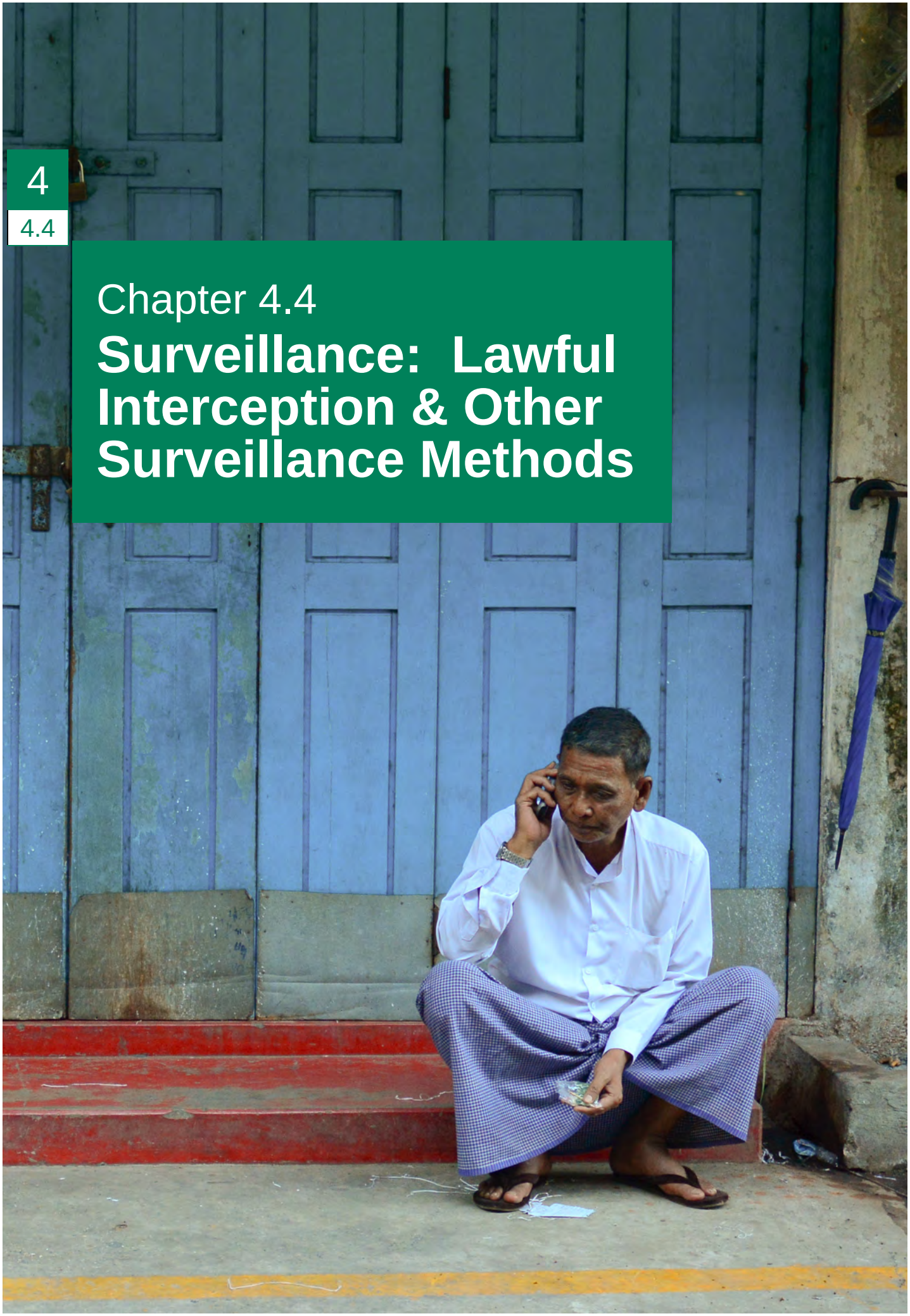
4

4.4

Chapter 4.4

Surveillance: Lawful Interception & Other Surveillance Methods



4
4.4

Chapter 4.4

Surveillance: Lawful Interception & Other Surveillance Methods

In this Chapter:

A. Context

Lawful Interception and Other Surveillance Methods

Governments have legitimate reasons to initiate surveillance of a person's communications i.e. intercept or monitor the communications of certain individuals or organisations. For example, the target may be legitimately suspected of planning to commit or having committed a serious crime, such as a terrorist act. There are two ways a person's communciations can be put under surveillance:

- Interception of the content of communications in real time (known as lawful interception); or
- Access to other, historical user data (known as 'communications data').

Lawful interception is permitted in most countries under legal statute in order to assist with criminal investigations, prosecute serious crime, or prevent national security emergencies. Usually, a telecommunications operator collects intercepted communications of private individuals or organisations, and then provides law enforcement officials with access. Lawful interception refers to the interception of, or access to, a person's communications in real time, as the communication is taking place.

