PRIVACY INTERNATIONAL

Report

A New Dawn: Privacy in Asia

December 2012

Report

A New Dawn: Privacy in Asia
December 2012

PRIVACY INTERNATIONAL

www.privacyinternational.org

Summary

Privacy has truly become an issue of global resonance. A quick glance at policy agendas in countries around the world shows that privacy and surveillance issues are increasingly important. The challenge, however, is improving the ability of governments and policy stakeholders to engage in a policy debate that is informed about the dangers of surveillance and the importance of protecting privacy. This is the primary objective of our Privacy in the Developing World programme.

In this report, we summarise our partner's research into privacy in developing countries across Asia. The experiences of privacy in these countries are illustrative of the many opportunities for and challenges to the advancement of privacy, not only the developing world but across the world.

Background

It was not always clear that privacy would become a global concern. It has shared a similar trajectory to the global discussion around human rights: not too long ago, cultural relativistic arguments were overpowering those who wished to argue for "universal" human rights that exist outside of the 'West'. Universal human rights were considered no more than a western construct, propagated by individualistic cultures, and thrust upon countries with more collectivist cultures. The modern articulation of this argument is focused around the needs of the 'north' vs. 'south'. That is, whereas human rights are convenient in developed countries that are not war-torn or in need of basic infrastructure, less developed countries need to focus on basic development, not luxuries like rights. Even now, it is challenging to reconcile efforts to promote human rights with development challenges – the silence in academic and policy debates is remarkable.

It was only relatively recently that the debate around privacy was stuck in this 'collectivist' vs. 'individualistic' cultural discourse. However, the revolutions and rebellions that have occurred in recent years have given rise to the plight of the protestor who cares not about culture but about societal change. This has permitted a different discourse to emerge that doesn't reduce all people in a country as being representative of some collectivist culture that cares not for safeguards and protections.

In our three-year study into privacy in Asian developing countries, we faced these arguments quite often, at least in the early days. The concept of personal privacy, as the argument went, is alien to Asian cultures, who preference collectivism over individualism. The experiences shared by our partners in Bangladesh, Hong Kong, India, Indonesia, Malaysia, Nepal, Thailand, Pakistan, and the Philippines, eventually revealed the untruth of this argument. The reports on privacy issues in these countries that we have compiled in cooperation with our partners show a much more nuanced and interesting picture.

Building a case for privacy wasn't always easy. Sometimes languages do not have terms for the concept of privacy. There are deep-seated differences both across and within nations, due to histories, traditions, or even conditions around spaces and customs. International industry and articulations of new 'social norms' also arose with alarming speed and repetition. Most interestingly, some of our partners themselves at the outset questioned whether there was any chance of seeing privacy rise on government agendas because of historic avoidance of the issues.

Over the course of this project, which included extensive research and consultation conducted by our partners who ran dozens of workshops and meetings, a very different picture emerged. First, all these countries were dealing with the same political, economic, social and technological dynamics as other countries around the world, including those in the West. Anti-terrorism policy, new economic opportunities

from the information and communications technologies sectors, a dramatic rise in use of internet and mobile communications, and eventually social networking, and the increased capacities of surveillance technologies have posed challenges to governments across Asia. In parallel, governments have been adopting new policies to expand personal information collection and sharing. Second, we discovered that privacy concerns and the need for safeguards were often embedded deeply in a nation, and not just as a response to modern phenomena. In sum, we found that privacy is not an alien concept, but rather is increasingly seen as a key political and emerging consumer right.

Privacy: emerging or entrenched?

'Culture' is a very difficult concept to capture, and understanding whether a right is in sync with or cognisable by a specific culture is equally challenging. This is especially true in the case of privacy; what are we to make, for example, of the complete absence in some languages of a word for privacy? This is certainly true in the West as well, evidenced by the use of terminology such as 'private life' rather than 'privacy' because of the lack of appropriate word in some Western languages. The absence of language does not necessarily mean that privacy is prioritised any less; in fact, in Europe, it is even arguable that some of those countries without specific terminology for privacy have very strong privacy traditions.

