Issue Paper: Asia-Pacific Bureau

Online Privacy

May 2017

Building on the online privacy framework and concepts presented in the *Internet Society Policy Brief on Privacy*,[1] this issues paper focuses on online privacy concerns and good practices in the Asia-Pacific region. Please refer to the policy brief for an introduction to the topic.

The Issues

Online privacy is a serious concern across all social, economic and cultural contexts, according to various surveys and studies.[2]

In a survey commissioned by Big Brother Watch, over 80% of the respondents across Australia, India, Japan and the Republic of Korea are concerned about online privacy (Figure 1).

In another survey supported by the World Economic Forum, between 40% and 70% of the respondents from different countries (with an average of 58%), value online privacy irrespective of the level of Internet diffusion. In Asia, the survey was conducted in Australia, New Zealand, China and India (Figure 2).

1 Internet Society, "An Introduction to Privacy on the Internet: An Internet Society Public Policy Briefing," 30 October 2015, http://www.internetsociety.org/policybriefs/privacy. See also Privacy International, "What is Privacy," https://www.privacyinternational.org/node/54

2 Big Brother Watch, "New research: Global attitudes to privacy online," 24 June 2013, https://www.bigbrotherwatch.org.uk/2013/06/new-research-global-attitudes-to-privacy-online/ Privacy International, "Report - A New Dawn: Privacy in Asia," December 2012, https://www.privacyinternational.org/node/928 Soumitra Dutta, William H. Dutton and Ginette Law, "The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online," INSEAD Working Paper, April 2011, https://sites.insead.edu/facultyresearch/research/doc.cfm?did=48408

Figure 1. Level of concern about online privacy

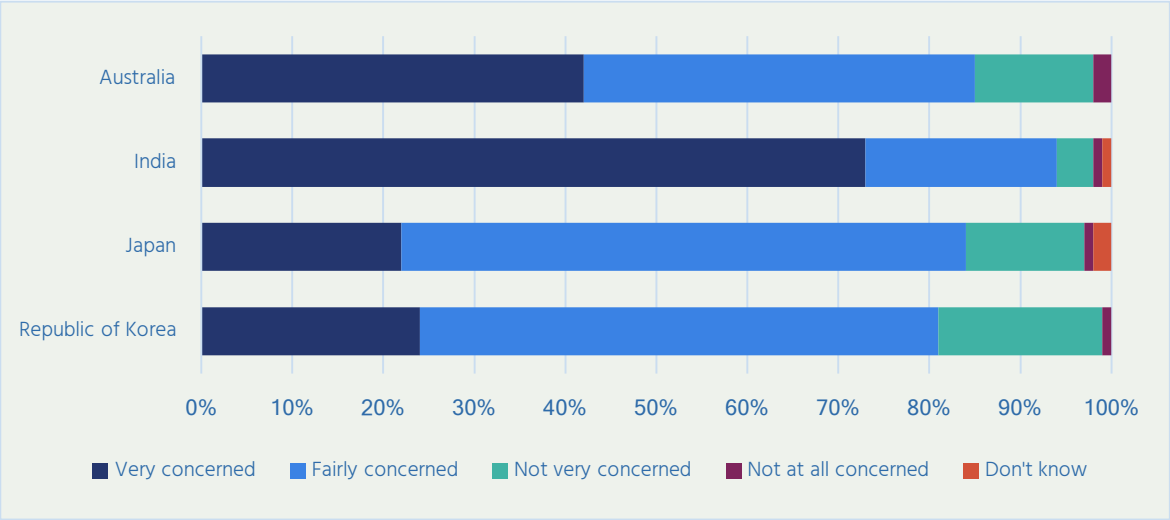
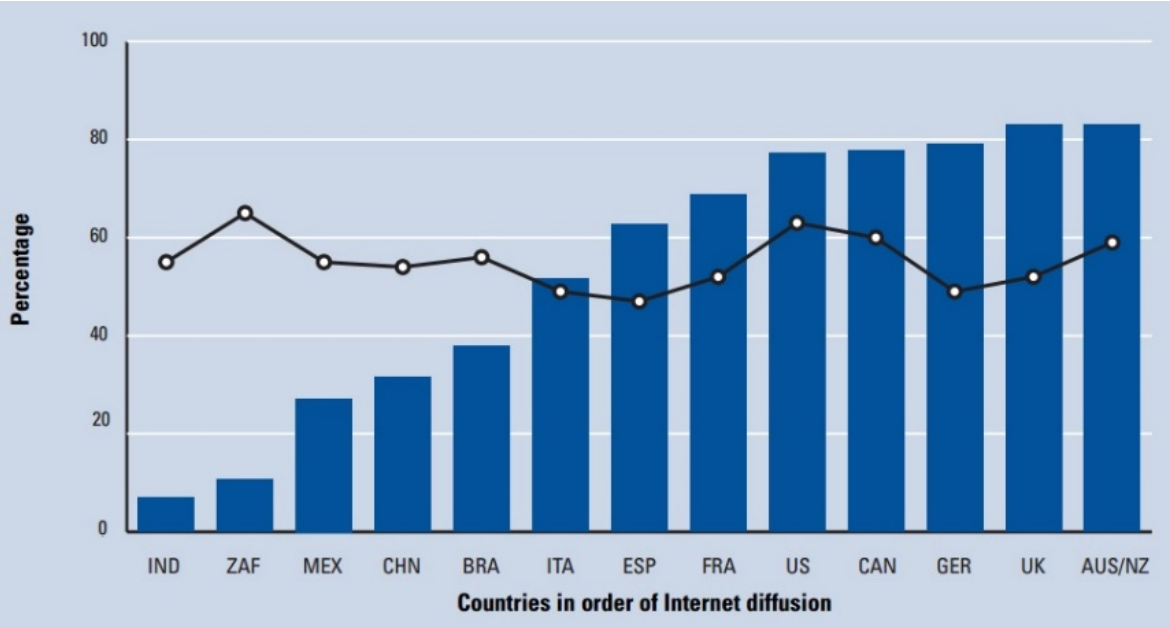


