By Nikolaj Nielsen

An obscure section in a US law is said to entitle authorities to access, without a warrant, data stored by any EU citizen on clouds run by American companies.

Although highly controversial for its indirect effects on Americans, the impact of the law appears to have been overlooked by its intended target - everyone else.

Rather than case-by-case snooping, the law authorises mass-surveillance of non-Americans, for purely political purposes, said Caspar Bowden who is the former chief privacy adviser to Microsoft, at a panel on cyber security organised by the CPDP conference in Brussels on Friday (25 January).

"It intentionally targets only non-US persons located outside the US and provides for a blanket authorisation to this for one year at a time. There is no individual warrantry," said Bowden, who is now an independent advocate for information rights.

The section in the so-called Foreign Intelligence Amendments Act (FISAAA) grants the US government sweeping powers to collect foreign intelligence information stored in US Cloud computing providers like Amazon or Google.

The article specifically states the US Attorney General and the Director of National Intelligence may authorise jointly, for a period of up to one year from the effective date of the authorisation, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

The amendment cites a number of limitations but Bowden, who also co-authored the 'Fighting cyber crime and protecting privacy in the cloud' report for the European Parliament, said FISAAA essentially makes it lawful for the US to conduct purely political surveillance on

foreigners' data accessible in US Cloud providers.

"It doesn't have to be a political party, it can be an activist group or anybody engaged in political activity or even just data from a foreign territory that relates to the conduct of foreign affairs in the United States," he said.

The EU's current data reform package is apparently unable to respond to the wording outlined in the US act.

Bowden says "binding corporate rules for data processors" was inserted into the European Commission's data protection regulation proposal with loopholes built-in which allow for FISAAA surveillance.

The binding corporate rules require cloud providers to hire a private-sector audit company to certify the generic cloud system for security.

But private audit companies, says Bowden, are unable to discover secret wire-tappings ordered by the national security law of another country.

The act may have wide implications on the right to respect for private and family life, reinforced by EU law in the charter for fundamental rights inscribed in the Lisbon Treaty.

'Anger and disbelief'

"When my attention were first drawn to the previsions of FISAAA, I went through a strange sequence of emotional reactions. From sort of laughter, through disbelief, to anger to denial," said another panellist, Gordon Nardell, a London-based barrister specialising in data protection and data retention in the telecoms sector.

The European Commission, for its part, was unable to provide a comment on FISAAA.

"This [FISAAA] is not something we have any comment about," said the spokeswoman for the European Commissioner of Justice Viviane Reding in an email.

But the issue is not unknown within the EU institutions.

"If it is a US company it's the FBI's jurisdiction and if you are not a US citizen then they come and look at whatever you have if it is stored on a US company server," stated Estonian president Toomas Hendrik Ilves, who also chairs a commission advisory group on cloud computing, at a separate panel discussion on cyber security held on Wednesday.

A high-ranking EU source told this website that the commission is actively looking into the amendment. The source drew some caution on the wide-spread snooping powers put forward by FISAAA but noted that "it is not outside the realm of possibility."

The Brussels-based European Data Protection Supervisor also refrained from any official comment though an inside contact said they are too investigating.

Meanwhile, a spokesperson for the United States Department of Justice told this website that the US is committed to privacy rights. "The FISA Amendments Act is not used indiscriminately or for political purposes," said the spokesperson, noting that a special court is used for judicial oversight on the requests.

But the section in FISAAA that is generating controversy is filed under 1881a.

The section expanded in 2008 on a 27-year old definition on "remote computing services" to include any providers of public cloud computing.

The amendment specifically targets data of non-Americans located outside the US and removes previous constraints which hindered continuous data collection and mass-surveillance.

FISAAA also notes that investigations should be conducted in a manner consistent with the US Fourth Amendment which guards against unreasonable searches and seizures.

But a US judiciary subcommittee on FISAAA in 2008 stated that the Fourth Amendment has no relevance to non-US persons.

FISAAA also forces US Internet giants and other tech companies operating clouds in the EU to hand over the data or face sanctions, says Bowden.

"The providers have to give all assistance, facilities, information to accompany this in total secrecy. If that secrecy is breached, it's a contempt of court and probably a breach of the US espionage act as well," noted Bowden.

Original article on the EUobserver.com webpage .