Our research points out that the notion of a surveillance state is deeply entrenched in Asian societies. In some instances, there are long traditions of state surveillance: Thailand's ancient Siamese states collected information and used coded wrist-tattooing for ID, for example, and China's policy of keeping a register of its citizens has been dated back to the 4th century BC. Again, however, these factors are again not entirely unique to these countries, if we consider the Roman census, the Norman Domesday book, and some of Europe's darker historical traditions of physically marking individuals. The influence of colonialism on the privacy practices in Asian countries is clear, and in fact our research revealed that the countries included in this study often had more in common because of their colonial past rather than some geographic proximity or shared traditions.

Religious values must also be considered as we undertake the process of capturing 'culture'. The results are again inconclusive. Our report from Thailand reflects on the meaning of Buddhist values regarding avoidance of "possessive individualism" and how this may affect privacy, but quickly the debate moves to empirics and finds that awareness of privacy in Thailand is high vis-à-vis voter privacy, police intrusion, and physical privacy, but low with regards to consumer protection and ID cards. Our report from Bangladesh, a secular state, ignores any discussion of Islam while noting strong interest in protecting consumer interests, while our Pakistan report reveals that Islamic scripture gives strong regard to privacy. Our report on the world's largest Islamic country, Indonesia, notes that there is a strongly collectivist culture with no strong privacy tradition.

Socio-economic factors also give rise to unevenness in the salience and application of privacy. Surveys conducted in Bangkok in 1996 showed that those who are higher on the socio-economic strata were more concerned about privacy rights, while those in lower socio-economic groups were found to be ignorant of surveillance practices. As increasing numbers across all socio-economic levels are gaining access to the internet, privacy perceptions have become more widespread: a 2001 study of internet users in Thailand found that 70% of internet users recognised their privacy rights online but only 50% knew what action to take when faced with data abuses. The same findings emerged in China where a 2008 study showed that 95% of

respondents felt that the government should set an example of proper data treatment and implement a data protection policy, but even though 42% felt that their personal data had been mishandled or abused, only 4% of victims of abuse had complained or attempted to file a lawsuit.

Conditions are changing around the world, but not just because of technological change. A 2007 study in China found an increase in expectations in privacy and linked this with the shift away from small traditional living environments to the rise of average living space for urban Chinese from 3.6 metres in 1978 to 11.4 metres by 2003.

Our partners also undertook some polling of their own during this project. Their findings have much more rich data than just mere articulations of 'culture'.

- As mentioned above, our Thai partners found concerns about physical, police intrusion, and voting privacy, but lower concerns about consumer privacy and generalised state surveillance. In response to an online intrusion, 56% felt that they would run a campaign to raise awareness of the problem, and only 25% would seek a technological fix, while only 19% would call for more rigorous laws and regulations.
- A Hong Kong survey showed that respondents were concerned about personal data such identity card number (96%), home address (93%), personal financial situation (e.g. bank account, income, etc.) (93%), home or mobile phone number (91%) and family financial situation (90%), but only 34% considered information about their religion "important". The majority of respondents (86%) were concerned about their personal data being sold to third parties by the companies/organizations that had maintained the personal data for purposes other than agreement during purchases of goods or services. They perceived that the information supplied for a specific purpose but used in another purpose was a misuse. Meanwhile just over half knew of the legal regime in Hong Kong.
- In the Philippines, 77% respondents agreed that privacy is a human right. Attention was particularly high in relation to financial (68%), internet privacy (55%), and privacy of the home (50%), but much less so to biometrics (31%). Interestingly, the majority believed that governments should be able to intercept communications, while 36% do not agree with the practice at all. More than 90% were opposed to the sale of personal information. Concerns about government or private sector processing were equal. More than half were not aware of the privacy laws in the country.

- According to the data from Malaysia, identity information and financial information were seen as most sensitive. Of those surveyed, 80% did mind when companies shared their personal information. More than half were not aware of the privacy laws in the country.
- In India, according to the study conducted by our partner, people considered ID information to be most sensitive, followed by financial information, but felt religion, postal mailing address, and full name, were lower priorities. People's awareness of legal protections was quite problematic, and up to 50% saw little problem with surveillance in public spaces. Meanwhile, concerns about online tracking were mounting, and over half of those surveyed believed that both government and private sector bodies would abuse surveillance.