Figure 2. Support for online privacy according to Internet diffusion



In the latest annual survey of the Internet Society on policy issues in the Asia-Pacific,[3] cybersecurity and privacy replace e-commerce and cloud computing in the top five most monitored policy areas. The survey also reveals that 59% of the respondents believe that their privacy is not sufficiently protected when they use the Internet.

These surveys show that there is a global culture developing in which Internet users worldwide share similar attitudes and values related to online privacy. The survey supported by the World Economic Forum also finds that when it comes to core Internet values, users generally want it all. They desire an online environment where they can simultaneously express themselves freely, protect their personal data and privacy, trust the people and information they find, and feel secure.

3 Internet Society, "The Internet Society Survey on Policy Issues in Asia-Pacific 2016: Final Report," August 2016, http://www.internetsociety.org/doc/internet-society-survey-policy-issues-asia-pacific-2016

But, the right to online privacy is often sidelined by claims for security and surveillance, transparency and right to information, and socio-economic progress.

Security and surveillance

Many countries are using the need to increase public safety and security as a way to justify policies that authorize invisible automated surveillance and violate privacy rights.

Encryption is an important technical element of the solution to online security and privacy. But for the purpose of law enforcement and national security, some governments are controlling the use or effectiveness of encryption by gaining access to the means of decryption or decrypted information.

For example, China's Anti-Terrorism Law that came into effect on 1 January 2016 requires telecoms and Internet service providers to provide decryption and other technical support to authorities that are investigating terrorist activities.[4]

After terrorism-related incidents, India began implementing the Central Monitoring System to intercept and monitor phone and Internet services in real time.[5]

Transparency and right to information

As corruption is prevalent in many Asia-Pacific countries, it is a positive sign when governments promote transparency and openness. The governments of Indonesia and the Philippines are two of the eight founding members of the Open Government Partnership that aims to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance.[6] But unfortunately in this environment, efforts to focus on privacy are linked with secrecy and undermining transparency.

For instance, Indonesia's amendment to the 2008 Electronic Information and Transactions Law in October 2016, included a "right to be forgotten" clause (the first in Asia-Pacific). The law allows citizens to request a court order to have information that compromises their privacy or unjustly damages to their reputation removed from the Internet. But critics fear that the law could be misused by those in power as a censorship tool and to set back press freedom, which will affect the public's right to information.[7]

---

4 Glyn Moody, "China's new anti-terror law: No backdoors, but decryption on demand," *ArsTechnica*, 29 December 2015, https://arstechnica.com/tech-policy/2015/12/chinas-new-anti-terror-law-copies-uk-no-backdoors-but-decryption-on-demand/

5 Sneha Johari, "Govt's Central Monitoring System already live in Delhi & Mumbai," *Medianama*, 11 May 2016, http://www.medianama.com/2016/05/223-india-central-monitoring-system-live-in-delhi-mumbai/