- ***Content*** refers to what was said during a phone call or what can be read in the content of an email or other type of digital message. Interception of content,

depending on the country, usually requires that law enforcement authorities seek a judicial warrant from a court or an executive warrant signed by a senior government official, an important procedural safeguard to protecting the rights of those under scrutiny. (See the Annex to the Recommendations for more information).

In addition to this, authorities may require access to communications data, which is generated as a person uses communications services. This is often known as the 'who, where, when and how' of a communication. With the many different ways to communicate electronically currently in existence, there is a much greater array of data and interactions that can be collected and therefore demanded by law enforcement authorities.

- ***Communications Data*** (this sometimes referred to as metadata but will be described as communications data in this SWIA) is basically everything but the content. It includes telephone numbers of both the caller and the recipient, the time and duration of a call, unique identifying numbers (each subscriber is allocated one, as is each mobile device), email addresses, web domains visited and location data. This information is important as it builds up a detailed picture of a person's life and movements. Often intercepting the content of a call or email is not necessary. In contrast to content, there are often weaker legal protections around interception of stored communications data.

Intercepting communications is an intrusive process into someone's privacy. That is why any such intrusion should be governed by a strict legal framework to prevent arbitrary violations of privacy.

Legal Requirements

The Annex to the Recommendations provides more detailed recommendations on the kinds of considerations any government, including the Myanmar Government, should take into consideration in establishing its procedures for lawful interception or other forms of communications surveillance at each step of the process. These steps include the authorisation process, oversight and remedy procedures for lawful interception, and other communications surveillance, to ensure that the procedures and practice are in line with international law.

Technical Requirements

Telecommunication systems or networks in most countries must include, by law, the technical capability to intercept communications. For example, providing the technical means for interception is a legal requirement for European companies under a *1995 EU Resolution on Law Enforcement Operational Needs with respect to Public Telecommunication Networks and Services,*[356] which allows lawful interception to assist law enforcement in investigating and preventing crime.

In order for communications to be intercepted, the telecommunications system needs to be configured in a specific technical way according to a set of standards. The European Telecommunications Standards Institute (ETSI)[357] (one of many industry-led technical standardising bodies worldwide) has taken the lead in producing globally applicable

[356] Council of Europe (1995) "Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services" (20 June 2001).
[357] See European Telecommunications Standards Institute (ETSI) (last accessed August 2015).

standards for ICTs, including lawful intercept requirements. ETSI defines lawful interception as:

> *"A security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organisations."*[358]

It is not yet clear or certain which technical standards Myanmar will be using to implement the technical requirements of lawful interception.

Mass Surveillance

In contrast to lawful interception, mass surveillance is understood to refer to the bulk access and/or collection of many users' communications without prior suspicion of criminal activity by the individual targets. Therefore mass surveillance involves no individual target, no prior suspicion, is not time bound and due to the technology employed, is potentially limitless. In contrast to technology provided for lawful interception, much of the technology that allows mass surveillance is unregulated. The adoption of mass surveillance technology thus impinges on the very essence of the right to privacy. [359]

Products that Facilitate Surveillance

- ***'Dual use' technology*:** 'Dual use' is a legal term applied to products, services or technology that can be used for both military and civilian purposes. In the ICT sector, it can apply to technology that can be used for commercial functions, but may also contribute to infringements on human rights. For example, a technique called 'Deep Packet Inspection' (DPI) was developed to analyse network traffic to make sure the network runs smoothly. However, it is also capable of reading emails and governments wishing to conduct unlawful surveillance can abuse this. Many states known to censor the Internet also use DPI.[360] In January 2012, the European Union banned DPI exports to Syria because of the monitoring and interception capabilities, as it was thought they were being used against dissidents.[361]
- ***Unregulated technology*:** There is growing concern that an increasing number of companies may be selling technology that goes beyond regulated, targeted and controllable interception of individuals under prior suspicion. It is currently considered by many experts to be 'single use', because it is difficult to justify a legitimate use for technology that is capable of intruding so much into a person's correspondence and home. There is evidence that some governments are using the technology to track and detain political dissidents as part of a wider pattern of intimidation.[362] Examples

[358] Ibid, "Lawful Interception".
[359] See: UN General Assembly, "Promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/69/397 (23 September 2014).
[360] Ben Wagner, Ludwig-Maximilians-Universität München and Universiteit Leiden, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control" Global Voices Advocacy (2009).
[361] EU Council, "Regulation No. 36/2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011" (18 January 2012) Annex V
[362] Citizen Lab, "From Bahrain With Love: Finfisher's Spy Kit Exposed" (2012); Electronic Frontier Foundation (EFF), Kidane Vs Ethiopia (last accessed August 2015).