This data should not be seen a statement about culture, such as 'Thai people don't have a problem with companies collecting information'. Rather, the inconsistencies and variances should be seen as indicators of where greater awareness raising may be required.

Similarly, we can't presume that the above data means that some countries' citizens do not care about privacy abuses just because in some cases they understand why governments must collect information. The political, legal, and media discourses all contain critical analysis of political rights. That is, a very common thread across these reports is how privacy interacts with political rights. Colonial-era internal security laws continue to cast a shadow over the protection of civil liberties. Requests to produce identity documents, traditionally a practice which occurred on the streets, is moving to the online sphere. The use of informants and undercover agents are now exhibited through extensive communications surveillance. Dissidents and opposition groups are increasingly under threat due to mounting government surveillance techniques. Thailand's financial surveillance of NGO activists in 2001 led to a key court case that set a precedent for the recognition of privacy. Bangladesh's and Pakistan's political turmoil is reflected in the practices of their surveillance agencies. Unfortunately, all of these countries share a lack of adequate protections for individual rights, insufficient procedures for the use of surveillance, and practically no oversight of public bodies and authorities, which are increasingly accumulating more and more information on their citizens.

Rising need and increased interest

Information and communications technologies present the same challenges to personal privacy in Asia as elsewhere. Almost with complete disregard to 'cultural' differences, Asians react with the same outrage as Westerners when their personal privacy is breached. As such, modern events have precipitated policy change and attitudinal shifts.

To cite a few examples: in Hong Kong, the public outcry at the sale by Octopus Rewards, the public transport payment system, of the personal data of 1.97 million registered users of its cards led to the 2012 passage of the Personal Data (Privacy) Amendment Bill. In the Philippines, a key moment came in 2008 with the "cebu spray" scandal, when a video of a surgical operation, which showed doctors making jokes as they removed an object from a patient's rectum, leaked onto the Internet. The case inspired the Filipino Hospital CCTV Act of 2008, which mandated the installation of CCTV cameras in hospitals and established penalties for publishing the resulting pictures other than in response to a court order. In India, the six years since the passage of the Right to Information Act (2005) has seen the commencement of more than 700 privacy-related cases in the Central Information Commission.

In China, in 2003, there was considerable public sympathy for an 18-year-old couple who sued their school after the principal broadcast CCTV video of them kissing in a classroom. In 2006, a regional newspaper objected strongly when police in the city of Shenzhen shackled 100 prostitutes, pimps, madams, and their customers and forced them to march through a local neighbourhood, dressed in government-issued clothing, while their names and addresses were announced to the public.

Even in Indonesia, a country with a strong collectivist tradition, privacy is an increasingly important issue. Research shows that this is partly due to the influence of international conventions and treaties to which the Indonesian government has become party, and partly the result of advocacy work by Indonesia's Press Council and the non-governmental organisation ELSAM.

A reactive approach to privacy can build momentum around a shift in attitudes. In the early 2000s, low levels of public concern about privacy in the United Kingdom resulted in government policies like ID cards and expansive communications surveillance; however, the public and political reaction against these policies ultimately led to their rejection. We're seeing similar dynamics elsewhere. The introduction of the world's most ambitious identity infrastructure certainly advanced privacy on India's policy agenda. Civil society groups, including our partners at CIS

in India, have been actively participating in consultations, running events, and even pursuing legal cases against the scheme. The Indian government has responded by initiating a commission to review the need for a privacy law in India. Indonesia's movement has been slower: despite public opposition after many court cases regarding wiretapping abuses, Parliament approved national intelligence legislation that enshrined in law many of the pre-existing poor practices in communications surveillance. While it is possible to overstate the extent of 'public opposition', the story in Indonesia is not dissimliar to the story of unwarranted surveillance in the U.S., political turmoil and the eventual Congressional approval of the FISA Amendments Act of 2008.

Lacking implementation and a strong foundation

The key difference between the protection of privacy in the East and in the West is thus not clashing cultural values regarding individual freedoms and social conformism. 'Cultural' arguments and traditional debates about human rights are always worth entertaining, but our challenges are much more detailed and the opportunities much more significant.

