

May 20, 2015 6:19 am

Complexity of data rules weaves a tangled global web

Murad Ahmed

[Share](#) [Author alerts](#) [Print](#) [Clip](#) [Comments](#)



Mario Costeja González has no particular axe to grind with Google. Indeed, he likes and uses the search engine. But the Spanish lawyer did object to how every aspect of a person’s life can for ever be dredged up by using it.

In 2010, he started a legal battle against the US internet giant after a search of his name brought up a 20-year-old article with details of the auction of a house he was forced to sell to settle his debts.

Data protection laws around the globe

Last May, Mr González won his landmark case at the European



Court of Justice in Luxembourg. The court enshrined a new “right to be forgotten online”, allowing the continent’s citizens to ask Google to request that sensitive information be removed from search queries.

The decision caught Google by surprise, though it has reluctantly accepted the judgment. The ruling has proved to be costly and cumbersome, with the company needing to create a large team to process thousands of requests from people asking for links related to them to be removed from its search engines.

The top daily pick of
FT business stories
for MBA students
and professors.

Sign up now

The incident is an example of the difficulties for companies, particularly large multinationals, that have to navigate complex data protection rules that vary widely around the world. It shows how even huge and powerful groups such as Google can be caught out by privacy measures that can have long-lasting implications for their operations.

Companies across all industries have built their businesses on the web precisely because it permits them to cross borders easily and allows them to reach an international audience. But as the internet has grown, different nations have developed varying rules and standards, as well as creating watchdogs devoted to regulating how bits of data are held and moved across cyberspace.

“It’s clear that data protection rules [worldwide] are fragmented,” says Chris Sherman, a security and risk analyst at Forrester Research. “It’s the cause of a lot of confusion for multinational organisations that want to transfer, store or process customer and other personally identifying information.”

Data regulation matters to consumers who are becoming increasingly aware that their personal information is not necessarily safe in the hands of organisations. One example of the response to problems around security is the introduction of “mandatory breach notifications”, where companies are forced to inform users if their personal data have been compromised following a cyber attack. Australia and the US are among countries that have adopted such rules.

Meanwhile, data protection regulations are crucial for companies. Unless they adhere to laws on how to store and transfer information about users, they could find national authorities blocking their operations. The difficulty for business is knowing how to navigate the complicated international framework on data protection. Argentina and Iceland have adopted some of the toughest data protection regulations in the world. Germany, a federal state, has a network of regional privacy watchdogs with real power — a response to the country’s unhappy history with secret police forces under both the Nazis and the Communists.

China, meanwhile, has almost no data protection laws for companies to contend with, but it has a mighty censorship regime that restricts what information can be seen by its citizens.

Analysts say that many countries have recently adopted even more stringent data protection regimes.

The catalyst for these moves has been revelations from American whistleblower Edward Snowden about the widespread intrusion by US and UK intelligence agencies, with claims that these nations' security services could readily access personal data stored by technology companies.

The Snowden disclosures have had a dramatic impact on companies wanting to use the services of big US-based technology businesses, particularly "cloud computing" companies, which offer to host the customer and commercial data of many organisations internationally.

According to a Forrester survey of more than 1,600 "technology and business decision makers" at companies in Asia, Canada, Europe and Latin America, about 26 per cent said they had halted or reduced spending with US tech companies for internet-based services following the Snowden leaks. Of those who had pulled back, nearly 34 per cent said it was due to "fear of intelligence community spying", while about 18 per cent blamed national rules forbidding the storage of certain information outside their home countries.

There is now 'global convergence around the EU standard'

[Tweet this quote](#)

The central issue is where data are physically held. Most information on the internet is stored by tech companies in huge warehouses filled with computer servers. Some countries are demanding these so-called data centres should be housed within their borders. Russia, for example, has already passed legislation designed to force businesses to keep all information about Russians inside the country, leading some entrepreneurs and engineers based within its borders to consider moving abroad. Brazil has also considered introducing similar legislation.

Suspicious of government snooping, companies are also demanding their information be stored in countries which are considered to have stricter data protection regimes.

For smaller enterprises, this is problematic. Jan Rezab, chief executive of Socialbakers, a Czech social media analytics company, says the requirement to hold customer details within the confines of different nations is a burden for start-ups. "I'm losing business because of that," he says. "It duplicates my costs which makes me uncompetitive."

However, privacy advocates argue that a company which maintains strong data protection policies and is able to show it can adhere to tough local laws could have a competitive edge.

"It's a very good way to create trust and to develop [a company's] markets," says Florence

Raynal, head of the department of European and international affairs at CNIL, France’s data protection authority.

“Privacy and the level of compliance is in fact now an element of competitiveness. Companies are now playing on that,” she says.

But bigger tech providers have been responding to the public and company concerns about data protection. In October last year, Amazon Web Services (AWS), the world’s largest cloud computing business, an offshoot of the internet retailer, said it was building its first data centres in Frankfurt.

At the time, Andy Jassy, senior vice-president of AWS, said that the decision was a response to the “cultural preferences” of companies in the region.

“We have thousands of German customers and a number of those customers have told us that they want to move their workload and data to AWS, but can’t do so until we have infrastructure here in Germany,” he said.

Mr Sherman at Forrester Research adds that all this activity shows how there is “global convergence around the EU standard”, with most multinational companies choosing to be compliant with whatever rules are set down in the continent.

Other countries may also see EU data protection rules as the way to go. South Africa and South Korea have already adopted the right to be forgotten.

RELATED TOPICS Data protection, Internet privacy, Ecommerce

 Share ▾

 Author alerts ▾

 Print

 Clip

 Comments



Technology tackles health hazards in sport



Can the 'connected' car save carriers?



Mobile World Congress: Top three innovations

VIDEOS