include malware[363] that infects a target's computer and switches on webcams and microphones on devices, and zero-days[364], which exploits vulnerabilities in a computer application to enable hacking of communications, therefore reducing digital security for many others using the same application. Companies selling these technologies often try to portray these products as having the same status as statutorily mandated (and regulated) 'lawful intercept' functionality – often simply because they are sold to a government purchaser. However experience has shown that some governments are using these technologies quite specifically because they are not regulated and to avoid following lawful interception procedures.[365] With these tools, surveillance is not limited to those within a country's borders, which puts exiles or the diaspora overseas at risk of intrusive surveillance.[366] Companies who sell this type of technology are increasingly being targeted by law suits and other legal actions.[367]

Concerns about Surveillance and the ICT Sector

Under international human rights law[368], individuals are protected from any unlawful and arbitrary interference with their privacy, family, home, or correspondence. The act of surveillance, whether physical (such as a house search) or of a person's communications (such as monitoring phone calls and emails) is an inherently intrusive act and risks violating a person's privacy. In addition, surveillance of person's communications can limit the exchange of information and ideas resulting in a 'chilling effect' on freedom of expression, as people are less likely to express themselves freely if they know they are being observed or monitored.

Intercepting communications is under particular scrutiny by international organisations, civil society groups and governments due to the impact of surveillance on privacy and other human rights such as the right to receive and impart information. [369] The same technology that can help law enforcement prosecute criminals may also be misused by authorities, such as when specific groups (opposition parties, human rights defenders, ethnic, religious or sexual minorities) are placed under surveillance for the purpose of intimidating, persecuting and silencing them. There is evidence in some countries that the technology is being used to track and detain political dissidents as part of a wider pattern of intimidation, often with negative consequences or harm to the individuals.[370]

---

[363] Software that is created and used to gain access to private computer systems, disrupt computer operations and/or gather sensitive information. Malware includes computer viruses, "Trojan horse" software and "worms".
[364] An attack on vulnerability in a computer application or operating system that developers have not yet addressed.
[365]Citizen Lab, "Shedding Light on the Surveillance Industry: The Importance of Evidence-based, Impartial Research" (20 December 2013).
[366] For example, there is evidence that the government of Ethiopia is using surveillance technology to target the diaspora overseas who may be critical of the government. Ethiopians living in the UK, US, Norway and Switzerland have been targeted with malware, resulting in an illegal wire-tapping case in the US. See Electronic Frontier Foundation (EFF), Kidane Vs Ethiopia (last accessed August 2015) and Reporters Without Borders "Enemies of the Internet" (2014).
[367] For examples of lawsuits and other official complaints, see OECD Watch and the Business and Human Rights Resource Centre.
[368] International Covenant on Civil and Political Rights, Article 17.
[369] See for example the Global Conference on Cyberspace 2015, the Global Commission on Internet Governance, the work of the United Nations and international civil society organisations such as Privacy International, Electronic Frontier Foundation, Citizen Lab, Access, and many local civil society organisations.
[370] See for example: Freedom House, "Freedom on the Net" (2013) details a particular example from Sudan:

Being able to locate a mobile phone also means being able to locate the person carrying the mobile phone, which is potentially a powerful tool for surveillance. It is important to have access to such information in emergency responses, such as abduction or identifying survivors in a natural disaster area. However mobile phone technology has unfortunately become increasingly dangerous for activists in some countries.

It is therefore critical that any intrusion into a person's privacy through the interception of communications is subject to legal process and includes protection for human rights. In countries where the relevant legal framework on lawful interception is absent or deficient, when there is a case of a misuse, companies within the ICT value chain that have had a role in that process (network providers, vendors, operators, over the top service providers) are often accused of contributing to the abuse of human rights through its operations. This may involve invasions of privacy or in some cases even more severe abuses such as torture. Some companies may actively assist the government in carrying out arbitrary surveillance by allowing secret access to their servers (often called a 'back door'). If the government responsible for the misuse is perceived to be repressive, this may increase scrutiny by human rights groups.

History of Surveillance in Myanmar

The former military government in Myanmar established an intrusive surveillance regime for many years, both online and offline, in order to suppress criticism and dissent and restrict access to information. The fear and threat of surveillance was part of life, especially for members of opposition political parties, student activists, and ethnic minorities in armed conflict areas.

Physical Surveillance

Under the former military government, intelligence agencies, some of which were originally established under British colonial rule, proliferated. Multiple organisations were charged with keeping people under surveillance. Intelligence activities expanded rapidly following the 1988 coup d'état which re-established military rule after its suppression of the nationwide pro-democracy movement. The hierarchy and structure of the intelligence agencies changed throughout the 1980s, 1990s and 2000's as the military government imprisoned or purged various members of the intelligence community. Before the reform process began in 2011, Myanmar's intelligence agencies played a consistent role in gathering information on real or impugned critics, in suppressing dissent, and in arresting and interrogating suspects.