One interesting dynamic in the question of the difference between 'the West' and 'the East' is that there is a curious form of political leapfrog being undertaken. The tradition notion of developmental leapfrog occurs as countries skip over a generation of technological developments straight to more current ones. This may or may not be the case in Asia – it is true that some Asian countries are using cheaper, more modern mobile technology infrastructure without first building older, more expensive landlines – but more interesting is that policies and new systems are being introduced in the absence of institutions which should have been established in earlier developmental phases. While in the West, legal frameworks have developed alongside technological advances over many decades, in many parts of the East, outdated legacy legal systems are struggling to adapt to technological change and modern policy ambitions. The Pakistani Telegraph Act, for example, dates to 1885 and enables broad interception powers as it is applied to modern communications.

Even without the technological shifts, this dynamic is clear: only in 2009 did India's High Court in Mumbai strike down colonial-era anti-sodomy laws on the basis of privacy protection, drawing from European and US jurisprudence developed over decades. While many of the countries in this study have constitutional statements of privacy, most lack the jurisprudence, developed in other countries in the 1960s and 1970s over sexual privacy, medical privacy, watchlists, and the advent of modern databases, which in turn informs laws and regulations.

In the case of privacy law, standards, and practices, the overall result has been an incoherent and piecemeal approach. In Indonesia, for example, increased corruption since the fall of the Suharto regime has led to a complex set of rules authorising wiretapping scattered among legislation concerning drugs, telecommunications, electronic transactions, and corruption. However, Indonesia's courts have been active in encouraging change: in a landmark 2008 case, the Constitutional Court annulled a provision of the Law Number 11 Electronic Information and Transactions (2008) in order to require the government draft legislation to regulate wiretapping rather than allow it to proceed by a simple regulation. The plaintiff in this case argued successfully that because privacy is a fundamental human right a limitation on it such as wiretapping could not be imposed solely by a regulatory instrument. Similarly, India's 1951 Telegraph Rules informed interception law in India until the key case of

PUCL v Union of India where the Supreme Court in 1997 declared the breadth of the orders unconstitutional. Yet in both Indonesia and India communications surveillance continues without adequate safeguards.

Many legislative initiatives are adopted in response to individual cases, while others are dictated by economic necessity, or become enshrined in domestic law through accession to international treaties. The result is legislative frameworks for the protection of privacy that lack coherence or fail to make the necessary legal tools available to citizens. For example, Indonesia ratified the International Covenant on Civil and Political Rights (ICCPR) in 2006 with the Law Number 12 on the Ratification of the ICCPR (2005), and the law became self-executing in domestic courts. However, the country still lacks legal protection for personal data, and there is no jurisprudence to provide guidance to the resolution of conflicts between the right to privacy and transparency laws. In Nepal, the right to privacy was inserted into the 1990 constitution, survived in the 2007 constitution, and is currently under consideration for inclusion in the new draft constitution. Yet, notwithstanding a few privacy protections in laws concerning telecommunications, court procedures, and postal activities, there are no privacy laws to support constitutional protections, or supervisory authority to accept complaints. In Hong Kong, the non-statutory code on access to information, written in 1995 and still in force, provides no statutory rights, and citizens cannot apply for judicial review of violations by government departments.

As these examples indicate, in many cases, citizens who suffer privacy rights violations lack a mechanism by which to complain, and are forced to use other means to claim their rights. In Indonesia, for example, victims of privacy violations are more likely to use defamation law or appeal to the Press Council to seek redress. In China, a 2008 study found that only 4% of those who had experienced a privacy breach had complained or attempted to file a lawsuit. Yet people in China do have the right to complain or file suit: China's Tort Liability Law was reformed in 2009, enabling citizens to sue for damages for privacy violations, and other laws provide a general level of privacy protection (though there is no data protection law). A lack of complaints or action, therefore, does not necessarily mean that people do not care about privacy; rather, their concerns are being masked by a lack of access to mechanisms for redress.

