ANALYSIS OF THE PROVISIONS OF THE DRAFT CYBER SECURITY LAW

This analysis of the draft CyberSecurity Law (Myanmar draft dated 6 February 2021, Unofficial EN Translation MCRB 12 Feb) identifies a number of serious problems with the draft including, but not limited to, its impact on the right to privacy (Section 357 of Myanmar's Constitution), and well as vague/wideranging provisions which impact on the right to Freedom of Expression (Section 354). Other organisations are welcome – and indeed encouraged - to make use of the analysis in their advocacy on the draft law. This analysis is for general informational purposes only and is not intended to constitute legal advice.

Reference	Provision	Analysis and Conclusion
Chapter V Section 10 (k) read with Chapter X Section 33 and 34	<u>*Section 10 (k)*</u> *The responsibilities of the Steering Committee shall be as follows:* *To approve or decline to issue the license to service providers prescribed in this Law and take any necessary actions in accordance with the policies, strategies, work plans, and frameworks*. <u>*Section 33:*</u> *Any person wishing to render Cybersecurity services within the Union of Myanmar shall apply to the Department in accordance with the stipulations in order to secure the license.* <u>*Section 34:*</u> *Any person wising to render online services within the Union of Myanmar shall register with the Department in accordance with the stipulations.*	A. Cybersecurity Services Provider means any "*online service provider or any cybersecurity service provider using systems or materials similar to cyber resources related to information technology systems."* B. Online Service Provider *"means a person or business which provides Online Services used in Myanmar."* C. The definitions of both cybersecurity service provider and online service provider have broad interpretation and includes a host of services as may be construed from the definitions. D. The present version of the Draft Cyber Security Law provides for a separate licensing framework for issuance of licenses for such kinds of services. <u>*Conclusion*</u> The law appears to require the licensing and governmental approval of cybersecurity service providers and online service providers. This may generally be unprecedented in a Draft Cyber Security Law and be coined as particularly regulated. Especially since, internet service providers as defined under the Telecommunications Law are approved in any case by the Posts and Telecommunications Department. However, the Draft Cyber Security Law, has a very broad definition of Online Service Provider which may extend to beyond what is contemplated under the Telecommunication Laws. Thus, if general online services also need licensing, it may be deemed to be restrictive/time-consuming and regulative.

Chapter VI Sections 13, 14 and 15	<u>*Section 13*</u> *A Personal Data Holder:* *a) Shall systematically maintain, protect, and manage the data concerned subject to the type of data and confidentiality level in accordance with the law;* *b) Shall not carry out the following other than with the permit under any provisions of any existing laws or approval of the owner of such personal data: allow any persons or organizations to scrutinize the personal data that are under his or her administration; disclose, notify, distribute and send such data to any persons or organizations; alter, delete, copy, and submit any personal data as evidence;* *c) Shall not use any personal data for administrative purposes that are not consistent with the objective; and* *d) Shall systematically delete personal data, which are collected with the aim to use them within the limited period, when a valid period for using them is over.* <u>*Section 14:*</u> *An investigation team that receives the information including personal data under any existing law or a person assigned by this team or under a direction thereof shall keep such information as confidential other than needing to disclose them subject to the law.* <u>*Section 15:*</u> *The following activities shall not be applicable to the management of the personal information:* *a) Submission of any evidence to the court, prevention, investigations, and detection by the government departments, investigation teams or regulatory bodies*	A. Personal Data under the Draft Cyber Security Law *means any information which has been or could be used to identify a person*. B. Personal Data Holders need to protect all personal data and manage such data maintaining a high level of confidentiality. Transfers/distribution of personal data is barred without receiving consent/approval from the owner of the data under Section 13. C. However, upon a reading of Section 14, it may be interpreted that the investigation team (governmental authority) can receive the personal data in accordance with law without any need for a consent or a warrant/sanction from a judicial body of competent jurisdiction. D. Therefore, the provision fail to stipulate or provide for any conditions under which personal data may be transferred to the investigation team. This may be considered to be a loss of privacy in so far as distribution/transfer of personal data to the investigation team is concerned. E. There is not enough statutory data protection given to personal data. However, there is a wide carve-out given under Section 15 with provisions to government activities on search, investigation, evidence, and other law enforcement sector activities where the management of personal data shall vest entirely with the governmental authorities. <u>*Conclusion*</u> This provision may be considered as restrictive of the citizen's privacy rights under the Privacy Law 2017 which states that "*every citizen has the right to enjoy the protection of his/her privacy*" and the Constitution of Myanmar ("Constitution") states that the Union shall be responsible to protect the privacy of its citizens.

