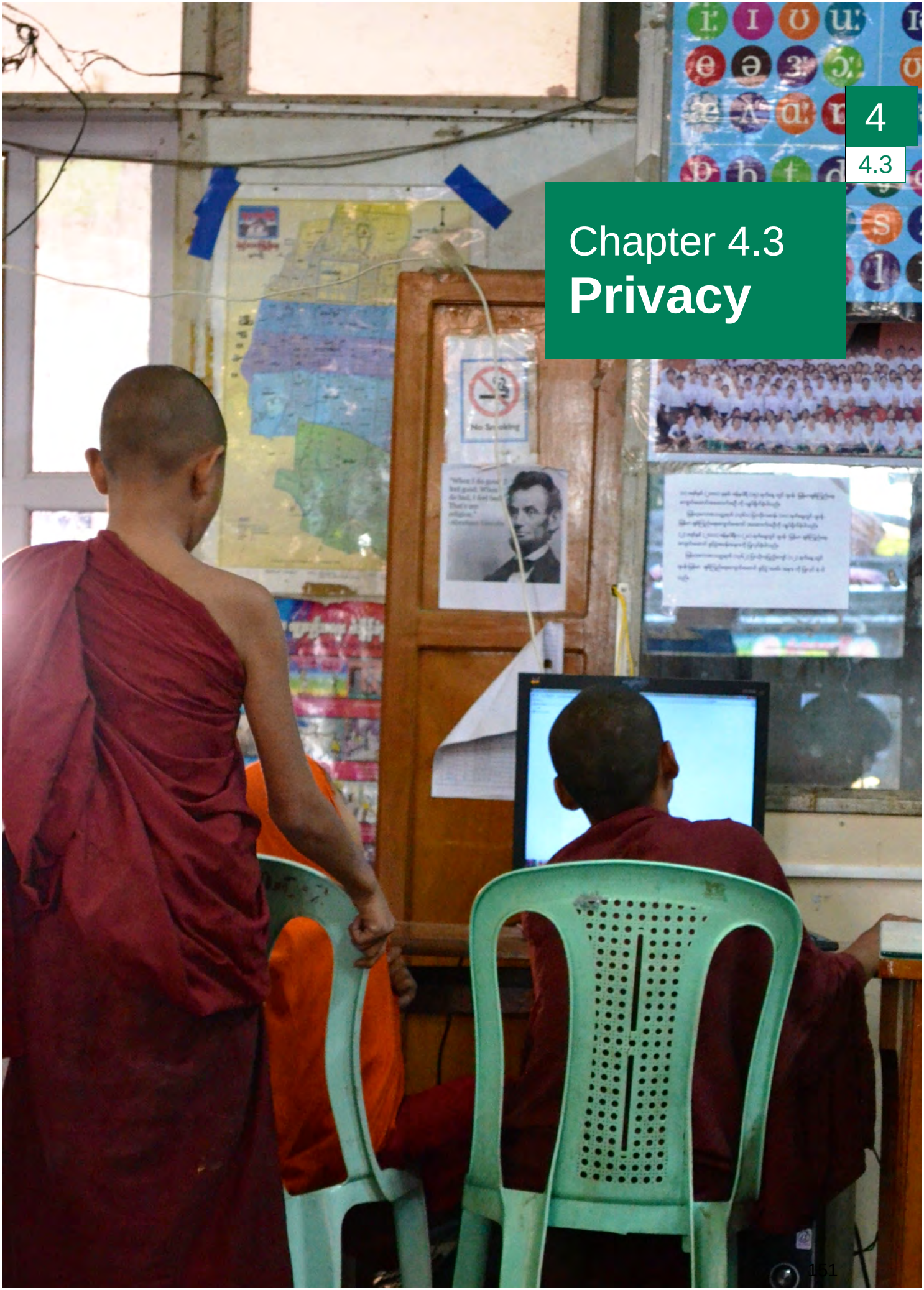
Chapter 4.3
Privacy



4
4.3

Chapter 4.3
Privacy

In this Chapter:

A. Context
- Data Privacy and Data Protection
- Concerns about Privacy and Data Protection in the ICT Sector
- Data Privacy in Myanmar
- International Human Rights Law on Privacy
- The Myanmar Legal Framework and its Current Application

B. Field Research Findings

C. Recommendations for ICT Companies
- General
- Web-Based Services

D. Relevant International Standards and Guidance on Privacy Issues

A. Context

Data Privacy and Data Protection

There are three dimensions to the right to privacy that are implicated by the collection, storage, use and access to digital information by ICT companies:

- data privacy or protection (the term used may differ from country to country[311]) of data held by businesses (covered in this Chapter 4.3 on **Privacy**),
- surveillance, including lawful interception and access to communications data (see Chapter 4.4 on **Surveillance**), and
- the protection of such data against attacks or threats of attack for criminal or other harmful purposes (see Chapter 4.5 on **Cybersecurity**).