The development of privacy protections in Asian countries is made more difficult by the absence or fragility of democratic mechanisms and traditions. Nepal is currently drafting its seventh constitution since 1948. China's constitution lacks comprehensive human rights protections, and the government continues to limit freedom of association, install CCTV cameras in its cities, develop email censorship technology, and monitor the activities of NGOs. In addition, the country has endemic censorship through a nationwide Internet firewall, and, as the scale required for that firewall grows out of bounds, is preparing to replace it with an infrastructure that will control and monitor all Internet connections. Bangladesh, which held its first free, fair, and credible parliamentary election as recently as 1991, is governed by two families

that trade off power but refuse to cooperate; neither respects Bangladeshis' freedom of expression. Pakistan, which became independent in 1956, was under military rule from 1979 to 1988, and again recently. The Indonesian constitution, originally written in 1945, had four amendments added between 1999 and 2002 in order to promote human rights and democracy after the fall of the Suharto regime's New Order. The Filipino constitution dates to 1987, while the Thai constitution is barely five years old.

Responding to global technological change

The growth of the Internet has been similarly uneven. While other Asian countries such as South Korea and Japan garner international attention for the ubiquity and speed of their bandwidth, in the countries studied here Internet penetration and usage are in general far lower, and are concentrated in relatively compact urban areas. In Nepal, as of June 2010 only about 2.2% of the population used the Internet, and government offices were only just beginning to incorporate it into their daily work. In Bangladesh, the penetration rate is 3.5%, while in Thailand the number of Internet users increased by an order of magnitude in the decade to 2011; the country now has a penetration rate of 27.4%. People getting online quickly opt for popular modern global services; Indonesia, for example, has the third highest number of Facebook users in the world. Alongside all this growth is even more rapid growth in mobile phone penetration.

However, whereas the developed world had extensive legal and policy knowledge and experience from which to draw in adapting to rapid technological changes, Asian governments and financial institutions are acclimatising to increasing internet penetration and the opening-up of online services without sufficient expertise to manage security. In India, law enforcement agencies lack the necessary skills, training, and experience to deal with country's many cases of identity theft. In Bangladesh, the Cybercrime Unit, which operates within the Criminal Investigation Department of the Bangladeshi Police, is largely ineffective because its skill level is inadequate to conduct even basic forensic examinations of hacked websites. Paying the private sector to provide technical assistance to government agencies is not only prohibitively expensive, it creates additional risks by putting sensitive information within the grasp of the private sector. A better resolution to the paucity of skills and expertise is the use of bilateral cooperation; for example, Indonesia has established a joint programme whereby Australian police provide the Indonesian police with tools and equipment to carry out investigations. This has resulted in a number of successful prosecutions.

The lack of technical knowledge and experience in developing countries is particularly concerning when considered in the context of two global trends: that of establishing comprehensive surveillance infrastructure; and that among Western countries to cut costs by outsourcing data processing and other back office IT services to third countries. India's lack of data protection or privacy laws is an undoubted contributor to its rampant problems with identity fraud, as is the widespread national deployment of no less than 17 forms of identification, including driving licences, passports, voting cards, PAN (tax) cards, and (the most common and commonly abused) ration cards. In 1999, the Indian government began to consider rolling out a multi-purpose national identity card backed by a National Population Register as a solution; this would incorporate a unique 16-digit identity number, and be populated by census data. Without privacy laws, however, this card and its database will be as vulnerable to abuse as the others.

Responding to global policy drivers

Just as the terrorist attacks of September 11 2001 was the catalyst for so many Western security initiatives, so too have terrorist attacks and other conflicts impacted upon privacy and security in Asian countries. In Hong Kong, post-9/11 anti-terrorism efforts took the form of increased financial tracking. In India, the 1999 Kargil War along the border with Pakistan sparked the push for a national ID card. In Thailand, nine bomb explosions in Bangkok during the 2007 New Year's Eve celebrations led to the installation of more than 10,000 CCTV cameras for traffic monitoring and security purposes. In Indonesia, the 2002 Jakarta and Bali bombs that killed 164 tourists led the government to pass anti-terrorism laws that granted very broad authority to a new intelligence agency. The government has used increased corruption since the fall of the Suharto regime as a justification for wiretapping. Since 2010, Indonesian citizens have been required to have the KTP, or "kartu tanda penduduk", a smart card with embedded fingerprints.