	assigned duties by the Central Committee in respect of Cybersecurity, Cyber-attacks, Cyber-terrorism, Cyber Misuse, Cyber Incident and Cybercrimes; *b) Any detection, inspection, collection of news, litigation and submission of the evidence to any court conducted by the government departments, investigation teams, or regulatory bodies assigned the duties by the Central Committee according to criminal cases;* *c) Any detection, inspection, collection of news and coordinating of information that are conducted according to the relevant Cybersecurity and Cybercrime related cases if such cases impact the country's sovereignty, stability and peace; and* *d) The administrative power shall be determined by the Central Committee or Related Ministry or Department in the course of administrating the cases prescribed in sub-section (c).*	Considering the wide scope of the provisions, the management of personal data for an enlarged scope of enforcement activities vests with the governmental authorities where personal data would necessarily need to be transferred to the governmental authorities.
Chapter VII Sections 16, 17 and 20	*Protecting Critical Information Infrastructure* *<u>Section 16:</u>* *The Critical Information Infrastructure shall be as following:* *a) e- Government Services,* *b) Electronic information and infrastructure related to finance;* *c) Electronic information and infrastructure related to water resources;* *d) Electronic information and infrastructure related to transportation;* *e) Electronic information and infrastructure related to communication;* *f) Electronic information and infrastructure related to public health sector;* *g) Electronic information and infrastructure related to electricity and energy;* *h) Electronic information and infrastructure related to natural resources; and*	A. Section 16 gives the definition of Critical Information Infrastructure as decided and designated by the government authorities. B. Further, under Section 17 it may be interpreted that unfettered power is given to the governmental authorities under which the governmental authorities may amend the list of the Critical Information Infrastructure as from time to time. C. In accordance with this chapter, the governmental authorities may lay down policies <u>for the storage and maintenance of the facts and information</u> that are related to the Critical Information Infrastructure. D. Most importantly, under Section 20, *the person responsible for the processing and maintaining of the Critical Information Infrastructure, shall keep the facts and information that are related to the Critical Information Infrastructure, at the place determined and approved by the Ministry*. Therefore, the effect of this is two-pronged- all such critical information (deemed to be) shall be kept inside Myanmar and such data may have unrestricted access by the governmental authorities.

	i) Electronic information and infrastructure that are not related to the public. <u>*Section 17:*</u> *The Central Committee shall:* *a) May amend the list of the Critical Information Infrastructure as necessary with approval from the State Administration Council;* *b) Shall direct the Ministry to inform about any stipulation and amendment of the list of the Critical Information Infrastructure, that is prescribed according to the relevant sector, to the person who is responsible for processing and maintaining of the Critical Information Infrastructure of the Related Ministries and government organization; and* *c) Shall set out the policies for the storage and maintenance of the facts and information that are related to the Critical Information Infrastructure.* <u>*Section 20*</u>*:* *The person responsible for the processing and maintaining of the Critical Information Infrastructure:* *a) Shall keep the facts and information, that are related to the Critical Information Infrastructure, at the place determined and approved by the Ministry;* *b) Shall distribute, issue, send, receive and keep the facts and information that are related to the Critical Information Infrastructure in accordance with the stipulations; and* *c) Shall submit the Cybersecurity report to the Related Ministries at least once a year.*	<u>*Conclusion*</u> The entire mechanism of what constitutes 'Critical Information Infrastructure' and the government's free role in its determination and control may be considered as restrictive of the fundamental freedom of privacy. Additionally, *Section 58* also seems like a very strict penalizing provision including imprisonment: "*If a person responsible to manage critical information infrastructure is convicted of failure to perform his or her duties under Section 20, he or she shall be punishable by an imprisonment for a term not exceeding 3 years or a fine not exceeding MMK 100 lakhs or both.*
Chapter IX Section 28 Chapter X Section 34	*Definitions:* *Online Service Provider "means a person or business which provides Online Services used in Myanmar."* *Online Services means "any activity which provides a service online using Cyber-Resources or similar systems or materials.*	A. The definition of Online Services (any activity where service is provided online using the cyber/internet space) under the Draft Cyber Security Law is broad enough to capture many forms of general online services. B. Online Service Providers, will need to register as a company under the Myanmar Companies Law as per Section 28 (b) and also pay relevant taxes

