Changing nature of privacy

40 billion – connected objects by 2020

86% – internet users have taken steps to remove or mask their digital footprints

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.

In 2016 the privacy conversation is still rather low key, a debate taking place in a closed community comprised primarily of academics, lawyers, regulators and security executives. This won't last. The privacy issue will transition from being considered a dry legal matter to one that is more widely understood and debated both commercially and by consumers. The new opportunities presented by big data, balanced with the increasing risk of data breaches, will ensure it climbs up the public agenda, becoming an important political issue along the way.

Currently the main international reference frameworks used for privacy and data protection are the OECD guidelines, the European Union Data Protection Directive and the Asia Pacific Economic Co-operation Privacy Framework. The approach to privacy differs with each organisation; some data protection regimes apply equally to those processing personal data; others apply different rules to specified industries such as the health sector, types of processing entity such as public authorities or categories of information such as data about children.

Up till now, personal data has driven the digital economy but the Internet of Things adds a rich new information source that can be collected, transmitted, and stored online at comparatively little cost. In order to maximise the opportunity this presents, technology companies will have to tread carefully around the privacy issue. Citizens will push back against the notion that their personal data can be used, seemingly without consent or direct benefit, for corporate profit, while governments, increasingly concerned about cyber terrorism, will demand more immediate access to personal data as a matter of national security. The challenge will be to satisfy both requirements, separating the practical from the ideological, while at the same time ensuring long-term profitability. Matters will become even more complicated when the networks are faced with the management of the expected torrent of new data from the myriad 'things' which will soon generate their own puffs of information.

Awareness both of the opportunities and risks this presents is growing as commercial organisations, governments and, increasingly, consumers, all vie to maintain control. Given the global nature of data some suggest the need for international regulation, an independent arbiter that can monitor activity and offer judicial support. But how can this be delivered?

One option put forward by Sir Tim Berners-Lee, the founder of the Internet, is the creation of a 'Magna Carta for the Web', to ensure the Internet remains open and neutral by enshrining key principles in a global constitution. He states there is a need to *"hardwire the rights to privacy, freedom of expression, affordable access and net neutrality into the rules of the game,"* and warns that if we are not careful, lack of awareness and general apathy might lead to a gradual erosion of the right to privacy by large organisations. Action should be taken to prevent this.

Technology companies will have to tread carefully around the privacy issue.

Data revolution

So something needs to be done but there is a lack of agreement about what this should realistically be; in 2015, the result of this impasse seems to be inactivity. Research by UNCTAD found that by 2013 only 107 countries had developed legislation to secure the protection of data and privacy, while another 33 draft bills were pending enactment. Many of those privacy laws have been developed on an ad hoc basis and are often bitty, disjointed and unable to keep up with the very technology they are designed to influence.

Meantime, technology is driving relentlessly onwards, and we are now witnessing the emergence of new business models designed to circumvent third parties and put the individual back in control of their personal data. Tech companies now provide consumers with increased encryption options thus absolving themselves, to some extent, of the responsibility of data protection. This has created problems for law enforcement agencies as end-to-end encryption makes it impossible for the companies that process or carry the data to unscramble it. Despite this, it is becoming the norm, e.g. IBM has licenced its server chip technology to Chinese manufacturers in a way that gives them control over encryption.

The implication is that huge swathes of the Internet can now "go dark". This presents a huge challenge for many of the established Internet business whose default model is based mining and repackaging data. Separating them from the sources of supply also challenges the assumption that the organization should be the natural and legitimate point of ownership and control of personal data.

Lack of understanding amongst politicians is delaying much needed privacy regulation that should protect both consumers and business. Perhaps particularly challenged as to how to respond are emerging markets, where the Internet take up was initially slow. Mobile technology has meant connectivity has risen exponentially and legislators are having difficulty in catching up. The UNCTAD report showed that out of 38 countries in Africa, Asia, Latin America and the Caribbean, 75% of government representatives have difficulties in understanding the legal issues related to privacy. This figure was reduced to 68% when understanding cyber crime.

Huge swathes of the Internet can now "go dark".

In addition, cultural differences about the interpretation of privacy also need to be addressed. There is no standard for anonymisation for example. The European ruling on the 'right to be forgotten' was described as "disappointing" in the US where the idea of deleting information from the Internet is interpreted by some as a threat to freedom of speech. That, in order to function effectively, personal data, codes and locations are shared across multiple jurisdictions by operators, manufacturers, developers and even the users themselves, complicates things. But differences are still more regional; even in the US every state has its own definition for what constitutes an adequate standard. If a global regulatory framework is possible it is likely that, although the principles will remain consistent, the implementation will be localised and diverse so the idea of privacy having borders will become a reality.

The establishment of clear principles is a good start but, such are the complexities that it is difficult for legislators to identify a specific body or organization that can take overall responsibility and in particular create standards around privacy that would be acceptable to all even at this stage of the game. In the next ten years it is hoped that harmonization will take place; the key question will be how this can be achieved, and which organization will take the crown and establish the global standards.

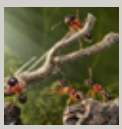
There is no standard for anonymisation.

Related insights

Data ownership

Individuals recognize the value of their digital shadows, privacy agents curate clients' data sets while personal data stores give us transparent control of our information: We retain more ownership of our data and opt to share it.

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.

Off grid

People living off-grid, by inequality or choice, can exacerbate societal division or improve privacy, health and wellbeing. Either way, doing so provides fertile ground for innovation.

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.