But despite the very real security threats in some Asian countries – Pakistan ranks second in the world in Maplecroft's 2010 and 2011 Terrorism Risk Indexes, behind only Somalia – these governments, like those in the West, also use terrorism as a way to justify policies that institutionalise privacy violations and invisible, automated surveillance. The Indian government wants to build a centralised monitoring system like the UK's Communications Capabilities Development Programme to intercept Internet traffic in real time. Bangladesh has authorised routine collection and monitoring of communications information. China has a force of 30,000 monitoring Internet traffic and is building surveillance intelligence into a network that will bring content filtering to millions of next-generation devices. Technology largely supplied by Western companies will incorporate facial, fingerprint, and speech recognition. DNA databases are proliferating in India, Nepal, and Thailand.

But it's too simple to blame a few exceptional events for all privacy-violating initiatives, many of which have existed for some time. ID cards, for example, have been required for all Chinese citizens over the age of 16 since 1985; these serve as driving licences and library cards and can store digital certificates, but are also used to monitor under-age drinking and the movements of citizens. As in India, card theft, forgery, identity fraud, and misappropriation of the data are significant problems. Hong Kong has had identity cards for residents since 1949; in 2002 these were updated to smart cards with thumbprints, immigration data, and a digital certificate, with room for future expansion to include medical and financial data and driving records.

A positive obligation

In the early days of the Internet, it was common for advocates to explain why censorship did not work by comparing the idea to controlling the cleanliness of water in a swimming pool by only prohibiting urination in the deep end of the pool. This analogy is equally true when applied to the regulation of privacy: in today's globally interconnected world, just as one careless friend on Facebook can expose an individual's movements and activities to external scrutiny by posting accounts, photographs, and video clips, the careless data handling practices or inadequate security training of one nation can expose the data of many others to theft, abuse, and criminal activity. These negative network externalities create a layer of global risk that can only be mitigated by the concerted action of all nations.

Our partners' research also shows how important legislation can be in setting the standards that other countries and regions copy. The most obvious example is the provision in the EU Data Protection Directive that prohibits the export of data to countries lacking similar protections, compeling any country wishing to do business with the EU to pass comparable legislation. A less well-known example is India's Right to Information Act 2005, upon which Bangladesh loosely based its right to Information Ordinance, passed in 2009. Similarly, in China, the first Freedom of Information legislation came in the form of the 2004 Shanghai Provisions, provincial-level legislation that provided the most comprehensive framework for accessing government information that China had ever had, and broke new ground by requiring an inclusive public consultation before the final version was passed. These Provisions were widely copied among local government authorities throughout China before being taken up at the national level in 2007–2008.

For this reason, it is wrong to imagine that privacy in Asia – or anywhere else – can be protected by purely national or regional means. All countries depend on each other to preserve privacy rights. For many of these countries – Hong Kong, Thailand, the Philippines, Indonesia, and especially India – supplying data processing and other back office services to businesses in Western countries is of great economic importance. Accordingly, Asia is a key battleground, caught in the crossfire between the US, which favours minimal interference with data flows in order to promote its business interests, and the EU, whose higher standards other countries must meet in order to facilitate EU contracts. The example Western countries set can be bad as well as good: when established democracies implement endemic surveillance and monitoring the message is sent to countries whose hold on democracy is tenuous that these are acceptable practices.

A continuing challenge

Any argument that privacy is not an important social and legal value in Asia completely ignores the rapid development of laws, technologies and attitudes in these countries over the past decade. The experiences of our partners during this time are testament to the increasing currency of privacy in public and political discourses. However, these experiences also serve to highlight the multitude of reinforcing obstacles to the evolution of both de facto and de jure privacy protections throughout Asia. The unequal development of laws is being hindered by the absence of democratic frameworks, knowledge and expertise deficits, and the challenges posed by instability and conflict. In order to ensure that legislation keeps pace with innovation, Asian governments must seek out comprehensive and collaborative regional arrangements and solutions for telecommunications, population management, media and security. And human rights protections must be incorporated into legislative and constitutional instruments, to ensure that protecting the right to privacy remains at the heart of all government initiatives.

In fact, this is the modern challenge faced by all governments around the world, whether they be in the East or West, North or South.