	Cyber Resources refers to "the computer, computer system, computer program or program, network, communication tools, facts, and data. *<u>Section 28:</u>* *The Online Service Provider within Myanmar shall carry out the following:* *(a) The device, that stores the information of service users, shall be kept at the place designated by the Ministry;* *(b) The online service shall be registered in accordance with the Myanmar Companies Law; and* *(c) Taxes must be paid in accordance with the provisions of the relevant laws if it is mandatory to do so in respect of any business conducted through the online service provider or similar profitable business.* *<u>Section 34:</u>* *Any person wising to render Online Services within the Union of Myanmar shall register with the Department in accordance with the stipulations.*	as per Section 28 (c). Also, a license would need to be obtained under Section 34. C. Importantly, under Section 28 (a), the device that stores the information of service users will need to be kept at the place designated by the Ministry. The effect of this is two-pronged- all such critical information (deemed to be) shall be kept inside Myanmar and such data may likely have unrestricted access by the governmental authorities. <u>Conclusion</u> The ambit and definition of Online Service Providers is very wide and if the law, in its present form, is enforced, it would need a separate licensing/registration procedure under the Draft Cyber Security Law.
Chapter IX Section 29	*<u>Section 29:</u>* *When the Department informs that Online Service Provider causes any of the following events in the Cyberspace within the Union of Myanmar, they shall be prevented, removed, destroyed and terminated in line with the stipulations:* *a) Speech, texts, images, videos, audio, files, signs or other means of expressions that lead to hatred, and destroy unity and peace;* *b) Fake news and rumors;* *c) Sexually oriented pictures, audio files, videos, phrases, signs or any other illustrations that are not in line with the community's culture;* *d) Child pornography, pictures, phrases, signs or any other illustrations; and*	A. The analysis of the provision from a legal perspective is as follows: This provision may be considered to be restrictive of fundamental freedoms guaranteed under the Constitution. Article 354 (a) of the Constitution states that "*every citizen shall be at liberty in the exercise of the following rights, if not contrary to the laws, enacted for Union security, prevalence of law and order, community peace and tranquility or public order and morality: <u>to express and publish freely their convictions and opinions</u>…*" B. The Constitution guarantees every citizen fundamental freedom of expression to publish freely their convictions and opinions. The said provision of the Draft Cyber Security Law may be considered to be restrictive and gives the Department unrestrictive powers to curb the freedom of expression. The Department (at its discretion without any

	e) Written statements, speeches or descriptions that infringe any existing laws	formal proceeding/finding) has the power to notify Online Service Providers to <u>prevent, remove, delete and suspend</u> content. C. The content includes (among others), *speech, text, picture, video, voice file, symbol or any other depiction that can cause hatred, disunity and affecting stability.* Thus, wide powers vest with Department to deem any content as depiction which can cause *hatred, disunity and affecting stability* without a systemic fact finding proceeding. D. Further *fake news and rumours* have not been defined and thus can deemed to be vague and unsubstantiated content where any form of dissatisfaction towards a government policy/rule/action can be deemed as *fake news and rumour,* thus once again giving the Department arbitrary powers. E. In terms of *sexual images, voice file, video, text, symbol and any other depiction that are inappropriate for Myanmar culture and Myanmar society,* there is no specific definition of Myanmar culture and/or society and practically speaking such terms are very subjective. There are many instances where sexual images or voice files (such as an emoji for instance) do not in effect tantamount to any offense/inappropriate, however, there is a wide discretion on the Department for interpretation. F. *Further written statements, speeches or descriptions that infringe any existing laws* can be considered to be any comments/analysis (regardless of its correctness or accuracy) of a draft law or an enacted law. The Department has the authority to request service providers to take down such content. <u>*Conclusion:*</u> The entire Section 29 seems to be giving arbitrary/excess powers to the Department to require the Internet Service Providers to <u>prevent, remove, delete and suspend</u> content which in turn may be interpreted to restrict the fundamental freedoms provided under the Constitution.