The *Village Act* and *The Town Act* required everyone to report the identity of overnight guests to local officials, who could refuse "*permission*" for houseguests. The law was enforced by periodic household inspections by authorities, often accompanied by Special

---

"The activist Mohamed Ahmed switched off his phone for a few days in early July 2012 to avoid arrest while in hiding from the NISS [National Intelligence and Security Service]. When he turned his phone back on as he was walking home to see his family, NISS officials roaming his neighbourhood managed to track his location based on the nearest telecommunications tower and arrested him later that night." pg. 14.

Branch agents, and mostly at night. It has been reported that these inspections were used as an opportunity to monitor, harass or arrest political activists and inspections increased during the pro-democracy uprisings in 1988, 1998 and 2007. [371]

In addition to intelligence agencies, a wide network of informants attached to various official groups operated throughout the country. A 2007 Human Rights Watch report stated that this group of informants systematically began to track down activists and organisers of the 2007 protest movement, often known as 'the Saffron Revolution'.[372]

Telecommunications surveillance

As early as 1990, reports surfaced that telephone calls and faxes were being monitored. A computer centre was reportedly set up which carried out more "*politically focused*" intelligence gathering, including monitoring communications of opposition groups both within and outside Myanmar.[373] This timing coincided with exiles fleeing the country in the wake of the 1988 crackdown on the pro-democracy movement and setting up exile media groups, newsletters and websites to report on the situation inside Myanmar.

It has also been suggested that wiretapping of phone conversations was common, in particular to identify leaders of activist movements. Once leaders had been identified, this would be followed up with a night-time "*inspection*".[374]

Online surveillance

Despite Myanmar's low Internet penetration, the Internet and its users were reportedly under near constant surveillance as the first Internet connections were established around the year 2000. For citizens wanting an email account, the only choice was to pay for an email account supplied by Myanma Post and Telecommunications (MPT), a state run telecommunications company. Users assumed these accounts were closely monitored. However, it is difficult to establish exactly what technology enabling online surveillance was purchased and utilised by the government.[375]

---

[371] Fortify Rights, "Midnight Intrusions: Ending Guest Registration and Household Inspections in Myanmar" (2015), pg 12.
[372] A 2007 Human Rights Watch report found the local ward Peace and Development Councils, the Union Solidarity and Development Association (a movement supporting the military government, disbanded in 2010) and Swan Arr Shin (a local paramilitary group) all contributed informants who conducted surveillance activities and gathered intelligence. Human Rights Watch, "Crackdown. Repression of the 2007 Popular Protests in Burma" (2007), pg. 83.
373 Brian McCartan, "Myanmar on the Cyber-Offensive" *Asia Times* (1 October 2008).
[374] Fortify Rights, "Midnight Intrusions: Ending Guest Registration and Household Inspections in Myanmar" (2015) pg. 31.
375 See for example: Joe Havely, "When States Go To Cyber-War" *BBC News Online* (16 February 2000). The BBC reported that the government had acquired surveillance capabilities by borrowing equipment from other countries: *"Using monitoring equipment loaned by the government of Singapore, analysts say the junta has been able to track online critics of the regime."* A 2005 Open Net Initiative report on internet filtering in Myanmar also mentions online surveillance, reporting that the state *"maintains the capability to conduct surveillance of communication methods such as email…"* Open Net Initiative, "Internet Filtering in Burma in 2005: A Country Study" (2005), pg. 4. A 2007 Berkman report stated that the military government was buying surveillance technology from an un-named U.S company. Chowdhury, M. Berkman Centre for Internet and Society at Harvard University, "The Role of the Internet in Burma's Saffron Revolution" (2008) pg. 13.

Although the Internet penetration in the 2000's was less than 1%, activists were quick to make use of the limited service they had. Despite pervasive surveillance, the 2007 Saffron Revolution came to global attention thanks largely to activists anonymously uploading images and video to websites such as YouTube, which were then picked up by international news agencies, as journalists were prevented from entering the country. Some managed to email images to friends outside Myanmar to upload onto sites such as the Democratic Voices of Burma (DVB), or smuggle content out of the country on USB sticks. This was the first time in the country's history that ICTs played a significant role in disseminating information about protests and the security forces' violent suppression of such protests. In addition, the 2009 documentary Burma VJ[376] featured some of the video footage and images, and revealed that many of the activists involved had either been arrested and punished, or fled Yangon.

