University of New South Wales Law Research Series

PRIVACY IN SOUTH ASIAN (SAARC) STATES: REASONS FOR OPTIMISM

GRAHAM GREENLEAF

(2017) 149 *Privacy Laws & Business International Report* 18

[2018] *UNSWLRS* 20

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Privacy in South Asian (SAARC) States: Reasons for optimism

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2017) 149 *Privacy Laws & Business International Report* 18-20

The SAARC region (South Asian Area of Regional Cooperation), comprising the eight states of South Asia (India, Sri Lanka, Bangladesh, Pakistan, Bhutan, Nepal, Maldives and Afghanistan), is the Asian sub-region with the least development of data privacy laws. This article reviews the position in the seven South Asian countries other than India, since mid 2014.

Development of privacy protection in South Asia has been stalled by many factors, but there are now some reasons for optimism. Since a previous comprehensive review in mid-2014, [1] there have been no new data privacy laws for any of these countries in the past three years. However, there are indicators that such laws are under development in four (Sri Lanka, Bhutan, Nepal and Maldives), plus significant developments in other countries in relation to Right to Information (RTI) laws, and some political and other developments important to note in relation to potential longer-term developments. There are no relevant regional developments resulting from the SAARC agreements. However, the most significant regional factor is the possible implications of the Indian Supreme Court decision on the fundamental constitutional right of privacy.

Constitutional rights of privacy after Puttaswamy

A nine judge 'constitution bench' of India's Supreme Court unanimously decided in *Puttaswamy v Union of India*[2] on 24 August 2017 that India's Constitution recognises an inalienable and inherent right of privacy as a fundamental constitutional right. It is an implied right, because privacy is not explicitly mentioned in the Constitution, but it is implied by Article 21's protections of life and liberty, and is also protected by other constitutional provisions providing procedural guarantees. Privacy protection is also required by India's ratification of the UN's *International Covenant on Civil and Political Rights* (ICCPR), article 17 of which protects privacy. The decision will affect private sector practices ('horizontal effect') as well as actions by the Indian state ('vertical effect'). The Court identified three main aspects of privacy: privacy of the body; privacy of information; and privacy of choice. Subsequent smaller constitution benches will now decide the constitutionality of various pieces of legislation, and practices, in light of the fundamental right of privacy. These include the constitutionality of India's ID system (the Aadhaar), the criminalisation of homosexual

[1] For the position to mid-2014, see G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014),

[2] *Puttaswamy v Union of India* , Supreme Court of India, 24 August 2017 (Writ Petition (Civil) No. 494 of 2012)

conduct, and prohibitions on consumption of certain foods, and probably many more issues. It is very likely that, in order to protect the constitutionality of other legislation and practices, the Indian government will now have to legislate comprehensively to protect privacy in relation to both the public and private sectors in India.[3]

This decision, and those that will implement it in relation to specific issues, could have a significant influence on some of the other seven South Asian states, as well as more broadly. All South Asian countries provide some potential constitutional protection of privacy. The first post-*Puttaswamy* constitutional privacy case has already been launched in Sri Lanka (discussed below). Explicit constitutional protection of privacy is provided in Nepal (see below concerning new Constitution of 2015), in Bangladesh (many specified aspects), Pakistan ('privacy of the home', but courts have found implied protection of information privacy), and the Maldives (explicitly to many aspects of privacy). In Bhutan and Afghanistan, and in most of the other countries, 'life and liberty' has constitutional protection, potentially implying implied protection of privacy as has occurred in India.[4] All South Asian countries have ratified the ICCPR, and in Nepal and Sri Lanka its provisions should automatically become part of domestic law (the 'monist' approach to international law).[5] In Sri Lanka's new constitutional challenge, the ICCPR could be significant. While it cannot be assumed that constitutional courts in other South Asian countries will be influenced by decisions of the Indian Supreme Court, the 547 page *Puttaswamy* decision will be difficult for any court dealing with privacy issues to ignore, even if it is not explicitly cited. The constitutions in those countries provide ample opportunities for constitutional litigation on privacy, and *Puttaswamy* may encourage such litigation.

