SECURITY EUROPE™

Security through knowledge.

Euro-View: Martina Francesca Ferracane on data localisation

How data localisation wipes out the security of your data

The Snowden revelations gave a pretty heavy boost to supporters of data localisation, which often argue that such measures would make the data more secure. Yet, while the rank of countries advocating the need to locate the internet data of their citizens within their own jurisdiction keeps expanding, it remains unclear whether such measures would actually increase the security of the data.

In fact, the evidence suggests that data localisation rather reduces the security of data which are arbitrarily retained within a certain country. As experts have argued, data security is not a function of where the data is physically stored.

Let's look at what the scholars say, and start from the basics. There is not yet a clear definition of data localisation. These measures refer to government-imposed restrictions that result in the localisation of data within a certain jurisdiction. These requirements can be extremely diverse – from outright bans on the transfer of data abroad to a requirement to retain only a copy of certain data within the country – and they can target different sectors and types of data. But what they all have in common is that they create virtual borders within the internet by creating restrictions to the movement of data across borders.

According to an analysis conducted at the European Centre for International Political Economy (ECIPE), there are today more than 80 measures implemented in the 65 countries studied. Most of these were implemented after the year 2000.

This 'data nationalism' has often been justified by governments via the argument that the localisation of data makes the information more secure. However, these measures only rarely contribute in a positive way to the objectives they are intended to support. Moreover, they clearly impose economic costs on the implementing economy, primarily through a loss of productivity and competitiveness.

Anupam Chander and Uyen P. Le, both professors of law at the University of California, carried out a comprehensive analysis on how data localisation does not decrease the data's vulnerability to foreign surveillance or cyber attacks.

First of all, they argue that many countries, including the United States, concentrate much of their surveillance efforts abroad, meaning that foreign surveillance would still be carried out from within the surveilled country.

Second, the use of malware eliminates the need for such operations on the ground in the countries targeted for surveillance. Through such malicious software security agencies are able to access the data stored in a given country from anywhere in the world.

Moreover, one should not underestimate the fact that localising data could even facilitate the work of foreign surveillance agencies by easing their logistical burden of identifying where certain data might be stored. Chander and Lê refer to this point as the "Jackpot" problem.

Finally, several countries have laws empowering their authorities to request access to all the data of corporations established under their jurisdiction. Again, it would not matter where the data is actually stored.

It is therefore clear that data is not immune from government surveillance simply because it is held in a specific country. To the contrary: such data would be more vulnerable to cyber attacks.

Data localisation requires foreign companies to either build their own data centres in that country or to switch to local suppliers of data storage and processing solutions. These alternatives are likely to be less secure because local companies usually have fewer means to apply state-of-the-art security solutions compared to those that operate on a global scale. And it is not always be easy to find top level computer security professionals who are able to deal with cyber security threats. This is what Chander and Lê refer to as the "Protected Local Provider" problem.

Another argument to consider it that, while foreign surveillance is definitely not welcome, citizens would still not be happy to learn that data localisation can lead to easier access to their data by their own government – a situation all the more galling in that the latter is often likely to share its citizens' data with its allies.

For example, as reported by Der Spiegel, Germany's foreign intelligence agency Bundesnachrichtendienst (BND) collaborates with the US National Security Agency, having passed some 500 million pieces of metadata in the month of December 2012 alone.

It is evident that governments should refrain from imposing any unnecessary costs on their citizens if they cannot provide clear evidence that data localisation increases the security of their data. Until then, such measures will remain an 'expensive fantasy', to quote Kenneth Rashbaum's blog article, that fall short of their objective, while imposing higher costs on goods and services – ultimately hampering a country's competitiveness and attractiveness for investment.

Martina Francesca Ferracane is a policy analyst at the European Centre for International Political Economy (ECIPE) in Brussels. She can be reached at martina.ferracane@ecipe.org

Published by:

SECEUR™

Brooks TIGNER, Chief Policy Analyst & Head of Technical Studies

Teri SCHULTZ, Policy Analyst

Chris DALBY, Policy Analyst

Robert DRAPER, Business Development Director

SECURITY EUROPE

goes out in headline form to approximately 13,000 public and private civil security stakeholders across Europe each month.

Contact us at:

SECURITY EUROPE
The Security Centre
235 rue de la Loi, box 27
1040 Brussels, Belgium
Tel: (+32) 2 230-11-62

general.enquiries@securityeurope.info **www.securityeurope.info**

Follow us on Twitter @SecurityEurope