In today's digital economy, the amount and type of personal information generated and stored electronically is unprecedented, ranging from email addresses, to bank account numbers, to national ID numbers. Whenever users interact with technology, such as mobile services or the Internet, 'communications data' (as it is commonly referred to in Europe), or 'metadata' (as it is commonly referred to in the U.S) is created and is typically stored by the service provider.[312] This type of data is created by a wide range of interactions with Internet services including email, web browsing, social media, search

[311] See: Baker Hostetler, "2015 International Compendium on Data Privacy Laws" (2015) and Norton Rose Fulbright "2014 Global Data Privacy Directory" (2014). Also see Francoise Gilbert "Privacy vs. Data Protection: What Is The Difference?" (1 October 2014).

[312] The National Information Standards Organization (NISO) defines metadata as "*structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource.*" NISO, "Understanding Metadata" (2004), pg. 16. The former UN Special Rapporteur on Freedom of Opinion and Expression expressed particular concern over the increasing amount of metadata generated by ICT usage and its implication for user privacy. See OHCHR, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" A/HRC/23/40 (17 April 2013).

engines, VoIP (e.g. Skype) and mobile phones. Globally, ICT companies use this information in various ways. For example, free applications or services frequently offer the advertisers who support them a platform for user-targeted advertisements, based on data collected from users. Geographic location data can be used to identify where a user is physically located and provide location based advertisements or services such as taxis, restaurant recommendations, or directions.

As a country's ICT sector grows, more and more personal data is collected and stored by governments and companies providing goods and services online. This more extensive and innovative use of personal data brings greater economic and social benefits, but also increases privacy risks.[313] How the information is shared and who has access to it determines whether or not privacy is protected and respected.

In many countries, national data protection laws require companies to secure and protect such information from access by unauthorised third parties. Data protection or data privacy laws[314] should safeguard user privacy. Such protections are intended to regulate how, when, and why a user's personal information or data may be used or stored by a third party.

They should put limits on governments and companies concerning the collection, storage and sharing of personal data generated by using ICTs when trading, or using goods and services online. This should ensure that it is gathered for a legitimate purpose and protected from misuse. There should be restrictions or limits in each country's data protection or data privacy legislation as to how this information is collected, stored and shared by companies for commercial reasons, or by governments obtaining this kind of information for services such as voting registration, health records or tax purposes.

Legislation that regulates data privacy typically details a consent mechanism to inform and request permission from users, provides a legal definition of what constitutes personal data, mandates an allowable timeframe for the use of any data after consent is given, and includes regulatory mechanisms for pursuing grievances about the use of data. However many national frameworks lack 'use limitations', instead allowing the collection of data for one legitimate aim, but subsequent use for others.[315] In addition, a lack of a data protection framework means there is no opportunity for individuals to seek redress or compensation in cases of unauthorised sharing or use of personal data.[316] Myanmar currently lacks a data protection law.

[313] OECD, "The OECD Privacy Framework", (2013).
[314] Outside Europe, the term 'data protection' and 'data privacy' is used to commonly mean the same thing.
[315] OHCHR, "The right to privacy in the digital age", A/HRC/27/37, (June 2014), para. 27.
[316] Privacy International, "UN Universal Periodic Review, Stakeholder Report 23rd Session, Myanmar, The Right To Privacy In Myanmar", (March 2015), para 32.

4
4.3

Concerns about Privacy and Data Protection in the ICT Sector

The increasing availability of Internet services accessed via a personal computer (PC), laptop, mobile phone or other devices, has brought many benefits and is seen as crucial to continued innovation and development. But it has given rise to numerous privacy concerns about the data that is collected, stored and shared when using such services. The collection and use or misuse of sensitive data has the potential to be used for discriminatory purposes. This could include data on racial origin, political opinions or religious or other beliefs, personal data concerning health or sexual life, genetic data, biometric information, trade-union membership, and data relating to criminal convictions. Unauthorised intrusions to access or destroy data stored for use in criminal purposes – such as unauthorised access to bank accounts – is an issue rising rapidly up the list of key concerns for many businesses. New business models based on the collection and sale of a user's data by the company gathering the data, where data is used for purposes not explicitly revealed to the user who provided the data and without their permission, raise concerns about the respect for user privacy.[317]

While 'Big Data'[318] may carry important benefits, it also carries serious risks. Data mining of large data sets has the potential to be discriminatory. It may discriminate against specific groups and activities (such as in profiling) and it may be used to draw conclusions about large groups of people who may be excluded from data collection, further perpetuating exclusion.[319] In addition to more generalised areas of data protection, there are other areas of online protection that have generated real concern, particularly around the protection of children who are active online.