6 Other participating governments from the Asia-Pacific region include Afghanistan, Australia, Azerbaijan, Mongolia, Republic of Korea, New Zealand, Pakistan, Papua New Guinea and Sri Lanka. See http://www.opengovpartnership.org/

7 Aulia Dwi Nastiti, "Who actually needs 'right to be forgotten'?" *The Jakarta Post*, 14 November 2016, http://www.thejakartapost.com/academia/2016/11/14/who-actually-needs-right-to-be-forgotten.html ; Krithika Varagur, "Indonesia Poised to Pass Asia's First 'Right to be Forgotten' Law," *VOA News*, 7 November 2016, http://www.voanews.com/a/indonesia-poised-to-pass-asia-first-right-to-be-forgotten-law/3584318.html ; Nadine Freischlad, "Controversial 'right to be forgotten' finds its way into Indonesian law," *TechInAsia*, 1 December 2016, https://www.techinasia.com/indonesia-recognizes-right-to-be-forgotten ; and Resty Woro Yuniar, "Indonesia's 'Right to be Forgotten' Raises Press Freedom Issues," *The Wall Street Journal*, 31 October 2016, https://www.wsj.com/articles/indonesias-right-to-be-forgotten-raises-press-freedom-issues-1477908348

Social and economic progress

The Sustainable Development Goal 16.9 aims to provide legal identity for all, including birth registration by 2030. National identification systems are being implemented throughout the Asia-Pacific region, and are increasingly linked to delivering public services and ensuring financial inclusion.

Services linked to national identity programmes[8]

Country/Programme	Financial Services	Social Transfers	Health	Elections	Surveillance and Security
Bangladesh National ID	Know Your Customer (KYC)	Welfare		KYC	SIM Registration
Cambodia National ID	KYC			Voter Registration	
China National ID	KYC			KYC	Law Enforcement
India Aadhaar	KYC, Digital Banking, Mobile Money	Cash Transfer, Welfare	Tracking Services and Treatment, Verification of Eligibility	Monitoring	Law Enforcement
Pakistan NADRA	Digital Banking	Cash Transfer, Relief	Tracking Services and Treatment	KYC, Monitoring, Voter Registration	Passport, SIM Registration
Sri Lanka National ID	KYC			KYC	
Thailand National ID	KYC	Relief, Welfare	Tracking Services and Treatment, Verification of Eligibility		

Many of these national identification systems are being updated to incorporate electronic and biometric elements as means of authentication for access to financial and social services (e.g., to fulfil requirements for opening bank accounts, and to benefit from government assistance programmes such as cash transfers, relief and welfare).

India's Aadhaar is the world's largest biometrics identity programme. The key privacy concerns related to this programme (and other national identity programmes that use biometrics) include the following:[9]

- Registration is being outsourced to a massive group of private and public registrars and operators, increasing the chance of data breaches.

8 International Telecommunication Union, "Review of National Identity Programs," May 2016.

9 Jessica McKenzie, "The Uncertain Future of India's Plan to Biometrically Identify Everyone," *TechPresident*, 28 August 2014, http://techpresident.com/news/wegov/25250/the-uncertain-future-indias-plan-biometrically-identify-everyone ; Malavika Jayaram, "Aadhaar debate: Privacy is not an elitist concern - it's the only way to secure equality," *Scroll.in*, 15 August 2015, https://scroll.in/article/748043/aadhaar-debate-privacy-is-not-an-elitist-concern-its-the-only-way-to-secure-equality ; Malavika Jayaram, "India's Big Brother Project," *Boston Review*, 19 May 2014, http://bostonreview.net/world/malavika-jayaram-india-unique-identification-biometrics

- Once a person's biometrics have been compromised, they cannot be reissued like passwords or signatures.
- There are no privacy and data protection laws in place, and no independent privacy regulator.
- Although the programme is voluntary, the need for an Aadhaar number for key services like attending school, getting married, buying cooking gas means that those without a number are excluded from these services.
- Individuals categorized as poor, transgender and disabled in the system risk being discriminated against.

Databases previously in silos are now being interlinked. This means if there is a breach, more data is at risk and it makes datasets a more attractive target. At the same time, it can also enable pervasive surveillance systems, which could lead to categorization of individuals, discrimination, exclusion, unjust treatment and unequal opportunities.

Online privacy concern does not match ability to protect oneself online.