Surveillance of Cybercafés

Public Internet access inside Myanmar was previously only possible from a few Internet cafes in Yangon and Mandalay, the two largest cities. The first cybercafé opened in Yangon in 2002[377]. From around 2006, cybercafés required a license to operate from the Myanmar Information Communications Technology Development Corporation (MICTDC). They were licensed as Public Access Centres (PACs) managed by Myanmar Info-Tech, a state-owned company. Regulations[378] stated that users had to register at the cybercafé before accessing the Internet and café owners had to take screenshots of user activity every five minutes, delivering CDs containing these images to MICTDC at regular intervals.

In 2008, the Open Net Initiative reported: "*Anonymous Internet use is impossible; cybercafé licences require that patrons register their name, identification number, and address to gain access. Opportunities for anonymous communications are further hampered by the state's ban on free email sites such as Hotmail and Yahoo! mail."*[379]

[376] Anders Østergaard, *Burma VJ: Reporting From A Closed Country* (2008). Among other awards, the film was nominated for the Academy Award for Best Documentary Feature in 2010.
[377] Reporters Without Borders, "Internet Under Surveillance 2004- Burma" (2004).
[378] "Public Access Center Regulations by Myanmar Info-Tech" (2006). See an unofficial English translation by the Open Net Initiative (ONI), which includes a link to the original version in Burmese.
[379] Ibid, pg. 11

Surveillance since the 2011 Reform Process

Little is known about intelligence gathering practices in Myanmar since 2011.[380] It is believed that at least two intelligence agencies are still operational – the Military Affairs Security (MAS) and the Special Branch of the Myanmar Police Force[381] . In 2011, *Irrawaddy* reported that a new intelligence unit had begun to operate, staffed by military and police officers. It was reported that the new unit would not operate as a separate entity, as intelligence agencies had previously done, and had to reports to "*both military and civilian authorities, as well as administrative officials*". According to the report, the role of the unnamed intelligence unit was to *"investigate the movements of political parties, ethnic armed forces and cease-fire groups, violent domestic actions such as bomb explosions and any matter that affects the state's security and stability, including non-disintegration of the military, and take necessary measures*."[382]

It is unclear which elements of the surveillance apparatus are still operational, but it appears that authorities are still conducting a combination of physical and electronic surveillance by replacing old laws with something very similar, and utilising new technology. For example, in 2011, Reporters Without Borders reported that new updated regulations had been sent to cybercafé owners, *"including a requirement to keep the personal data of all their clients along with a record of all the websites they visit, and make it available to the authorities."*[383]

In 2012, *The Village Act* and *The Town Act* was replaced by The *Ward or Village Tract Administration Law,* which upholds the process of overnight guest registration and inspection. Although inspections have reportedly declined, and more people are ignoring the law as there are no longer the same fears of reprisal, there have been recent crackdowns on student protesters, forcing many to go into hiding.[384] Student's houses have reportedly been "*inspected*" in the middle of the night, had their mobile phones seized and their Facebook accounts hacked.[385]

Reports suggest that surveillance of community leaders, opposition political party members and journalists continue. Some reported being physically followed or enquired after, and some fear their phone conversations are monitored.[386] In 2013 it was reported that the website of the Myanmar news group Eleven Media, was under surveillance. One of its journalists was physically followed by intelligence agents while reporting on the war in Kachin State.[387] Journalists from Eleven Media and others working on Myanmar reported they had received notification from Google, which runs the Gmail email service,

---

[380] Andrew Selth, "Burma's Security Forces: Performing, Reforming or Transforming?" *Griffith Asia Institute, Griffith University, Australia* (2013), pg. 16.
[381] The Hindu, "In Myanmar, Internal Spy Network Lives On" *Associated Press report* (30 July 2013).
[382] The Irrawaddy, "Burma Forms New Intelligence Unit" (3 May 2011).
[383] Reporters Without Borders, "Surveillance of Media and Internet Stepped Up Under New Civilian President" (2011).
[384] Wa Lone and Guy Dinmore, "Student Activists Go Into Hiding After Crackdown" *The Myanmar Times* (20 March 2015).
[385] Ibid
[386] Andrew Selth, "Burma's Security Forces: Performing, Reforming or Transforming?" *Griffith Asia Institute, Griffith University, Australia.* (2013), p17.
[387] Bertil Lintner, "The Military's Still In Charge" *Foreign Policy* (9 July 2013).

that their accounts may have been hacked by "*state-sponsored attackers*".[388] It is unclear if the purpose of these attacks were to gain access to journalist's emails and identify sources, or to stem the flow of information to and from Myanmar. It was also reported that government agents visited cybercafés to "*install some software*", widely believed to be 'keylogging' software, which records and stores keystrokes for later analysis. Some café owners have put up signs warning customers not to use the Internet for "*political reasons*".