Table 38: Toward a Social Compact for Digital Privacy and Security[320]

Below are excerpts of the core elements that the Global Commission on Internet Governance advocates in building a new 'social compact' for digital privacy and security:

- "*Fundamental human rights, including privacy and personal data protection, must be protected online. Threats to these core human rights should be addressed by governments and other stakeholders acting both within their own jurisdiction and in cooperation.*
- *Businesses or other organisations that transmit and store data using the Internet must assume greater responsibility to safeguard that data from illegal intrusion, damage or destruction. Users of paid or so-called 'free services' provided on the Internet should know about, and have some choice over, the full range of commercial*

[317] The Global Commission on Internet Governance was established in January 2014, to articulate and advance a strategic vision for the future of Internet governance. With work commencing in May 2014, the two-year project will conduct and support independent research on Internet-related dimensions of global public policy, culminating in an official commission report.
[318] 'Big Data' refers to large datasets that are collected and analysed to find correlations or predict trends. For example, it can be used by business to predict which products will be popular, but can also be used for social issues, such as predicting outbreaks of disease in certain areas.
[319] See Privacy International, "Data Protection" (last accessed August 2015). See also, European Commission, "EU Data Protection Reform and Big Data, Factsheet" (April 2015).
[320] Global Commission on Internet Governance, "Toward a Social Compact for Digital Privacy and Security Statement" (2015).

use on how their data will be deployed, without being excluded from the use of software or services customary for participation in the information age. Such businesses should also demonstrate accountability and provide redress in the case of a security breach.

- *There is a need to reverse the erosion of trust in the Internet brought about by the non-transparent market in collecting, centralising, integrating and analysing enormous quantities of private information about individuals and enterprises — a kind of private surveillance in the service of 'big data', often under the guise of offering a free service."*

Increasingly, there are calls for standards and accountability mechanisms to bolster confidence in the use of the Internet. 'Data due process', access to remedy, and greater transparency – by governments and business – are all being advocated as important steps in maintaining an open and accessible Internet.

In addition, because companies may hold a lot of personal information, they may be subject to requests to hand over information about a user to a government - with or without legal authorisation - in a manner that is not in line with human rights. When a country's law enforcement or intelligence agencies request, access or intercept information collected and stored by ICT companies to support law enforcement or national security investigations, this triggers privacy concerns. This dimension is addressed in Chapter 4.4 on Surveillance.

Privacy in the Myanmar Context

In Myanmar, businesses and Government are transitioning from storing information in filing cabinets to electronic databases. Data can now be stored on remotely located servers, and accessed over the Internet, otherwise known as 'the Cloud'.[321] It means that users have access to an almost unlimited amount of storage of their data, which can be accessed from any computer. Cloud storage is most commonly used for email (such as Gmail) and storing data (such as Dropbox).

The improved efficiency and ease of access provided by digitally storing information is obvious, as are the potential human and commercial risks and need for accompanying legal frameworks. Myanmar companies who long operated in isolation may be finding that data protection requirements are now necessary if they are involved in the cross-border exchange of commerce and data. ASEAN has already put in place frameworks on data protection, as have other regional bodies,[322] including the EU, where appropriate data protection is a prerequisite of before any data can be transferred from the EU.[323]

[321] In the simplest terms, cloud computing means accessing files and applications over the internet, rather than on personal hard drives or servers, via third party services.
[322] See in particular, the basic principles on data protection in the OECD, "Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data" (2013).
[323] Under the EU Data Protection Directive, personal data may only be transferred to third countries i.e. countries outside of the European Union, if that country provides an adequate level of data protection. This created an incentive for some countries to increase data protection standards, due to the economic benefits through increased trade with EU countries.

Equally, whereas protection of privacy was until recently an unknown concept in Myanmar, awareness is growing among the Myanmar business community about the importance of personal data protection even without mandated privacy standards, such as for emerging services such as mobile money.[324] As users weigh competing services, companies that fail to provide strong data safeguards may start to find they lose customers, although currently, the public's awareness of the need to protect personal data is quite low. A recent high profile case involving a (now dismissed) employee of an operator giving unauthorised access to communications data to a friend will have further served to raise awareness[325].