Sri Lanka

With the demise of the authoritarian Mahinda Rajapaksa government in an unexpected presidential election defeat in 2015, and a subsequent second defeat in Parliamentary elections, the prospects for data privacy laws in in Sri Lanka under the new Sirisena government have improved. The Sirisena government has aimed to implement a more parliamentary and less presidential government.

Only six weeks after the *Puttaswamy* decisions, Sri Lanka's Supreme Court will on 12 October commence hearing a petition against at attempt by the Department of Registration of Persons, by regulations under an existing law, to build a central database 'with comprehensive data, profiling every citizen, containing entire family trees'[6] and said by the petitioners to give 'virtually unrestricted access to any information concerning any citizen recorded with any public authority'. An ID card is also said to be part of the proposal. The challenge is made under Part III 'Fundamental Rights' (Articles 10-14A), and in accordance with the Article 17 rights of persons 'to apply to the Supreme Court, as provided by Article 126, in respect of the infringement or imminent infringement, by executive or administrative action, of a fundamental right.'[7] The fundamental rights described in Sri Lanka's Constitution are worded quite differently from those in the Indian Constitution (with no clause giving general

---

[3] See G. Greenleaf 'Constitution Bench' to decide India's data privacy future' (2017) 148 *Privacy Laws & Business International Report*, 28-31, for details of the committee established to draw up such a law, and background to the Court's decision.

[4] Greenleaf, *Asian Data Privacy Laws*, Chapter 16.

[5] Greenleaf, *Asian Data Privacy Laws*, p. 474.

[6] Staff reporter 'Sri Lanka Supreme Court petitioned on invasion of privacy, central database profiling' *economynext*, 10 October 2017 <http://www.economynext.com/Sri_Lanka_top_court_petitioned_on_invasion_of_privacy,_central_database_profiling-3-8896.html>

[7] Constitution of the Democratic Socialist Republic of Sri Lanka.

protection to life and liberty as in India), but there are numerous specific protections (such as for freedoms of thought, speech and association) where specific aspects of a right of privacy relevant to an ID system could be implied. In general, these fundamental rights may only be 'subject to such restrictions as may be prescribed by law in the interests of national security, public order and the protection of public health or morality or for the purpose of securing due recognition and respect for the rights and freedoms of others or of meeting the just requirements of the general welfare of a democratic society' (Art. 15(7)). It is difficult to predict whether the petitioners may be successful in this case, but if they are then (as in India) it may push the Sri Lankan government to implement a data privacy law, in part so as be able to validly enact an ID system.

Sri Lanka's *Right to Information Act*[8] came into force on 4 February 2017. The RTI Act also establishes a Right to Information Commission.[9] The Act covers all public authorities, with a very broad definition of same (s. 43). The RTI Act has protections against the disclosure of personal information from government records, but only if the information is less than ten years old (s. 5). The Commission consists of five members appointed by the President upon the recommendation of the Constitutional Council, for five year terms (s. 12), and with other indicia of independence. The Commission has considerable powers, including to determine appeals against decisions by agencies (s. 15). Subsequent appeals can go to the Court of Appeal (s. 34). Every public authority must appoint an information officer, to whom individual make requests for information in the first instance (s. 23). This RTI Act is a very straight-forward 'access to documents' Act, and does not have any of the privacy-protective provisions of Nepal's similarly-named legislation, not even correction of inaccurate personal records. However, in establishing an independent Commission in this area, it provides one possible path for expansion to deal with data privacy issues (at least concerning public authorities).

The government's previous approach on data protection was that it is 'is pursuing a policy based on the adoption of a Data Protection Code of Practice, encompassing the private sector, with the possibility of the code being placed on a statutory footing through regulations issued under the *Information and Communication Technology Act of 2003*.[10] As such, this approach can be seen as self- or co-regulatory approach.'[11]

However, the Information and Communication Technology Authority's (ICTA) legal adviser described the prospects for enactment of a Data Protection Act as 'very positive', particularly in light of the establishment of the RTI Act and Commission. He said there was a need to 'look whether we could make use of Information Commissioner's Office to take additional requirements to monitor and implement' data protection.[12]

Bhutan

The *Bhutan Information Communications and Media Bill 2016*[13] was passed by the National Assembly in June 2017, but must still be submitted to the National Council, with enactment

[8] *Right to Information Act* (Act No. 12 of 2016) (Sri Lanka) <https://www.parliament.lk/uploads/acts/gbills/english/6007.pdf>

[9] RTI Commission website <https://www.parliament.lk/get-involved/right-to-information> .