It is also unclear what kind of relationship Myanmar's existing intelligence agencies have with foreign counterparts, and what kind of intelligence exchange agreements exist. It is thought that Embassies routinely reported on the activities of the diaspora.[389]

The Legal Framework in Myanmar

There are currently few protections in Myanmar's legal framework to prevent the kind of pervasive surveillance previously conducted by intelligence agencies and about which there is justifiable concern. It is unclear under which legal regime the existing intelligence agencies are operating, what their remit is and how they are exercising their powers. Although Article 357 of the 2008 Constitution does provide for privacy[390], there are no privacy protections in national legislation. The existing legal framework referring to surveillance is vague. Article 75 of the 2013 Telecommunications Law [391] grants unspecified government agents the authority *"to direct the organisation concerned as necessary to intercept, irrespective of the means of communication, any information that affects the national security or rule of law".* Although the clause adds this should be undertaken without impacting the fundamental rights of citizens, there are no further details on the process or privacy protections.

Most states have a specific legal framework in place to govern instances where interception of communications is permitted in real time (lawful interception). However Myanmar currently has no specific legal framework or regulations governing lawful interception, leaving an important gap in the regulatory framework. The MCIT has confirmed its interest in developing a law in accordance with international standards. It has committed to a public consultation of draft lawful interception regulations.[392] One of the current telecommunications operators, Telenor, has stated publicly that they will not respond to any interception requests from law enforcement officials until the legal framework is in place.[393]
The EU has agreed to provide technical support to the Government to develop its regulations in line with human rights. The programme of work will come within the Council

[388] Thomas Fullller, "E-Mails of Reporters in Myanmar Are Hacked" *New York Times* (10 February 2013).
[389] Andrew Selth, "Burma's Security Forces: Performing, Reforming or Transforming?" *Griffith Asia Institute, Griffith University, Australia* (2013), pg. 18.
[390] "*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.*"
[391] See unofficial English translation of the Myanmar *2013 Telecommunications Law*.
[392] In November 2013, MCIT published draft proposed rules, stating: *"The Ministry will be drafting other rules and procedures on a variety of issues such as standardization, type approval, and lawful interception in due time. Such rules and procedures also will be subject to a public consultation process."* MCIT, "Proposed Rules for Telecommunications Sector Relating to Licensing, Access and Interconnection, Spectrum, Numbering, and Competition" (4 November 2013), Section I, B5 (pg. 5).
[393] Telenor, "Myanmar sustainability presentation" (19 August 2014), pg. 8 of the transcript.

of Europe programme on cybersecurity, particularly focused on the Council of Europe Convention on Cybercrime.[394] Regulations are needed to govern the use of surveillance to ensure any infringement of privacy rights is legal, necessary and proportionate and the act of surveillance is not abused to cover people who are not suspected of carrying out a crime but whom the government may disagree with.

The Government has already committed to requiring judicial authorisation of any request for lawful interception, which is an important first step. Given the weak state of the Myanmar judiciary, it is clear that any judicial authorities involved in such authorisation processes will require thorough training, both in the technicalities of lawful interception, but also in the importance of the legal safeguards that an independent review represents. See Chapter 4.9 on Stakeholder Engagement and Access to Remedy for a short overview of the judiciary.

The idea of a judicial authority challenging and even denying authorisation to the executive branch to carry out surveillance for what the government claims is a national security issue or emergency, will be an unfamiliar concept in Myanmar. Even in countries with highly developed judicial systems, there is little open scrutiny of the decisions made by judicial authorities on lawful interception. The challenges of establishing a gatekeeping system in Myanmar that respects rights and establishing a proportional, targeted approach to security are therefore significant. The companies involved in executing lawful interception requests may currently be one of the few credible counterpoints in the system. (See Section C providing Surveillance Recommendations for ICT Companies) The Annex to the Recommendations also suggests the main issues for the Government of Myanmar to take into account in developing lawful interception law and procedures.

B. Field Research Findings

Current Status of Lawful Interception in Myanmar

Human Rights Implicated: Right to Privacy, Freedom of Expression

Key Findings

- Many people in Myanmar **grew up under a repressive surveillance regime**, and are familiar with methods of physical surveillance, such as being followed. However, the majority do not know how digital surveillance is carried out and who has access to their data, phone records, etc.
- There is a prevailing **lack of trust** between the public and the government, as well as a belief that the government will not protect or respect citizens' privacy or personal data. There is a feeling among the general public that there is still physical surveillance and that government agencies likely monitor their digital communications.
- There is **no oversight body** (parliamentary or otherwise) for lawful interception, and no clear process in place.
- **There is currently a lack of legal framework for lawful interception:** In May 2015 with support from international consultants, MCIT held an initial "*fact finding*" session, focused on cyber-crime and electronic evidence, in which MCRB participated. The next steps are unclear. In the interim, PTD has requested

[394] Council of Europe, *Convention on Cybercrime* (CETS 185) (2001).

operators comply with requests for data in cases related to human trafficking, terrorism, and drug offenses.

