ECONOMIST IMPACT

Privacy in Asia-Pacific: Shifting perspectives and changing expectations

SUPPORTED BY Google

A rigid approach to data privacy cannot capture the full range of needs, perspectives and realities.

An evolving conversation

Data privacy may seem like a modern concept but has its roots in the 1890s, when the introduction of portable cameras and "snapshot" photos led to legal fights over the right to disseminate such images in newsprint. Ever since, society and regulators have grappled with ever-evolving privacy issues created by new technologies and data collection methods.

Today, those debates have become more salient in light of growing reliance on consumer data for everything from business strategy, innovation, and customer engagement, combined with the next wave of digital technologies which raise questions around data security.

In November 2021, regulators, academics and researchers in data privacy came together for a closed-door session with Economist Impact, that discussed the challenges data privacy presents for citizens, companies and countries in Asia-Pacific. This article reflects some key discussion points from the session.

What are privacy expectations today?

In 2020, model and writer Emily Ratajkowski penned a viral essay about her quest to reclaim control of her image,[1] and in doing so, opened up questions about the blurred lines of ownership in the internet age. What rights does the individual have to control how his or her data is used, even if "control" results in the decisions to publicly disseminate it?

During the roundtable discussion, participants suggested that privacy isn't an "on-or-off" issue, but one that lies on the spectrum of personal choice. In other words, the decisions we make about how our personal data is used are influenced by not just individual choices, but also cultural and societal norms, as well as technological changes.

Participants also said that consumer attitudes to data privacy will shift in response to changes in technology or external circumstances, like Covid-19. In Singapore[2] and South Korea[3], for example, local authorities relied heavily on contact tracing and exposure notifications.

1 https://www.thecut.com/article/emily-ratajkowski-owning-my-image-essay.html
2 https://www.lowyinstitute.org/the-interpreter/singapore-covid-vs-privacy-no-contest
3 https://www.voanews.com/a/east-asia-pacific_south-korea-balances-privacy-public-health-virus-fight/6188556.html

While citizens understood the importance of contact tracing in managing the pandemic, authorities needed to first ensure the tools and technology solutions were designed with user privacy and security in mind, and that citizens were well informed about how these tools worked.

Building trust through a privacy-first model

The concept of "privacy" may shift based on cultural and national values, but at its core lies the question of trust. Consumers have some level of understanding that their personal data is exposed—the problem is that that sense isn't corroborated with a solid understanding of *how* it's being used, and what their rights are in online spaces.[4] Public awareness of privacy-related laws is low in many Asian countries. For example, while 70% of Indians are aware of national or multinational privacy laws, the numbers are particularly low in China (33%), Australia (31%) and Japan (25%).[5]

This, combined with the swell in news of high-profile data breaches[6] and the difficulty in understanding privacy policies, makes it easy to see why consumers distrust companies with their personal data.[7] "There's a growing sense that those who hold power in our society need to be held accountable for violations of privacy and there's now an appetite for regulatory reform. There's been a huge loss of trust in large technology companies—and also governments—who have been too lax or too liberal in acquiring data and then using and misusing it," said Lizzie O'Shea, chair at Digital Rights Watch, Australia.

Mr Yeong Zee Kin, deputy privacy commissioner, Personal Data Protection Commission, Singapore, said: "Privacy is developing in Asia and we are in the midst of a transition. Data security and online scams are top of mind for consumers." He said trust-building needs to start by addressing issues such as securing personal data against breaches and the misuse of personal data to defraud. "Businesses who are custodians of consumer data need to be accountable. Consumers also need to be savvy and pick the right apps to use and services to use," he added.

Individuals derive a sense of trust in institutions based on how they perceive their privacy in online spaces, which in turn is connected to what efforts they see a company making to protect their data and educate them. Consumers are likely to be more confident in and trust companies that create safer products (or devices), and continue innovating to improve trust. When data creators are provided with privacy controls over their data, trust in that company is bound to grow. To an extent, it is because consumers feel safe in the knowledge that only data necessary to improve their user experience is being collected.[8]

Roundtable participants noted that just giving consumers control over their data isn't enough. More effort should be put towards educating users of their rights, and how these rights can be exercised. The need for organisations to move away from the idea that privacy is an "add-on" component, and towards a conceptualisation of privacy as a license to operate,[9] was also discussed.

4 https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/
5 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf
6 https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative
7 https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust
8 Ibid
9 https://advisory.kpmg.us/articles/2020/new-imperative-corporate-data-responsibility.html

There needs to be a collective shift in thinking of privacy as more than just a box-ticking exercise into something that is forward-facing and flexible, but also simple to understand.[10] The European Union's General Data Protection Regulation (GDPR) makes the right to be informed a core component of the law, and includes a requirement for companies to simplify their privacy policies.[11] However, the GDPR too, is evolving. "While we may think that the new GDPR is moving towards a single market and it's just one privacy regulation, it's not that simple," says Ms Rama Vedashree, chief executive officer of the Data Security Council of India. "The main challenges are the evolving regulatory landscape by sectors, the lack of harmonisation across geographies and the different expectations of civil society, users and companies of privacy."

Collaboration is key

There is no "one size fits all" approach that can provide long-term solutions, especially in light of the differences of opinion in what privacy means to each person.[12] A better approach to privacy would enable a shared narrative to act as a foundation that can be layered with a variety of perspectives from all stakeholders.

"Ultimately, just like what we saw in the EU with the GDPR, the race for industries to change becomes significantly quicker and the timeline of change shortens. That's something we foresee happening," said Mr Arshan Saha, chief executive officer of Xaxis and GroupM Specialty Businesses, Asia Pacific, Singapore.

With rapid changes in the privacy landscape, it has become increasingly difficult for governments to stay ahead of the curve. It is therefore critical that the technology industry and governments engage in a transparent manner and collaborate to ensure greater trust, particularly as data becomes more fundamental to business and personal user experience by the day. In this context, by educating consumers and businesses on the benefits of data protection and responsible data use, as well as sharing of expectations and best practices between governments, the technology sector and businesses can contribute to a privacy-preserving ecosystem that keeps in mind both businesses and consumers.

10 https://theconversation.com/heres-what-a-privacy-policy-thats-easy-to-understand-could-look-like-97251
11 https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed-1-0.pdf
12 https://journals.sagepub.com/doi/10.1177/2056305116688035