In May 2013, Human Rights Watch sent a letter to mobile network operators shortlisted in the MCIT telecommunications license process seeking clarification regarding how new telecommunications firms entering Myanmar would seek to mitigate potential human rights impacts given Myanmar's lack of legislation related to privacy, censorship, and interception. Both Telenor and Ooredoo issued responses. Their company positions on data privacy took different approaches. MPT and Yatanarpon Teleport have not issued public statements on data privacy. Myanmar's remaining Internet service providers also do not provide any clarification on data privacy policies on their websites.

Ooredoo highlighted its "*commitment to Myanmar to use Singapore as a benchmark"* and the intent to "*implement policies and procedures that are compliant with the 2012 Singapore Data Protection Act.*"[326] The Singapore *Data Protection Act* (PDPA) defines personal data as "*data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.*" [327] The PDPA requires private sector companies to notify and provide individuals with an explanation when their personal data is collected and disclosed. With regard to telecommunications, the Singapore Personal Data Protection Commission has issued advisory guidelines for the telecommunications sector.

However, the Singapore PDPA does not provide adequate protection for human rights. It lacks references to specific and relevant human rights principles under international law, exempts Government agencies and entities working on their behalf, has ambiguous limitations on legitimate purpose for data collection and disclosure under the PDPA, exceptions to individual consent requirements, poor transparency and accountability mechanisms, and broad language that allows for organisations and data to be exempt from PDPA regulations in the future.[328]

Telenor's response to Human Rights Watch's letter cited Telenor's "*well established privacy and data protection regime*".[329] A section of the Telenor website explains that, "*Telenor Group only processes personal data for the purposes the data was originally*

[324] See Myanmar Times, "Preparing the Financial System for Digital Attacks" (March 2015)
[325] 'Ooredoo data breach brings legal action', 3 September 2015, Myanmar Times.
[326] Ooredoo response to Business and Human Rights Resource Centre's request for a response to HRW's Report: Burma Telecom Winners Should Safeguard Users
[327] Personal Data Protection Commission Singapore, "Legislation and Guidelines: Overview" (last accessed August 2015).
[328] Internal analysis prepared for the Institute of Human Rights and Business.
[329] Human Rights Watch, "Response from Ms. Oldgard, Vice President, Head of Group Corporate Responsibility, Telenor Group" (4 June 2013).

collected, and only for as long as the purpose exists. The companies in Telenor Group will ensure that:

- "Persons we process data about are properly informed when their personal data is being collected;
- All persons we process information about have the right to obtain relevant information on the processing of personal data related to them;
- Persons we process and store data about are able to exercise user choice and control and have appropriate rights to correct or delete their personal data;
- Personal data are kept in a form which permits identification of persons for no longer than is necessary for the purposes for which the data were collected;
- Transfer of personal data does not compromise an adequate level of protection;
- Risk based, planned and systematic measures are undertaken to ensure satisfactory information security in connection with the processing of personal data;
- The processing of personal data is properly documented;
- Appropriate training is given to relevant personnel involved in the processing of personal data."[330]

Telenor specifically cited its participation in privacy projects with the GSMA (where it is a full member),[331] and the European Telecommunications Network Operator's Association (ETNO) working group on data protection[332]. In their Mobile Privacy Principles, the global industry association GSMA defines personal data more specifically than Singapore does in the PDPA. While acknowledging that personal information ultimately depends on its local legal definition, the GSMA defines personal data as:[333]

- "Any data that is collected directly from a user (e.g. entered by the user via an application's user interface and which may include name and address, credit card details);
- Any data about a user that is gathered indirectly (e.g. mobile phone number, email address, name, gender, birth data, location data, IP address, IMEI, unique phone ID);
- Any data about a user's behavior (e.g. location data, service and product use data, website visits);
- Any user-generated data held on a user's device (call logs, messages, user-generated images, contact lists or address books, notes, and security credentials."