In a survey commissioned by Privacy International, respondents from Hong Kong, Malaysia and the Philippines were interviewed. Results showed that:[10]

>80% were concerned about the sale of their personal data | **>50%** were not aware of privacy laws in the country

Today, large databases of data about us exist in the form of open data and big data. Increasingly, we are not being informed about the monitoring we are placed under, and are not equipped with the capabilities or given the opportunity to question these activities.

Open Data

As part of the open government movement, governments are opening up their previously locked datasets on population, public budgets, education, health, housing, trade, etc. Open data is linked with stimulating research and development, and driving innovation through the use and re-use of data to address development problems. These datasets, however, may include individual records that threaten individual privacy if released openly.

One of the most significant risks is the re-identification of de-identified data. For example, Australia's Department of Health released over a billion lines of de-identified personal health data in 2016 but withdrew it shortly afterwards because Melbourne University researchers re-identified it.[11] In response, the Australian Privacy Act has been amended to make it a criminal offence to re-identify individuals from anonymized government datasets,[12] but in other countries of Asia-Pacific, re-identification is not a criminal offence.

10 Privacy International, "Report - A New Dawn: Privacy in Asia," December 2012, https://www.privacyinternational.org/node/928

11 Karen Middleton, "Millions of Australians caught in health records breach," *The Saturday Paper*, 8 October 2016, https://www.thesaturdaypaper.com.au/news/politics/2016/10/08/millions-australians-caught-health-records-breach/14758452003833

12 The Parliament of the Commonwealth of Australia, Privacy Amendment (Re-identification Offence) Bill 2016, http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1047_first-senate/toc_pdf/1614720.pdf;fileType=application%2Fpdf

Big Data

Corporations are collecting and using all forms of data—every online search made, webpage visited, e-mail or message sent, product or service purchased, leaves hundreds of thousands of electronic tracks about an individual. Tools are available to aggregate these electronic tracks to form individuals' profiles. A research shows that the automated analysis of "likes" on Facebook alone can accurately predict in over 80% of cases, individuals' sexual orientation, ethnicity, and religious and political views; and in over 65% of cases use of addictive substances.[13] Big data has become a profitable commodity, as evident in targeted advertising, a multi-billion dollar business. Big data is also used for mass surveillance.

China uses big data to give its citizens a social rating[14]

The social credit system collects information on all citizens from mobile phones, social media, e-commerce sites and various other sources, including government records, to rate not only individuals' financial creditworthiness but also personal conduct. Those with high ratings are rewarded with access to loans, scholarships, jobs and various benefits like faster services at government offices, while those with low ratings risk being denied access to these services. The system is being piloted in various cities and expects to be rolled out nationwide by 2020.

At the same time, big data can offer insights to determine side-effects of drugs, optimize energy use, improve traffic control, and tackle other development issues. Mobile phone records have been used to track dengue fever, malaria and Ebola, for instance.

Lack of Awareness

Nevertheless, many individuals are unaware that they are being tracked. Do you agree to the terms of agreement on online sites without reading or understanding them?

A study analyzed the standard terms of agreement of popular online sites, highlighting terms that have an impact on users' privacy rights.[15]

	Google	Facebook	Yahoo	Amazon	Twitter	YouTube
Unfettered right of provider to access user data	✓	✓	✓	✓	✓	✓
Access to private chat, emails	✓	✓	✓	✓	✓	✓
Access to location, GPS, IP address, Wi-Fi points and cell towers without further user consent	✓	✓	✓		✓	✓
Right to delete any user data without notice		✓	✓	✓	✓	✓
Right to modify any user data without notice	✓	✓	✓	✓	✓	✓
Right to share user data with law enforcement	✓	✓	✓	✓	✓	✓
Right to share user data with advertisers without user opt-out	✓	✓	✓		✓	✓
No clearly stated deletion policy for user data and metadata	✓	✓	✓	✓		✓

13 Michal Kosinski, David Stillwell and Thore Graepel, "Private traits and attributes are predictable from digital records of human behavior," *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 110, No. 15, pp. 5802-5 (2013), http://www.pnas.org/content/110/15/5802.full

14 Simon Denyer, "China wants to give all of its citizens a score - and their rating could affect every area of their lives," *Independent*, 23 October 2016, http://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html ; The Economist, "China invents the digital totalitarian state," 17 December 2016, http://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian ; The Wall Street Journal, "China's 'Social Credit' System: Turning Big Data into Mass Surveillance," 21 December 2016, http://blogs.wsj.com/chinarealtime/2016/12/21/chinas-social-credit-system-turning-big-data-into-mass-surveillance/

15 Emily Taylor, *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality* (Centre for International Governance Innovation and Chatham House, 2016).

