

## Privacy: Laws play catch-up with online world

By David Gelles

High quality global journalism requires investment. Please share this article with others using the link below, do not cut & paste the article. See our Ts&Cs and Copyright Policy for more detail. Email [ftsales.support@ft.com](mailto:ftsales.support@ft.com) to buy additional rights. <http://www.ft.com/cms/s/0/5ed232ae-0150-11e1-ae24-00144feabdco.html#ixzz1d8bLRH00>

Hardly a week goes by without news of a big company suffering a breach of sensitive data or mishandling customer information.

Whether it is Sony's continuing efforts to protect the 80m accounts of its PlayStation Network users, or Citigroup coming under cyberattack, online privacy is an issue of central importance for businesses in every industry.

"There are those who know that they've been breached and those that don't," says Mark Lobel, principal in the advisory services division of PwC, the consultancy. "If you connect with the internet today, you're getting scammed."

Recognising as much, policymakers around the globe have begun introducing new privacy laws, and have become stricter about those already on the books.

The rules differ widely from country to country, with varying degrees of enforcement, making it difficult for businesses to organise compliance.

In the US, privacy regulations tend to be sectoral, focusing on specific industries. Instead of one broad law to protect consumer privacy, there are regulations that focus on health records, financial information, and credit and insurance.

Other countries, the UK, Germany and Canada, for instance, have stricter laws focused on protecting individuals. This year, India introduced a tough consumer data protection law.

This large and growing body of different national privacy regimes means that multinational businesses operating in many markets, face an increasingly difficult task in complying with them all.

"Businesses know they have to act," says Ann Cavoukian, Information and Privacy Commissioner of the province of Ontario, Canada.

And indeed, companies are beginning to become more proactive about compliance, aiming to put in place broad programmes that secure sensitive data across the enterprise.

"What we should be doing now is protecting privacy proactively," says Ms Cavoukian. "Embed privacy into the design of whatever you're doing. Make privacy, the default setting. Have it entrenched in your business practices, as a core functionality."

Rob Sadowski, director of technology strategy at RSA, the data security company owned by EMC says the attitude has shifted over time. "Early on, it was very difficult to get people to do anything.

“As organisations seek a competitive advantage, they look to these sources of data. To know [customer] preferences, to know their purchase history, can be used to advance their business, but that has to be done securely.”

RSA says there are three steps to securing data.

First is knowing what you have, or “data discovery”. This is the process of taking an inventory of what needs to be secured, and where it is.

“[Companies] need to find where all that personally identifiable information is,” Mr Sadowski says. “They can get an idea of how big the problem is.”

Once the extent of the data is known, it becomes simpler to protect them. “Once they find the material, they have to secure it,” says Mr Sadowski. That is the second step.

There are several ways to do this, from access controls that let only select administrators near private data, to encryption, which makes sensitive material unreadable, to “tokenisation”, a new process that scrambles symbols while leaving the data architecture intact.

The third step is to make sure that when regulators come calling, there is ample documentation of the security systems.

Known as “governance risk and compliance”, this is essential step companies who want to stay in the good graces of regulators.

“If an auditor or agency comes to you, you need to be able to prove to them that your data are secure,” Mr Sadowski says.

These steps are poised to become more complicated with the spread of cloud computing, whereby more and more company data are stored on external, third-party servers, distancing a company from its information.

“The consumer trusts the company, the company trusts the cloud vendor, the vendor trusts subcontractor,” says Mr Lobel. “The big concern for enterprises is their uncertainty [about how] to monitor it all.”

The US Federal Trade Commission, the consumer protection and regulatory body, is working on a comprehensive privacy bill, and has made recent strides with its “Do Not Track” rules to protect internet users. Other jurisdictions, meanwhile, continue refining their laws.

However, technology changes faster than law and as social media, mobile devices and cloud computing grow more popular, regulators may struggle to keep up.