The ETNO works closely with the GSMA, and focuses on the review of legal frameworks impacting data protection in Europe. In terms of data protection and privacy, the draft EU General Data Protection Regulation (GPDR) is regarded as providing high standards in the protection of personal data by the international community.[334] As part of that process, the ETNO has supported the notion that there should be no preferential treatment in data

[330] Telenor Group, "Our Privacy Position" (last accessed August 2015).
[331] GSMA, "Mobile and Privacy" (last accessed August 2015). The GSMA is an industry association representing mobile operators worldwide.
[332] ETNO, "Data Protection, Trust & Security" (last accessed August 2015).
[333] GSMA, "Mobile Privacy Principles" (2012).
[334] See European Commission, "Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" (25 January 2012). The legislation is not without criticism from global technology firms such as Google who have recently complied with users' "right to be forgotten and to erasure" requests under Article 17 of the GPDR. Telenor Myanmar is a wholly owned subsidiary of the Telenor Group per the license requirements stipulated by MCIT. Telenor Group is headquartered in Oslo, Norway. Norway is not a member state of the European Union but has implemented the EU Data Protection Directive 95/46/EC.

protection requirements between the private and public sectors.[335] This is a notable difference between the GPDR and the PDPA in Singapore.

As the UK NGO Privacy International notes in their submission to Myanmar's Universal Periodic Review (UPR) at the Human Rights Council, whilst some ICT companies, such as Telenor, have developed and adopted their own data protection and retention policies, the lack of national legislation regulating data retention and the circumstances under which the Government can request access to user data means that such internal policies may not be strong enough to protect the privacy of users and secure the freedom of services.[336]

In recent years, many other countries have passed data protection or data privacy legislation for the first time or updating them in response to the impact of ICTs on privacy.[337] In Asia, in addition to Singapore, Malaysia, and Taiwan have a "*Personal Data Protection Act*".[338] The law of Japan is called "*Act on the Protection of Personal Information*".[339] South Korea's law is called the "*Protection of Personal Data Act*".[340] The equivalent law of the Philippines is called the "*Data Privacy Act*".[341]

International Human Rights Law on Privacy

Every person has the right to privacy under international human rights law, including privacy of his/her communications.[342] Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) provides:

> *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

---

[335] ETNO, "ETNO supports the choice of the legal instrument for the future Data Protection framework" (4 July 2014).
[336] Privacy International, "UN Universal Periodic Review, Stakeholder Report 23rd Session, Myanmar, The Right To Privacy In Myanmar" (March 2015), para 33. See also A Alderaro, "Digitalizing Myanmar: Connectivity Developments in Political Transition", *Internet Policy Observatory*, (2014) pg. 10.
[337] In the European Union, the suite of laws protecting personal data are currently being updatedIn 2012, the European Commission proposed to unify data protection in the EU under a single law, the General Data Protection Regulation (GDPR), to take into account technological developments such as social networking and cloud computing. A draft was presented at the European Parliament in March 2014. A final version is expected to be adopted by end 2015. See: Greens/EFA "EU General Data Protection Regulation State of play and 10 main issues by Jan Philipp Albrecht" (17 January 2015) and European Commission, "Commissioner Jourová: Concluding the EU Data Protection Reform is essential" (28 January 2015).
[338] See Malaysia and Taiwan *Personal Data Protection Acts*.
[339] Government of Japan, *Act on the Protection of Personal Information Act No. 57* (2003)
[340] Korean LII, "Personal Information Protection Act" (last accessed August 2015). See also Francoise Gilbert, "Privacy v. Data Protection. What Is The Difference?" (1 October 2014).
[341] Republic of the Philippines *Act No. 10173 2012 Data Privacy Act*.
[342] The right to privacy is also include in a wide range of international and regional human rights instruments, signalling its wide acceptance: Article 14 of the United Nations Convention on Migrant Workers; Article 16 of the UN Convention on the Rights of the Child; Article 10 of the African Charter on the Rights and Welfare of the Child; Article 4 of the African Union Principles on Freedom of Expression (the right of access to information); Article 11 of the American Convention on Human Rights; Article 5 of the American Declaration of the Rights and Duties of Man, Articles 16 and 21 of the Arab Charter on Human Rights; Article 21 of the ASEAN Human Rights Declaration; and Article 8 of the European Convention on Human Rights. See a compilation of privacy references in international and regional human rights instruments and see also http://gilc.org/privacy/survey/intro.html

2. Everyone has the right to the protection of the law against such interference or attacks."

Legitimate Restrictions on the Right to Privacy

Article 17 of the ICCPR on privacy is less specific about permissible reasons for restricting the right to privacy as compared to Article 19 on the freedom of expression (See Chapter 4.1 on the Freedom of Expression). Restrictions on the right to privacy must be neither "unlawful" nor "arbitrary".

A restriction is "unlawful" when the interference is not authorised by States on the basis of national law authorising interference. The national law must be sufficiently accessible, clear and precise and also must not conflict with other provisions of the ICCPR, such as the prohibition on discrimination, or the country's own constitution.