The problem with raising awareness about privacy issues is the difficulty of visualizing privacy harms, especially online. Users feel little sense of violation about their e-commerce transactions being tracked to profile them, or their e-mail messages being read.

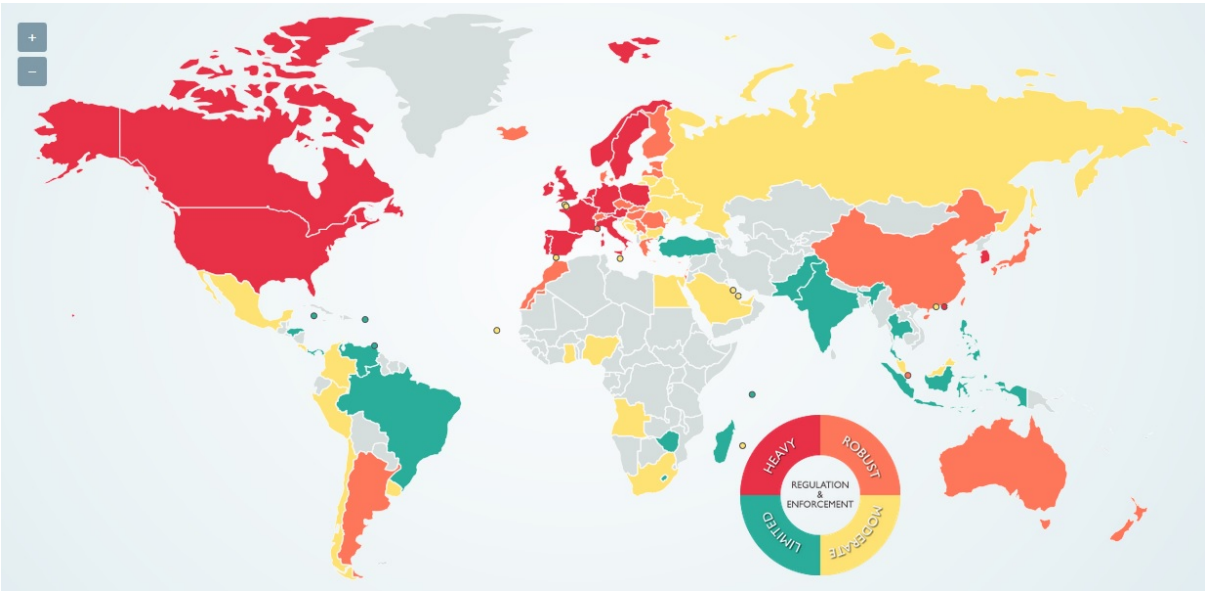
But fundamentally, privacy is about promoting equality, about the ability to assert our rights in the face of significant power imbalances. Already, big data is being used by corporations to offer differential prices to consumers. It can also be used by those in the position of power to discriminate against specific groups, leading to denied access to services and employment, and harassment and violence.

The threats that women and men face online are different, and because of power imbalances, women are generally more vulnerable to cybercrimes, online surveillance and their impacts. For example, men are less likely to be threatened with death or rape for their oppositional or challenging views.[16] Tackling online privacy therefore needs to be gender sensitive.

The Opportunities

Global and regional efforts are bringing online privacy issues to the fore.

Figure 4. Comparison of data protection laws



Source: DLA Piper, "Data Protection Laws of the World," https://www.dlapiperdataprotection.com/ (accessed on 3 February 2017).

Laws are important in setting the standards that other countries and regions copy. For example, the European Union (EU) Data Protection Directive that prohibits the export of data to countries lacking similar protections, compels any country wishing to do business with the EU to pass comparable legislation. Japan, the Republic of Korea, the Philippines and other

16 Katerina Fialova and Flavia Fascendini, "Voices from Digital Spaces: Technology Related Violence Against Women," *GenderIT.org*, 27 March 2012, http://www.genderit.org/resources/voices-digital-spaces-technology-related-violence-against-women ; Tactical Technology Collective, "The Other Internet: Gender, Privacy and Digital Security," https://tacticaltech.org/news/other-internet-gender-privacy-and-digital-security

countries in the Asia-Pacific have recently passed or amended privacy laws to meet EU privacy standards.[17]

In the Asia-Pacific region, the **Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR)** system sets the standard for cross-border privacy protection. Japan is the first country in Asia to join the CBPR system. Other countries that have joined this system include Canada, Mexico and the United States. A recent survey indicates that the Philippines, Republic of Korea and Singapore "plan to join", and Australia, Hong Kong, Taiwan and Viet Nam are "considering" joining the CBPR system.[18] On an individual company level, those that have been through the CBPR certification process include large corporations like Apple, HP, IBM and erck.

