Privacy regulation

78% – people feel concerned about data protection and privacy on the Internet

62% – agree that most businesses will take advantage of the public

Privacy regulation

The push towards global standards, protocols and greater transparency is a focus for many nations driving proactive regulation, but others choose to opt-out of international agreements and go their own way.

Technology has created a new type of geopolitical interaction. As data whizzes across borders, creating workable rules for business out of varying national standards is tricky. It's also important. Differences in privacy laws act as an unintended trade barrier and restrict innovation. There's a need to establish global standards that each country can sign up to and use as a basis going ahead. But the task is complex. Garnering local agreement in Europe has been difficult; America has a different approach; China and India, both of which have more people online than Europe and America have citizens, have another.

It's time that the regulation caught up with the technology. Existing data protection regulation emerged in the 1970s and 1980s in response to the developments of the time. The assumption was that data processing would always be a complex and labour-intensive activity and therefore would always be the preserve of large well-resourced organisations. The rules therefore were devised for static organisations and were designed to protect the individual who lacked any means to exercise control. Given that more than 500 million photos are uploaded and shared every day, along with over 200 hours of personal video every minute it is clear this assumption no longer holds true. On top of this the volume of information that people create themselves, including voice calls, pales in comparison with the amount of digital information generated about them each day. It is clear that the technical capabilities of big data, in its myriad forms, have reached a level of sophistication and pervasiveness that demands careful thinking on how best to balance the opportunities it affords with the social and ethical questions these technologies raise.

In addition to what happens within national boundaries many governments are also concerned about how their citizens' information makes its way in and out of other countries' jurisdictions. Catalysed by the Snowden revelations, some, including South Korea, Russia, Indonesia, Vietnam and Brazil, are now pushing forward new data localisation laws, which in theory ensure the privacy and security of citizens and enable domestic growth within the technology sector. However, given the decentralized structure of the Internet, these requirements alone will not prevent information from flowing across borders. Indeed, some authoritarian regimes seem to be using the policies for other goals, such as enhanced domestic surveillance or to reduce competition for domestic Internet companies. While data localization may succeed in boosting the economic success of local data centres, they could also have costly effects for other domestic businesses that rely on foreign Internet companies and cheap technology such as cloud computing. In the future a global agreement on standards seems a flexible solution.

A global agreement on standards seems a flexible solution.

Data revolution

There is a basis to work from. The United Nations Guiding Principles on Business and Human Rights states that every country has a duty to protect individuals from abuse by business and other third parties. In addition the UN General Assembly adopted a resolution 68/167 which expresses deep concern at the negative impact that surveillance and interception of communications may have on human rights and affirmed that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communication. So far so good but although it is not hard to agree with these principles their application is far more difficult.

Some suggest that the EU's consensual style of politics is poorly placed to deal with the problem - being too protectionist, focusing too much on controlling the data and not on managing the users. Others point out that this is because regulators are obliged to deal with legacy legal systems and governance structures bound by geographic borders at a time when the world has moved on. Certainly the current European model is designed to help existing market leaders adapt to change and collaborate with challengers. Brussels is taking a tough stance on privacy, increasing fines, placing requirements on organisations for obtaining consent and creating a "data protection by design" obligation. The US on the other hand is more open to creative disruption. China and India veer to the European approach. In a multicultural, multi-lingual environment there is a lot to be said for this as only the well-established companies can afford the time, money and resources to work with regulators to identify the challenges and opportunities ahead.

Brussels is taking a tough stance on privacy.

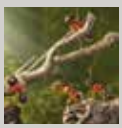
Despite some important differences, the privacy frameworks in the United States and those countries following the EU model are both based on the Fair Information Practice Principles. The European approach, based on a view that privacy is a fundamental human right, generally involves top-down regulation and the imposition of across-the-board rules restricting the use of data or requiring explicit consent for that use. The United States, in contrast, employs a sectorial approach that focuses on regulating specific risks of privacy harm in particular contexts, such as health care and credit. This places fewer broad rules on the use of data, allowing industry to be more innovative in its products and services, while also sometimes leaving unregulated potential uses of information that fall between sectors.

Going forward, the US is keen to encourage bilateral engagement with the European Union, Asia Pacific Economic Cooperation (APEC), and Organization for Economic Cooperation and Development, and with other stakeholders, to collectively take stock of how existing and proposed policy frameworks will address big data. It also aims to strengthen the U.S.-European Union Safe Harbor Framework, encourage more countries and companies to join the APEC Cross Border Privacy Rules system, and promote collaboration on data flows between the United States, Europe and Asia through efforts to align Europe's system of Binding Corporate Rules and the APEC CBR system.

The US is keen to encourage bilateral engagement.

Related insights

Deeper collaboration



Partnerships shift to become more dynamic, long-term, democratised, multi-party collaborations. Competitor alliances and wider public participation drive regulators to create new legal frameworks for open, empathetic collaboration.

Organisation 3.0

New forms of flatter, project-based, collaborative, virtual, informal organisations dominate - enabled by technology and a global mobile workforce. As such the nature of work and the role of the organisation blurs.

The changing nature of privacy

As privacy is a public issue, more international frameworks seek to govern the Internet, protect the vulnerable and secure personal data: The balance between protection, security, privacy and public good is increasingly political.

The increasing value of data

As organisations try to retain as much information about their customers as possible, data becomes a currency with a value and a price. It therefore requires a marketplace where anything that is information is represented.