BIZCOMMUNITY

What will shape data privacy in the future?

By Nigel Tozer

5 Feb 2019

2018 was a landmark year for regulators and businesses alike following the introduction of GDPR. There was a move from businesses to step up when it came to protecting personal data and respecting the individual's rights over their own information, or information about them. However, results of a recent poll, conducted by Commvault at the first Data Protection World Forum in London, suggest that there is still more to do.

Nigel Tozer

Eighty percent of IT and data experts polled at the event noted they were less than fully confident in their business' current level of compliance with data protection regulations like GDPR, yet 37% still thought more regulation was required.

This echoes a changing consumer view: that data privacy is an individual human right, and one not to be superseded by commercial interest.So what would more regulation look like? Here are three trends I predict will shape the future of data privacy:

- ## Consumer activism

  I am hopeful that consumer awareness and involvement will trigger a much greater conversation about what data privacy means, and how it is applied.

In addition, I hope to see consumers provided with more ways of tracking down where a company got their data from (similar to how services like Have I Been Pwned can show when your email has been compromised), as well as more transparent information around individual rights, and easier processes to opt out and withdraw consent across the board.

This will form part of an evolving conversation about trust between consumers and organisations – ranging from corporations through to charities. Data breaches, cold calling scandals, and data misuse court cases have all eroded the trust that individuals place in for-profit and non-profit entities.

I firmly believe that this damage can be repaired, but it will take work on the part of organisations to win trust through transparency, and a candid relationship with consumers over how data is, and indeed is not, being used.

Consumers also have the power to shape how regulators enforce sanctions for GDPR non-compliance. It would be impossible for organisations like the ICO to monitor the entire Internet for breaches in the policy, so it will fall to wronged citizens to flag up the issues that matter to them. While we're still waiting to see what sort of transgressions lead to what fines we should all exercise our rights, which will, in turn, exert pressure on the regulator to meet public demand.

- ## International co-ordination will remain patchy at best

Since the formal introduction of GDPR, we've already seen other regions move to instate their own legislation, including California, South America and Asia Pacific – although many of the proposed drafts and new regulations are less stringent than GDPR.

In an ideal world, our culture of international business would lead to an international standard for data privacy, although I suspect we will never see that, especially with some states actively monitoring their own populations.

Instead, on the global stage, we'll most likely see enforcement shaping how international companies go about approaching data privacy in their business practices. Some will work as best they can to apply the tightest standards on a global basis, providing that benefit to all. Others will risk-assess and act by region, while others will continue to pay lip-service to the regulation due to the limited number of cases where significant penalties were enforced.

That said, the €50m fine levied on Google may raise some eyebrows, though I believe that will not worry many businesses out there. As a percentage of its overall revenue, it's small beer for such a large company. Furthermore, as Google is such a giant in the public eye, it will be seen as an easy target, with many other large enterprises feeling safe due to their relative obscurity.

- ## Ethical questions around automation

Privacy difficulties around the automated processing of personal data from the likes of IoT, mobile and wearables,

when combined with machine learning and AI, are sometimes avoided by anonymising the data. However, I predict that we are still in the infancy of any ethics discussions around how anonymised, once personal, data is used and managed.

Firstly, even with anonymised data, businesses are still profiting from the use of a person's information, just without their name attached. We could see some consumers getting smart to how their information is being monetised – and want a piece of the action.

Tap My Data is a great example of this, and research published at the end of 2018 suggested that Facebook users would want to be paid more than $1000 to deactivate their accounts for a year. However, given the value that an individual's data provides to Facebook in the same period, I would love to see a world where services end up paying the individuals for the use of their data – with consent of course.

Secondly, there is an ethical dilemma around this anonymised data. Say, for example, that a wearable health device tracks information on heart activity – which is then analysed, anonymously, by healthcare researchers using AI. If one of these researchers finds a correlation between a certain reading and a healthcare risk, is there an ethical obligation to then inform users who exhibit this pattern? But of course, if the data is all anonymised, this should not be possible.

The UK Data Protection Act even expressly forbids efforts to de-anonymise data, with significant penalties including the threat of jail time. How these types of issues get handled will likely remain a topic of debate for years to come, as deep learning and AI generate more insight from increasingly sophisticated ways of collecting this sort of data.

So why should businesses take note now, before these changes even come into effect? In the poll I mentioned earlier, experts at all levels of confidence with their compliance reported that stronger regulation on data usage, protection and privacy can have a beneficial impact on businesses; overall 80% agreed with this view.

Taking a more stringent approach to data protection inevitably leads to better data management overall, which means that businesses can save money and use their data more efficiently to solve business challenges. At the same time, you can earn and build the trust of your customers.

It's a win for everyone, and I am truly looking forward to seeing what the future of data privacy will include – particularly as businesses make an active, long-term commitment to privacy and unltimately, trust.

ABOUT THE AUTHOR

Nigel Tozer is solutions marketing director for EMEA at Commvault.