[10] *Information and Communication Technology Act of 2003* (Sri Lanka) <https://www.gov.lk/elaws/wordpress/wp-content/uploads/2015/07/Information_and_Communication_Technology_Act_No.27.pdf

[11] Government of Sri Lanka *Analysis of e-Laws* (for Cybercrime Convention) <https://www.gov.lk/elaws/wordpress/CMSWrapper/content/elaws?appcode=cp&lang=en&gen_from=hme>

[12] CICRA Holdings website 'Data Protection Act implementation looks positive: Jayantha', undated, 2016 <http://www.cicra.lk/data-protection-act-implementation-looks-positive-jayantha/> ; interview with Jayantha Fernando.

[13] Bhutan Information Communications and Media Bill, 2016 (Bhutan) <http://www.nab.gov.bt/assets/uploads/docs/bills/2016/FinalBICMAbill2016Eng.pdf>

possibly delayed until 2018.[14] The Bill contains extensive and complex provisions related to data privacy which, if enacted, will give Bhutan a data privacy law according to the criteria used in this book, but one which is restricted to provision of ICT services and to consumer e-commerce, whether provided by the private or public sectors. A brief summary only is given here.

Chapter 17 'Protection of online or offline privacy' requires organisations to protect personal information received from users or consumers, including sensitive personal information (which is defined). They must have an accessible privacy policy which sets out the purposes for which information may be collected and used, and details of rights of access and correction. Collection, use and disclosure are limited to 'that which a reasonable person would consider appropriate in the circumstances'. Users can require information to be removed. Organisations may only disclose information to third parties for these purposes (with an 'opt-in' exception for other uses), must ensure by contractual and other means that such third parties observe these requirements, and remain liable for their actions if they do not.

Chapter 21 of the Bill, 'Data Protection' sets out quite a comprehensive data privacy code which in some places repeats what is in Chapter 17, but often in a more strict form, and with more clarity in relation to offences and compensation. The chapter heading seems to limit it to data collected electronically. Collection, processing, and disclosure of personal information requires written permission or authority of law. Organisations must be 'delete or destroy all personal information which becomes obsolete'. Failure to protect data by 'reasonable security practices', unlawful disclosure of data, and unlawful copying of data, all constitute offences and liability to pay compensation.

The Bill also establishes an independent Bhutan Infocomm and Media Authority, and an Office of Consumer Protection, which have powers to investigate and resolve complaints, with rights of appeal to an appellate tribunal and then to the courts.

Nepal

Nepal replaced its 2007 Interim Constitution with a new Constitution in 2015, amidst violent protests across the southern Tarai plains by ethnic groups, and dissatisfaction by other groups who consider they have been marginalised. Subsequent amendments in 2016 have not satisfied dissident groups.[15] Nevertheless, Nepal does have a constitution for the first time in nearly a decade. Devastating earthquakes in early 2015 have impeded progress in other areas.

The new Constitution of 2015[16] gives explicit protection to privacy, providing in Article 28 that 'Except in circumstances provided by law, privacy in relation to the person, and their residence, property, documents, records, statistics and correspondence, and their reputation are inviolable.' Article 47 requires that the state must make 'legal provisions' for 'the enforcement of the rights conferred' within three years of the Constitution's commencement, so it seems that a data privacy law should be on the legislative agenda. Nepali citizens can challenge the constitutionality of any legislation before the Supreme Court (Art. 133).

