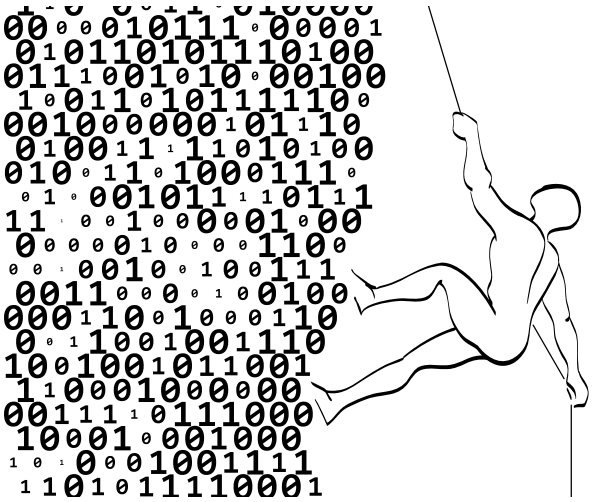
The Economist Intelligence Unit

MANAGING "MULTINATIONAL" INFORMATION

Cross-border businesses have a mountain of data rules and regulations to climb

Written by The Economist Intelligence Unit



At first glance Fjällräven is far removed from the information economy. The Swedish consumer goods company specialises in outdoor accessories for mountain trekking. Still, technology has played an important role in the company's development. The move from teleprinters to fax machines aided its early efforts at outsourcing production to South Korea in the 1960s—images of new designs could suddenly be sent overseas at the touch of a button instead of merely by text.

The efficiencies of outsourcing have not come without increased risks, however. "In the West it is obvious that you just don't copy products, but in China copying is viewed as a good solution," says Martin Axelhed, CEO at Fjällräven and deputy CEO at its parent company, Fenix Outdoor, which has operations in 20 countries around the world and had revenue of about Skr1,725m (US$265m)in 2012. Mr Axelhed's chief concern is brand perception. "In our world, it is a long-term problem if illegal copies carry our brand but don't meet the functional and material specifications," he says.

According to a recent global survey of senior executives, conducted by The Economist Intelligence Unit, outsourcing came high on the list of business and technology trends most likely to increase risks to company information; it came out top among respondents located in Europe, large businesses with annual turnover of more than US$1bn and—perhaps most revealing—those that had experienced information loss within the past two years.

OFFSHORE INFORMATION

The above model of traditional outsourcing—moving production to low-cost countries with weak intellectual property (IP) protection—is hardly new, of course. Companies in sectors such as fashion and luxury goods have for decades swapped greater risks to their designs for greater efficiencies in production. More recently, however, the explosion of "big data" and "the cloud" has brought the risks of outsourcing to the storage of data, albeit from a different angle. For information-intensive sectors, such as online commerce, the foremost information risks surround personal data, often in developed markets with mature regulations.

Cloud computing allows companies to outsource the storage of this data to external providers, reducing the need to maintain costly and inflexible data centres. In 2013 Gartner, a research firm, estimated the value of the global cloud services market at US$131bn, up from US$111bn a year earlier. US providers account for an 85% market share. This may dwindle as non-US companies discover that they may be subject to US regulations—and potentially surveillance—but it underlines the need for companies to be aware of the regulations governing where data is stored, not only where it is generated.

This is already proving to be a headache for businesses across the world. Over two-thirds (68%) of senior executives in our survey—and three-quarters (75%) of European respondents—agree that regional differences in the rules and regulations around data protection and privacy make the management of information risk more difficult. To complicate matters, the rules in the three largest jurisdictions by GDP—the US, China and the EU—are under review. In the EU, there is a single directive governing data across industries and member states, but it is uneven in implementation. In the US, there is a patchwork of legislation that is industry specific. China is busy trying to put a rulebook in place.

DEVELOPING RULES IN THE DEVELOPED WORLD

Two years ago a European Commission survey found that 70% of EU citizens are concerned about personal data misuse. This finding contributed to proposed reforms to the EU's existing 1995 data protection rules. On October 21st this year, a European Parliament committee voted to toughen up the Commission's proposal on data

protection. The committee wants stricter controls on how personal data is shared or transferred to non-EU countries.

A European data authority, say EU lawmakers, should regulate the cross-border flow of information. Companies should also explain to customers why they need personal data in the first place and seek consent before using it. For good measure, the committee recommended that the fine for non-compliance should be bumped up from 2% to 5% of worldwide annual company turnover (or at least €100m (US$134m) if the company's turnover is below €2bn).

"Companies subject to the new EU data protection rules will need to document practically every activity that involves personal data, including profiling of individuals and 'big data' analytics," says Wim Nauwelaerts, a partner at the law firm Hunton & Williams.

In the US, meanwhile, the Obama administration unveiled its "Privacy Bill of Rights" on February 23rd 2012. The proposal sets out a uniform improvement to consumer online protection by giving consumers the right to access and correct their personal data across industries. Some argue that this would undermine the advantages of sector-specific regulation. To date, little progress has been made in moving the proposal forward.

PAPER TIGERS LACK BITE

Similarly, China has been paying close attention to its data protection rules. Last year the Ministry of Industry and Information Technology (MIIT) published guidelines on the protection of personal data. Data collection by companies must be in line with their intended purpose, it suggested. The MIIT also published the "regulation of market order Internet information services". This administrative law subjects Internet service providers (ISPs) to personal data collection and use limitations, such as restrictions on sharing information to third parties without user consent.

"For the first time, they have elaborated on personal data principles and provided a definition, which is an important development," says Yun Zhao, a professor and director of the Centre for Chinese Law at the University of Hong Kong.

Writing or tweaking the rulebook is only one half of the exercise, however. The other half is how these rules are locally applied and enforced. For instance, many US companies have been at odds with Europe's more stringent privacy regulations. In April German regulators fined Google €145,000 over illegal collection of personal data during development of its Street View feature. In September French officials said that they would impose sanctions against Google after it missed a deadline to explain how it collects and uses personal data in France.

In China it pays to be aware of the different levels of regulations. In a strict sense, only the National People's Congress makes law, while the State Council can make regulations and the ministries make administrative rules—the weakest level. This can lead to a lack of enforcement. "You can put good principles on paper but if no one takes them seriously, that's an issue," notes Mr Zhao, who says the lack of awareness is likely to continue until the administrative rules are upgraded.

As China looks to catch up with international standards, Western companies targeting China's growing middle-class consumer should be wary of their new obligations: IP protection may not be enforced to the extent that satisfies companies like Fjällräven, but the rules around private data might well be.