In a survey by Telenor Group on Asia's entrepreneurs, results show that more than a third of the respondents believe that cybersecurity and data privacy is their number one priority, and keeping their customers' data safe and secure is the biggest challenge facing Asian startups.[19]

Privacy commissioners are building online trust through engagement with multiple stakeholders.

Privacy commissioners generally provide independent oversight and enforcement of privacy laws, as well as raise awareness of online privacy issues. Members of the Asia Pacific Privacy Authorities include privacy commissioners from Australia, Hong Kong, Japan, Republic of Korea, Macao, New Zealand, the Philippines and Singapore.

For example, the Hong Kong Privacy Commissioner for Personal Data (PCPD) is very active in responding to public enquiries and complaints about privacy, taking action on breach incidents, and raising awareness through engagements with government organizations, business professionals from different sectors, media agencies, students and the elderly. The PCPD has been promoting the implementation of the Privacy Management Programme in organizations. The programme aims to incorporate personal data privacy protection as part of organizations' governance responsibilities.[20]

This is part of the trend to shift the onus of privacy protection to public and private organizations, as user consent alone in this increasingly complex digital environment place an undue burden on the user, most of whom do not have the ability to full understand the risks and ramifications.[21]

17 Julia Fioretti, "EU aims for data transfer deal with Japan, South Korea," Reuters, 10 January 2017, http://www.reuters.com/article/eu-data-idUSL5N1EZ5X3 ; Mark Parsons and Louise Crawford, "Philippines Finalizes Data Privacy Act Implementing Rules," *Hogan Lovells Chronicle of Data Protection*, 9 September 2016, http://www.hldataprotection.com/2016/09/articles/international-eu-privacy/philippines-finalizes-data-privacy-act-implementing-rules /. **Note: On 25 May 2018, the EU General Data Protection Regulation will replace the directive.**

18 Calli Schroeder, "Growing focus on privacy in Asia," International Association of Privacy Professionals, 9 January 2017, https://iapp.org/news/a/growing-focus-on-privacy-in-asia/

19 Telecomasia.net, "Mobile fuelling growth in Asia's startup scene," 5 January 2017, http://www.telecomasia.net/content/mobile-fuelling-growth-asias-startup-scene

20 Hong Kong PCPD, "Privacy Complaints Appear to Start to Stabilise Generally Despite a Significant Increase in Direct Marketing Related Cases," 24 January 2017, https://www.pcpd.org.hk/english/news_events/media_statements/press_20170124b.html

21 EY, *Privacy Trends 2016* (2016); International Association of Privacy Professionals, "Demonstrating privacy accountability," 28 April 2011, https://iapp.org/news/a/demonstrating-privacy-accountability/

Alignment with the SDGs

The SDGs does not explicitly address online privacy issues, but it does reaffirm the importance of the Universal Declaration of Human Rights, as well as other international instruments relating to human rights and international law, which includes the right to privacy.

The United Nations Statistical Commission created a Global Working Group on Big Data for Official Statistics to investigate the benefits and challenges of big data, including the potential for monitoring and reporting on the SDGs. Privacy is recognized as one of the key issues.[22]

Questions to Think About

What are the good practices (in law, governance and technology) for promoting innovation through the use of open data and big data, and at the same time ensure that privacy rights are protected?

How can countries that have just started building its digital economy accelerate efforts towards addressing the lack of adequate national legislation and enforcement to protect individuals' privacy rights?

How can countries address: (1) insufficient procedures for the use of surveillance; (2) practically no oversight of organizations that are accumulating more and more data of individuals; and (3) lack of remedies for violations of privacy?

What are the privacy implications of new and emerging technologies, such as the Internet of Things and Artificial Intelligence, and how can they be proactively managed (rather than merely reacting to their effects)?

22 United Nations, "Using Big Data for the Sustainable Development Goals," http://unstats.un.org/bigdata/taskteams/sdgs/