BIIA NEWS
Market Intelligence - Industry Developments & Trends - Information Technology - Regulatory Issues - User Community

Do not look to Europe to protect our data!

It is wrong to assume the US is the worst regarding surveillance, says Christopher Wolf in the Financial Times on July 15th 2013

Is **personal data better shielded in Europe** from the prying eyes of national security investigations than in the US? That is a general assumption of some following the revelations by former US intelligence contractor Edward Snowden. But it may be incorrect.

It is naive to think that European intelligence agencies do not use data collected from phone and internet companies in their investigations. Privacy hawks may also be surprised to learn that the US imposes at least as much due process and oversight on foreign intelligence surveillance as others. Currently, there is quarrelling over how well the judicial and legislative approval process is working in America. But the fact that it exists at all is the critical point because few countries provide the kind of framework of judicial authorisation and legislative oversight of national security investigations found in the US.

In **France**, for example, no court is involved in interceptions under the law governing access to information on national security grounds, and the interceptions are kept secret. Requests for interception are presented to the prime minister's office, which grants authorisation. Afterwards, the authorisations are presented to a special security commission that can evaluate the justification for the warrant and inform the prime minister of any concerns.

The lack of court involvement in France is in contrast to the US Foreign Intelligence Surveillance Act. In France, "oversight" is undertaken by a committee that can only recommend modifications to the executive. In addition, the law is broader than Fisa in that it permits interceptions to protect "economic and scientific potential".

In **Germany**, the federal office of investigation has broad authority in investigations that concern national security or terrorism. For example, it is permitted to use a computer virus, the *Bundestrojaner* ("Federal Trojan"), to search IT systems, monitor communications and collect data without the knowledge of users or service providers. While a court order is needed to use the Trojan, service providers are not aware of its deployment. In the US, service providers are notified of acquisition orders, which they can contest.

In the UK, interception warrants relating to foreign intelligence are generally issued by the foreign secretary. Unlike in the US, the courts play no role in the authorisation or review of these interceptions.

There is an Investigatory Powers Tribunal, a judicial body independent of government, that hears complaints under the surveillance law. But the absence of after-the-fact notification to those placed under surveillance means that many who might have cause to bring claims to the tribunal will not in practice do so.

European scepticism about the privacy protections in Fisa is understandable. A casual reader of the US law might conclude – mistakenly – that foreign intelligence measures targeting non-Americans are indiscriminate and conducted without court supervision. In reality, the government must certify before the relevant court that the surveillance is to obtain "foreign intelligence information", a term closely tied to the hostile acts and official activities of foreign countries and terrorist organisations.

It is also worth noting that, in the EU, there is an obligation for telecoms and internet companies to retain personal information, potentially for up to two years. The EU data protection supervisor has called this rule the most privacy-invasive instrument ever adopted by the union. That data retention directive, combined with the lack of transparency and formal checks on national security access to personal data in many European countries, should give advocates pause when they single out the US for its national security activities.

There are no guarantees, in the US or anywhere else, that authorities are abiding by the laws restricting access to personal data in the name of national security. But the degree of authorisation required and the kind of review that occurs is relevant indeed to a determination of how well personal privacy and liberty are protected.

Viewed that way, the US fares better than many others. European critics of US privacy protections would be well advised to take stock of their own countries' national security access to personal data.

The writer is head of global privacy and information management at law firm Hogan Lovells and is co-author of a study of national security access to data in the cloud

Source: ***Financial Times***