- There are **inconsistent policies for handling data requests from law enforcement.** One operator mentioned that they have an in-house policy regarding lawful interception, allowing them to provide data to the government in serious criminal cases. This operator has a specific department for lawful interception to review requests. Requests must have an authorised signature of Ministry of Communications Information Technology to be reviewed by the operator before providing any data.
- A mobile network operator's regional office noted that little scrutiny is applied when law enforcement requests location data or call records. The information is usually provided.
- One operator has designated **a small internal team** to review the legitimacy of any data requests received from law enforcement.

C. Surveillance and Lawful Interception: Recommendations for ICT Companies

The following section focuses on the use of ICT for surveillance, rather than physical surveillance. (See also Chapter 4.3 on Privacy)

General

- **Understand Myanmar's history**: ICT companies that operate within those parts of the ICT value chain that may be subject to surveillance requests from the Government should understand the extensive historical level of surveillance in the country and its often severe consequences. The population and civil society organisations are therefore justifiably sensitive to the possibility of continued surveillance, and the current lack of appropriate legal safeguards on surveillance.
- **Understand the wider global discussion about surveillance**: Just as foreign companies coming into Myanmar need to understand the historical context around surveillance and its connotations for the population and its customers, local companies also need to understand the wider context of the active, on-going debate around surveillance and its implications for human rights.

Tower Construction

- **Be aware of the possibility of interception and misuse of base stations:** It is possible for other actors to intercept signals sent from cell towers by setting up technology that essentially pretends to be a base station and collects the information[395]. There is some evidence this being done elsewhere to locate activists and political opposition[396]. There are different types of hardware that can act as a base station and enable interception of mobile signals. The devices do not necessarily have to be in the vicinity of the cell tower or real base station to work. Tower

[395] One such example is an International Mobile Subscriber Identity (IMSI) catcher which works by masquerading as a base station, in order to track a mobile phone's location in real time. IMSI catchers are subject to export control in the US and EU.

[396] For example, during the 2014 Euromaidan protests in Ukraine, protestors in the vicinity of one march in the Ukrainian capital Kiev were sent unsigned text messages reading: *"Dear subscriber, you are registered as a participant in a mass disturbance".* Local mobile operators denied sending the message to their subscribers on behalf of the government, and one insisted that the messages were sent from a "*pirate base station*". Heather Murphy, "Ominous Text Message Sent To Protesters in Kiev Sends Chill Around The Internet" *New York Times* (22 January 2014).

construction companies should therefore be aware that their infrastructure may be targeted by actors wishing to illegally intercept mobile phone signals for the purposes of surveillance, impacting both freedom of expression and privacy. When tower construction companies carry out their regular checks and maintenance, they should therefore be especially vigilant for any signs that cell tower or base station equipment has been tampered with.

Infrastructure

- **Do not provide lawful interception services until a legal framework is in place:** Lawful intercept solutions provided as part of the network infrastructure of operators should not be operational until national legal framework and regulations are in place and it is clear which set of technical standards Myanmar will adopt (ETSI standards or another). Without legal safeguards in place, companies requested to take action by the government to action lawful interception may be contributing to human rights violations of the right to privacy and potentially further severe impacts, depending on the action taken by the government once it has secured the information. Vendors should be prepared for such requests and consider through their due diligence processes the human rights risks associated with these transactions. This includes due diligence pre-sale, during the sale in putting appropriate conditions or procedures in place in sale documents or contracts, and in post-sale due diligence.[397]
- **Train operator personnel:** In addition to carrying out the appropriate due diligence, vendors should ensure that equal attention is given to training of operator personnel as part of the sale of technology products, including lawful interception systems. Myanmar staff may not be informed or even consider the wider implications of their actions unless they are provided with specific training.
- **Send clear messages about business relationships**: The opening of the Myanmar ICT market has seen a rush of new companies to the market. Unlike other bigger footprint sectors, smaller ICT companies have far fewer downside risks in entering and exiting markets quickly. Some of the companies selling unregulated surveillance technology market themselves by asserting that their technology can be added to a particular vendor's network as lawful intercept 'solutions' when in fact they provide capabilities that go well beyond what is lawful. Network vendors should publicly distance themselves from these companies, ensuring that their company's logo and name are removed from any marketing literature by such enterprises and by providing a clear message to the Government that they do not condone such products.

[397] See for example guidance on dealing with government requests: European Commission,"ICT Sector Guide on Implementing the Corporate Responsibility to Respect Human Rights" (2013), pg. 32-33. IHRB, "Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems. Case Study: Ericsson" (2014).

