Publication: Financial Times (EUROPE); Date: Jul 29, 2013; Section: World News; Page: 2

Snowden saga reveals gaps in protection of European data

Cyber security

Fears have grown that data stored on the cloud are highly vulnerable to foreign surveillance, writes Chris Bryant

Cloud computing has been hailed as a revolution that would reduce the need for capital investment and provide near unlimited computer power and storage on demand. But in recent weeks fears have grown that European data stored on the cloud could be vulnerable to foreign surveillance.

Revelations by Edward Snowden, the US contractor turned whistleblower, have underscored the shortcomings of Europe's data protection laws in the age of the cloud, where data are stored at external data warehouses rather than on a local hard drive. As data flows across national borders at lightning speed, often existing simultaneously on servers in multiple countries, protecting and regulating transfers of data has become more complex.

Such is the concern for the security of data on the cloud after the Snowden revelations that last week Germany's data protection authorities called for the suspension of the Safe Harbour agreement, which allows cloud providers to make data transfers from the EU.

Politicians are in the process of reforming the bloc's data protection rules but some analysts fear planned changes could create more problems for international cloud companies.

Under US foreign intelligence laws, including the Patriot and Foreign Intelligence Surveillance Amendments Acts, US authorities can oblige US cloud companies to hand over data on people who are not US citizens. EU data rules offer little protection against foreign intelligence agencies, leaving not only EU citizens but also US cloud providers in an unenviable position.

"If I am a German provider and the [US] National Security Agency comes to me [to ask for data], then I can say: 'I'm not allowed to and have no interest in doing so'," said Klaus Landefeld, board member for infrastructure and networks at Eco, the Association of the German Internet industry. "But if I'm a US provider in Germany then I have the problem that under Fisa [the US act] I'm bound to comply."

The vast majority of cloud companies are based in the US. But even cloud providers with headquarters in Europe could in theory be compelled by the US authorities to hand over European data if they have a subsidiary or office in the US. That is because US law applies to all companies that conduct "continuous and systematic business in the United States".

> 'Our holding company is Swiss and has no concept of extraterritorial jurisdiction'

CloudSigma, a cloud operator based in Switzerland, said it had structured its global cloud locations so they were operated by separate entities, meaning there could be no legal basis for the US to make a data request.

"Our holding company is Swiss and has no concept of extraterritorial jurisdiction. The US authorities can try that kind of stuff but it's possible to hold firm and explain your position," said Robert Jenkins, its chief executive.

In practice, US authorities would be "reluctant to put pressure on [European cloud companies]... for fear they will report them to their home governments", said Ian Brown, associate director of Oxford university's cyber security centre. Surveillance programmes such as Prism and the obtaining of 500m pieces of metadata a month by the US from Germany, as reported in Der Spiegel, are by their nature secret and US law forbids companies from revealing the existence of a Fisa order.

In practice, it is impossible for EU data protection authorities to know if secret surveillance is happening or not, Caspar Bowden, an independent privacy advocate and former chief privacy adviser at Microsoft, warned in a report to the European Parliament last year.

European politicians hope a revision of the EU data protection directive, initiated last year, will help solve the problem. A controversial amendment called Article 42 – dubbed by campaigners the "anti-Fisa clause" – would prohibit third-country access to EU personal data without express permission of an EU supervisory authority.

The new EU data protection regulation is supposed "to make crystal clear that even companies based in the US but offering services to EU citizens must obey EU law," said Mr Brown.

However, some academics warn tougher EU data protection rules could create a Catch-22 scenario for international cloud companies.

"US intelligence requests will keep on coming and... cloud providers will be either in breach of US or EU law," Axel Arnbak, at the institute for information law, University of Amsterdam, and co-authors wrote in a recent study, "Obscured by Clouds".

There are doubts whether EU data protection laws will bring the required level of transparency. Mr Bowden says Article 42 "could be a tactical error, because given there is no sufficient deterrent and minimal risk of detection, data protection law would continue to be flouted in secret".

Some EU politicians say the solution is for Europe to promote completely autonomous cloud services to protect its citizens' data. Until that happens, the security of its data is set to remain "obscured by clouds".