UNESCO implemented an EU-funded project (to 2016) to make Nepal's *Right to Information Act 2007* more effective, and reported that the National Information Commission (NIC) had

---

[14] Sonam Yangdon 'Bhutan Information Communication and Media Bill passed in the NA' *The Bhutanese*, 10 June 2017 <http://thebhutanese.bt/bhutan-information-communication-and-media-bill-passed-in-the-na/>.

[15] Crisis Group 'Nepal's Divisive New Constitution: An Existential Crisis' 4 April 2016 <https://www.crisisgroup.org/asia/south-asia/nepal/nepal%E2%80%99s-divisive-new-constitution-existential-crisis>

[16] *Nepal's Constitution of 2015*, Constitute Project <https://www.constituteproject.org/constitution/Nepal_2015.pdf?lang=en>

received 470 appeals from different information seekers, and has issued the order to public agencies to provide information to 409 of these appeals, but that NIC orders were not observed in all cases.[17] The have been no specific developments on data protection issues.

Pakistan

In April 2017 Pakistan's IT Minister announced that the Ministry of Information Technology and Telecommunication (MoITT) would introduce a Data Protection Act (DPA) to Parliament 'within three months' in order to protect the rights of internet users.[18] Such claims are easy to make and break. A Privacy International report notes the provisions of the *Prevention of Electronic Crimes Act* 2016 which make it easier for police agencies to invade privacy.[19]

In February 2017 a Pakistan Senate select committee, which had been deliberating since 2012, approved for transmission to the Parliament a Right to Information (RTI) Bill to replace the Freedom of Information Ordinance 2002 which has uncertain scope and effectiveness.[20] The provincial assembly in Sindh passed the *Sindh Transparency and Right to Information Bill, 2016*,[21] which will become an Act with its assent by the governor, and will repeal The Sindh Freedom of Information Act 2006.[22] A Sindh Information Commission will be established.

The other jurisdictions: Bangladesh, Maldives and Afghanistan

There have been recent no data privacy developments in ***Bangladesh***. The Right to Information law has been actively implemented by the Information Commission, which from 2009 to 2015, received 1,450 complaints about non-receipt of requested information, almost all of which had been finalised by 2016.[23] This may be a base on which a data privacy law could be built.

The Ministry of Economic Development of the ***Maldives*** put out a tender in May 2017 for 'Translation of Privacy and Personal Data Protection Act',[24] and while there have been no other announcements about such plans, this does indicate that legislation is under consideration.

The ongoing war in ***Afghanistan*** makes the prospect of any data privacy laws unrealistic.

Conclusions: Potential positives for both trade and for human rights

Bangladesh, Pakistan and Sri Lanka have significant economies, and so the development of data privacy laws in those countries has potential impacts on international trade, including making it easier for personal data to be transferred from not only the EU, but from any of the 90% of the 121 countries with data privacy laws which have some data export restrictions in their laws. From the human rights perspective, the development of a full data privacy law in any these seven countries would be a considerable step forward, as would the extension of constitutional privacy rights, as is now being tested in Sri Lanka.

---

[17] UNESCO EU project EIDHR/2012/292-704 project report <http://www.unesco.org/new/en/kathmandu/communication-and-information/eu-right-to-information-project/>

[18] Maheen Karwai 'IT Ministry to introduce Data Protection Act in Pakistan within three months', Techjuice, 6 April 2017.

[19] Privacy International 'State of Privacy: Pakistan', 14 March 2017 <https://www.privacyinternational.org/node/970>.

[20] Staff 'Pakistan parliamentary body approves Right to Information Bill', *The Indian Express*, 14 February 2017

[21] *Sindh Transparency and Right to Information Bill, 2016* (Pakistan) <http://shehri.org/rti/foi%20laws/Sindh%20Transparency%20&%20Right%20To%20Information%20Bill%202016.pdf>

[22] Habib Khan Ghori 'Sindh Assembly passes transparency, right to information bill', Dawn (newspaper), 14 March 2017.

[23] Muhammad Zamir 'Evolving Dimensions of the Bangladesh RTI Act' 3 November 2016, freedominfo.org website

[24] Tender documents (Maldives) < http://www.trade.gov.mv/dms/325/1494911558.pdf>,