The protection against "arbitrary interference" means that the interference should be reasonable in the particular circumstances. It must be in proportion to the aim, and the least intrusive option available to accomplish the aim, and be necessary in the circumstances for reaching a legitimate aim.[343]

The Myanmar Legal Framework and its Current Application

The 2008 Constitution

Most countries have provisions to protect privacy as part of their constitution. At a minimum, these provisions usually include the rights of privacy in the home and of communications. The 2008 Constitution of Myanmar provides certain privacy protection:

"357. The Union shall protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of this Constitution."[344]

The constitutional provisions provide for a wide scope of protection by using the term "*other communications*" but the protections are available to citizens only and are not specific about the kinds of protections it will offer. Moreover, the guarantees are "*subject to the provisions of this Constitution*" (Art. 357), which has numerous restrictions on these constitutional guarantees that are quite broad. There has been little constitutional jurisprudence developed in Myanmar, meaning there is little to rely on that might limit the application of these broadly worded restrictions.

[343] The limitation must also be shown to have some chance of achieving that goal while at the same time not being so overly restrictive that the restriction makes the exercise of the right meaningless. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary. Pillay report

[344] *Constitution of Myanmar* (2008).

4
4.3

Current Legal Framework and Gaps

Although the Constitution declares that privacy will be protected under the law, currently there are no separate privacy laws in Myanmar. In addition, there is no legal framework on data protection or data privacy. A Consumer Protection Law was adopted in March 2014 but its focus is on food safety[345]. As part of its ASEAN membership, Myanmar has agreed to develop best practices on data protection by 2015 but there have been no announcements to date on forthcoming plans.[346] Civil society have highlighted that Myanmar has an opportunity to leapfrog its peers in regulating privacy, data protection, Internet governance, freedom of speech/expression (partially due to the lack of legacy regulations) and to ensure that the push to improve access does not compromise these other issues. A civil society coalition suggested a proactive discussion among Government and civil society and operators, rather than waiting until the Government demands 'private' data (for purposes of national security).[347]

The integrity of technical processes for protecting user data in Myanmar is unclear, particularly in regards to Myanmar's National Certificate Authority. Certificates have significant impacts on user privacy, as they are used to verify a chain of trust whenever a user submits personal information (such as an account username and password) to an online service. These certificates are used to verify the website's validity and prevent users from submitting data to an unauthorised third party. Myanmar's certificate authority was established under the *Electronic Transaction Law* (No.5/2004).[348] Policies and practices related to Myanmar's existing certificate authority are unclear. Websites for Myanmar's Root Certification Authority, and Yatanarpon Certificate Authority are currently offline. As the Internet now represents a global community, a lack of clear processes and transparency among certificate authorities puts users' private information at risk and promotes distrust. Recently, Google and Mozilla took steps to de-trust all certificates signed by China's National Certificate Authority.[349]

Privacy International also noted in the UPR submission,

> *"In 2013, the government announced that it would replace the paper National Registration card with a smarter digital identification card to include biometric data. Whilst it seems plans have been put on hold for such a change because of financial constraints, it is an issue that must be closely monitored as if digitised the data stored will have privacy implications which will need to be considered to ensure that the right to privacy of citizens and their personal data are protected."*[350]

---

[345] 'Burma President approves consumer protection law' Irrawaddy, 17 March 2014
[346] ZicoLaw, "ASEAN Insights, Personal Data Protection" Issue 4 (7 November 2013).
[347] Verena Weber "Diversifying the global content and apps market" (last accessed August 2015).
[348] *Myanmar Electronic Transactions Law* (2004).
[349] In April 2015, both Google and Firefox stopped trusting certificates issued by China Internet Network Information Center (CNNIC). Google noted that CNNIC had signed fake certificates for Google domains, while Firefox noted that CNNIC lacked documented PKI practices. For additional information please see: Emil Protalinski, VentureBeat "Google and Mozilla decide to ban Chinese certificate authority CNNIC from Chrome and Firefox" (April 2nd 2015)
[350] Privacy International, "UN Universal Periodic Review, Stakeholder Report 23rd Session, Myanmar, The Right To Privacy In Myanmar" (2015), para 33.