Telecommunications Operators

- **Challenge lawful interception requests without appropriate legal safeguards**: Operators are the party in the ICT value chain that receives any request from the government for interception of the content of phone calls and emails, or access to other information such as user/subscriber information and records. As noted above, Article 75 of the *2013 Telecommunications Law* includes a sweeping provision on surveillance. Subsequent regulations for assistance with real time surveillance are not in place. One of the current telecommunications operators, Telenor, has stated publicly that they will not respond to any interception requests from law enforcement officials until the legal framework is in place.[398]. Even when such regulations are in place and even assuming that they are aligned with international law, given the history and current state of development of Myanmar's judiciary, the operators may be one of the few credible actors in the process capable of challenging overly broad or inappropriate requests.
- **Develop robust systems for responding to government requests** to avoid over-complying with illegal requests.[399] Such a company system could include for example, ensuring that there is a process in place to review each request submitted; a designated contact person in the company; a list of government departments authorised to request information; a requirement that the request to the company must be made in writing (or at least followed up in writing if such a request is made during the course of an emergency); challenging requests that do not comply with the law or human rights standards; developing criteria for escalation of requests; and where feasible, notifying affected customers or users. See the Annex to the Recommendations for further information.
- **Be transparent about the number of requests for surveillance:** Out of three telecommunications operators in Myanmar, only one telecommunications operator issues a transparency report disclosing interception requests from law enforcement, including cases the company has complied with.

'Over the Top' Companies (National and International)

- **Challenge requests for user information without appropriate safeguards:** Like telecommunications operators, over the top companies which store data on servers inside Myanmar need robust systems for screening and responding to such requests to ensure that they do not contribute to potential human rights violations. [400] While certain information about a user may be publicly accessible, for example by looking at a public profile on social media, companies store much additional personal information about their users, such as names, addresses, contact numbers and private online conversations. Depending on the service, companies will also have a lot of information about a person's movements, how they spend their time and money and the opinions they hold, which could potentially be used in gathering intelligence. Over the top companies may also be requested to turn over user information by the Government as part of its surveillance activities.

---

[398] Telenor, "Myanmar sustainability presentation" (19 August 2014), pg. 8 of the transcript.
[399] See for example guidance on dealing with government requests: European Commission, "ICT Sector Guide on Implementing the Corporate Responsibility to Respect Human Rights" (2013), pg. 44-45 and the Telecommunications Industry Dialogue.
[400] See for example guidance on dealing with government requests: European Commission, "ICT Sector Guide on Implementing the Corporate Responsibility to Respect Human Rights" (2013), pg. 44-45 and the Global Network Initiative (GNI), "Principles and Implementation Guidance" (last accessed August 2015) on dealing with government requests.

- **Establish clear company terms of service** which are understandable to local users, setting out what information the company collects and stores and under what legal justification that information can be accessed by the government.

Software

There are many different kinds of software, but the focus of this chapter is the tools that can aid surveillance; that is, the software that can be added to a telecommunications network in order to increase surveillance capabilities.

- **Do not sell surveillance software to Myanmar.** Surveillance software is not a new issue for Myanmar. As far back as 2000 it was reported that Burmese exiles were being targeted with malware. However, this kind of technology has advanced rapidly in recent years. While the goal of the military government in the 2000's may have been to stop information exchange or communication by freezing computers or taking websites offline, viruses, malware and spyware contained in infected emails are now capable of doing much more intrusive surveillance. Companies selling surveillance equipment, whether 'off the shelf' or bespoke services are under particular scrutiny due to the clear implications for human rights.[401] Sellers of such technologies often justify their use by saying they are intended to support law enforcement or protect the public welfare (e.g. through protecting against terrorist activity), but they often can also be used to facilitate human rights violations by the purchasers. There are currently debates in Europe about tightening export controls to restrict the kinds of surveillance technology that can be exported, particularly to governments with a poor human rights record.[402] Due to the lack of legal framework around surveillance, interception and privacy protections, Myanmar should be a no-go area for companies selling surveillance technology.[403]

D. Relevant International Standards on Surveillance and Lawful Interception

Relevant International Standards:

- International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles) 2014

Relevant Guidance:

- Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance (2015)
- Electronic Frontier Foundation (EFF) Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes (2012).

[401] See commentary by the Chair of the OECD Working Party on Responsible Business Conduct, "Responsible Business Conduct in Cyberspace" (30 April 2015).
[402] For example, the Stockholm International Peace Research Institute (SIPRI) is working on a data collection program in support of the European Commission's ongoing impact assessment for the review of the EU dual-use regulation.
[403] For more guidance, see Tech UK "Assessing CyberSecurity Export Risks" (2014).