolution on *Supporting consumer rights in the digital single market* the European Parliament recalls "that cloud computing entails risks for users, in particular as regards sensitive data". The Parliament called on the Commission to take the lead in promoting international standards and specifications for cloud computing. The European Commission now tackles cloud computing primarily as an internal market issue with the intention to turn the EU's high standards of data protection and security into a virtue for Europe. Europe could become

the world's leading trusted cloud region, although neither the resolution nor the European Commission's Cloud Computing Strategy require the localisation of cloud services or proposes to set-up a dedicated "European Super-Cloud".

JURISPRUDENCE RELATED TO CLOUD COMPUTING

The major impulses for a change to the status quo are to be attributed to the entry into force of the EU Charter of Fundamental Rights in 2009 and the judiciary. The 2014 judgement of the Court of Justice of the European Union (CJEU) that invalidated the EU Data Retention Directive delivered a first hint about its view on international transfers of personal data. The judges required that the personal data from retention measures are to remain within the EU in order to ensure control and independent supervision. Earlier this month, the Court expanded its view of international transfers of personal data in the Schrems judgment which invalidated the legal basis for the EU-US Safe Harbour. The judges objected to the European Commission's Safe Harbour decision on the formal ground that the European Commission did not assess the US legal system in its entirety.

With Safe Harbour gone, in order for transatlantic transfers of personal data to continue, it would require another legal basis in EU law. Certain cloud providers who anticipated this already came up with new contractual arrangements. Even though the alternatives

- e.g., standard contractual clauses and binding corporate rules - remain formally effective, they are equally unfit to protect EU citizens' personal data against unfettered US surveillance and disclosure authorities.

While pundits warn against the balkanization of the Internet this momentary rift over transatlantic flows of personal data may actually turn out to be the most forceful argument for improving the system of human rights protection in relation to the internet and online services. After all, cause and effect should not be confused. In the EU, data localisation is the effect of the asymmetric protection of privacy and personal data on both sides of the Atlantic. The loss of confidence in cross-border cloud services has already developed its own dynamic with clients being increasingly risk-averse, even before the Court struck down the Safe Harbour framework. The economic pressure on US stakeholders is real and they have been vocal about their quest to make the US government change policy.

References

Bygrave, L. A. (2015). *Internet Governance by Contract*. Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780199687343.001.0001

Irion, K. (2012). Government Cloud Computing and National Data Sovereignty. *Policy & Internet*, *4*(3), 40–71.

Irion, K. (2015). Your digital home is no longer your castle : how cloud computing transforms the (legal) relationship between individuals and their personal records. *International Journal of Law and Information Technology*. doi:10.1093/ijlit/eav015

Severson, D. (2015). American Surveillance of Non-U . S . Persons : Why New Privacy Protections Offer Only Cosmetic Change. *Harvard International Law Journal*, *56*(2), 465–514. Retrieved from http://www.harvardilj.org/wp-content/uploads/562Severson.pdf