In 2014, the Myanmar Government held a public consultation on the issue of mandatory registration of personal information of SIM card and mobile phone purchasers' cards.[351] This indicates the Government may not be considering the data privacy implications of its telecommunications regulations. The mandatory registration of SIM cards in other jurisdictions has shown that there are a range of unintended consequences, prompting other governments to consider and then reject the idea.[352] MCIT proposed that mandatory SIM registration would enable new and innovative services (e.g., mobile money and mHealth services). However, where such sensitive data is exchanged, these services should be required to register for extra mobile-enabled services; such registration should always be service focused. Mandatory registration could act as a barrier to accessing mobile services because people may not have an address or registration number or may be reluctant to provide personal details due to distrust of the Government.

MCIT is yet to define its procedures for the lawful interception of user communications, or access to communications data (See Chapter 4.4 on Surveillance), though it has committed to doing so. This is a crucial and important procedure that requires further consultation and consideration before any mass collection of customer data through mandatory registration is considered. Without data retention requirements, large amount of data, held for an indefinite amount of time, would be susceptible to unlawful uses, including unauthorised surveillance, leaks, and security breaches resulting in negative, and in some cases, severe impacts on the enjoyment of the right to privacy.

B. Field Research Findings

Privacy Policies by Myanmar Companies

Human Rights Implicated: Right to privacy

Field Assessment Findings

- **MCRB reviewed the websites of 73 companies** as part of the Transparency in Myanmar Enterprises project (TiME) (or 'Pwint Thit Sa' in Burmese) to collect a small sample of the use and disclosure of privacy policies and protections by Myanmar companies.[353]
- Of the 73 company websites reviewed, **only 6 explicitly explaine how they handled and used** customers', users', workers' and others' data.
- **Only 1 company actually adopted a formal privacy policy** outlining in detail its security and data handling measures**.**
- **4 company's statements were contained within other operational policies,** such as a code of conduct or code of ethics**.**
- **1 ISP explicitly did not commit to any level of data protection**, instead confirming that it may monitor its service from time to time and disclose any information regarding customers or their use as required under national law, regulations, Government requests, or that it saw fit.
- **A majority of the companies reviewed presented no accessible information** about the ways in which they handle and use data.

[351] See: MCRB, "MCRB calls for Further Consideration of the Impacts of Requiring SIM Card Registration in Myanmar" (21 May 2014).
[352] Ibid.
[353] MCRB, "Pwint Thit Sa Project (TiME)" (2015).

- One company confirmed that it would **"*only*" guarantee the privacy of the company email system to the extent required by law**, whereas a separate statement in its Communications Policy stated that as a leading institution in Myanmar it would strive to be as open and transparent as possible while protecting privacy and personal information.

Stakeholder Engagement and Grievance Mechanisms

Human Rights Implicated: Right to privacy

Field Assessment Findings

- **The concept of privacy:** The concept of privacy as outlined in international human rights standards is not fully understood in the context of Burmese culture, in which people live in close proximity and often with extended family, making the notion of a truly private space in Myanmar uncommon. Stakeholders note that this lack of familiarity with the concept carries over into the digital space.
- **Lack of user concern about privacy**: There is, therefore, a lack of understanding of the importance of the right to privacy online, the basic steps users should take to protect it, e.g. using passwords to protect their online accounts and information, and the consequences of a failure to protect one's own privacy e.g. posting personal information such as bank details online.
- **Lack of awareness on appropriate protections on social media**: Users on social media were observed sharing sensitive personal data including bank statements and checks for donations or even more sensitive information about health status without appropriate protections. Users reported being unaware of how to configure privacy settings in their social media accounts. Users also reported being unaware of how to report on content on social media.
- **Lack of policies or clear communication of policies**: Data retention policies were absent, or in some cases not clearly communicated to the customer/user even when internally present (e.g. 5 years for retention of customer data on paper).
- **SIM Card Registration:** The Ministry of Communications and Information Technology (MCIT) has mandated a system that in theory requires an ID, which is recorded, to buy a SIM card. However in practice, people use their own ID and buy multiple SIM cards for their friends and family members. People have raised concerns regarding data protection and their ID being associated with another user's activity incorrectly. It was noted that in many other countries (e.g. Thailand and India), people are not required to show IDs or register with their IDs to purchase SIM cards.

Data Protection

Human Rights Implicated: Right to privacy

Field Assessment Findings

- **Physical protection of data**: There was variation in the level of access control in place for businesses with data centers. Some businesses logged visitors to data centers, while others had multiple levels of security in place (biometric such as a fingerprint reader, access card, and close circuit television).
- **Protection of data in case of emergencies**: Data backups or disaster response

policies were mostly absent. One bank maintained a data centre for production and a data centre for disaster recovery.

- **Protection of data from unauthorised access within the company**: Role-segregation varied among businesses collecting customer's personal data. One bank segregated employees conducting a 'Know Your Customer' check (where basic information was provided, such as a National Registration Card) from employees conducting financial transactions.
- **Affordability of data protection**: Many businesses used pirated software for internal business functions including email which presents a data protection risk. Small and medium size businesses complained about the cost of buying licensed software.
- **Lack of policies or clear communication of policies**: Data retention policies were absent, or in some cases not clearly communicated to the customer/user even when internally present (e.g. 5 years for retention of customer data on paper).

Myanmar Good Practice Examples:

- Companies are beginning to conduct threat and vulnerability assessments across their applications, network, and infrastructure on an ongoing basis to test the security of the data held in their systems. One bank uses two separate companies to perform assessments (one local and one international).

C. Privacy: Recommendations for ICT Companies

General

- **Understand contextual risks around Myanmar's history and Government action**: Given Myanmar's historical legacy of Government surveillance and information control, coupled with ICT policies and laws that are not aligned with international human rights standards, there exist significant risks for violation of ICT user rights to protection of privacy and anonymity. There are also risks for any ICT company that may be implicated in such violations. Risks related to the violation of the right to privacy in Myanmar with respect to Government actions can be categorised into at least two separate but closely related areas of concern:
  - Government monitoring and surveillance of user activity and content; and
  - Government access to user-identifying information (See Chapter 4.4 on Surveillance).
- **Use company procedures to plug gaps in the Myanmar legal framework:** As Myanmar currently has no legal requirements for mandatory protection of data of ICT users, this means that the protection of personal data is left to individual companies or Government departments, if at all. Sectors such as ICT or the financial sector are likely to be more aware of the importance of data protection. Companies in these sectors may have their own policies and procedures, or industry-specific standards to assist in developing systems and policies. But other companies will also need to develop systems to protect personal information, as well as externally available policies to inform customers about how their data is being handled (see next point).
- **Develop and implement appropriate policies and procedures to safeguard data privacy**: Companies in the ICT value chain, which often collect and store a large amount of personal information about their users, need processes and policies in place to ensure they protect user information. These must be clear about how they will collect, store and share user information with third parties, and under what circumstances the Government (or others) can have access to information or intercept communications. This information would usually be set out in a company's 'privacy

policy'. This policy should be written in easy-to-understand language, spelling out the implications of when the user's data would be shared, with whom, and why. They should be clearly made known to all staff, particularly those with accessnto sensitive data, and the sanctions for breaching them known. The International Standards and Guidance in section D below set out what issues to address when developing their policies and systems.[354]

- **Ensure that businesses' terms and conditions or privacy policies are publically available** so users or customers are aware of what personal data may be collected or shared. The policies should be available in Burmese and local languages. Putting in place robust data protection standards is a good way for local companies to show they are ready to meet data protection requirements from business partners, trading partners and users.

Web Based Services

- **Develop and promote privacy controls**: Overall digital literacy in Myanmar remains low. Many users are interacting with web-based services for the first time. Some international companies have controls in place that allow a user to manage his/her 'digital footprint' online in addition to their broader online experience. A large majority of users in Myanmar are not familiar with these features. On social media, privacy management controls allow the ability to selectively share or restrict information, including access to photographs, contact information or profile accessibility (e.g. public and private settings). For email communication such as newsletters or mailing lists, this involves the ability to unsubscribe or customise subscription settings. Companies need to raise awareness of these features through appropriate media and ensure these features are available in local languages.
- **Develop and promote content-reporting mechanisms**: Abusive or offensive content can violate a user's privacy. Larger social media platforms now maintain community standards, which outline acceptable use online, while also providing guidance to users on how to address violations of these standards in the case of prohibited content or behaviour. Content reporting mechanisms allow users to report abusive or invasive content to platform moderators. For first time users, understanding how and when to report content is a critical part of ensuring a safe experience online. Similar to privacy controls, companies must raise awareness of these features through appropriate media, and ensure that community standards and reporting tools are available in local languages[355].

D. Relevant International Standards and Guidance on Privacy Issues

Relevant International Standards:

- Asia Pacific Economic Cooperation Group (APEC) 2005 Privacy Framework
- EU Data Protection Directive 95/46
- EU Directive on Privacy and Electronic Communications 02/58

[354] See for example, European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" (2013), pg. 21, 45-46.

[355] In September 2015, Facebook launched a Burmese version of its community standards 'Facebook rules get local to tackle abuse', Myanmar Times, 10 September 2015