Chapter IX Section 31	*An Online Service Provider in Myanmar shall provide all or any part of the information prescribed in Section 30 upon the request of a person or organization assigned by any existing laws.*	A. Section 30 of the Draft Cyber Security Law requires Online Service Providers to store for three (3) years information of its users such as (username, IP address, telephone number, ID No. etc.). B. Upon being requested by the governmental authorities, the Online Service Provider will be required to provide all such information to the governmental authority. C. The governmental authority does not need to provide any reasoning or a warrant/sanction from a judicial body of competent authority to the Online Service Providers to share such information. <u>*Conclusion:*</u> Therefore, this provision may also be seen as a breach of privacy as the governmental authorities can obtain user information without providing any justification or valid sanction/warrant from a judicial body of competent authority.
Chapter XI Section 41 Chapter XII Sections 47 and 48	<u>*Section 41:*</u> *Interception made to a computer program or data by a person with any of the following methods shall be deemed an illegal interception:* *(a) If the person is not the authorised person for a specific computer system;* *(b) If the person is not the authorised one to decide whether to make the aforementioned interception or not;* *(c) If the person is not the one who has a permission from a responsible person to make interceptions for a specific computer system.* <u>*Section 47:*</u> *The State Administration Council shall grant the right to the relevant person or organization in order to intercept as prescribed in any existing law.* <u>*Section 48:*</u>	A. Under Section 41, the term 'authorised person' has not been defined under the Draft Cyber Security Law and thus there is a possibility that 'authorised person' may be deemed to be a 'person' or 'authority' as designated by the Committee/Department under the Draft Cyber Security Law. In such a case interception made to a computer program' by such person will not be deemed to be illegal. B. Further, sections 47 and 48 make interceptions by the government authorities legal and the companies and organizations are required to prepare and arrange for governmental authorities to intercept. C. The provisions are broad enough to include surveillance through any online devices and thus the government authorities may have the right to intercept a computer/a mobile phone or any such device without the knowledge or the consent of the owner of such data/device. However, there is no clear indication whether '*snooping*' would be a part of such interception. There is no express restriction under Draft Cyber Security Law either.

	The companies and organizations providing services as prescribed in the Telecommunication Law shall make arrangements and preparations in advance so that the relevant person or organization authorized under Section 47 can intercept.	<u>*Conclusion:*</u> In the above-mentioned provisions, the governmental authorities have been given a wide spectrum of powers to 'intercept' systems. The definition of *interception* means "*intercepting and acquiring of any information or part of it which is communicated and processed by using a network*." Therefore, it is pretty broad, but there is no indication/restriction on 'snooping' as part of the definition of 'interception'.
Chapter XII Section 49	<u>*Section 49:*</u> *A relevant person or organization authorized to intercept subject to Section 47 shall conduct any of the following interceptions without interfering the fundamental rights of the citizens:* *(a) Preventing any actions that can harm the sovereignty and territorial integrity of the State;* *(b) Performing any acts for the defense and security of the State;* *(c) Performing any acts for the rule of law and public order;* *(d) Investigating crimes;* *(e) Issues approved under any existing laws; and* *(f) Act of safeguarding and protecting public life, property and public welfare.*	A. In this provision, the authorised person (in order to prevent cyber-attack, cyber fraud, cyber terrorism) has the right to take a broad scope of action. B. This is especially true considering the broad scope of action under the provision which may be construed as providing unrestricted power to the authorised person. For instance, *preventing issues that can harm the sovereignty and territorial integrity of the State*- this has no defined boundaries or modes of steps to be taken by the authorised person. C. Further, *performing acts of state defense and security; performing acts of rule of law and public order*- there is no prescribed process/mode of action to be taken. <u>Conclusion:</u> Similar to the above analysis, there is a possibility that the governmental authorities may carry out any form of interceptions for the stated reasons which are also undefined and open-ended.
Chapter XII Section 50	<u>*Section 50:*</u> *A Related Ministry or a department and organization which is assigned by the Ministry may investigate, and supervise any services being operated and processed at the online service provider and may request them to provide written records if it is necessary for the country's protection and security purposes and public interest.*	A. Section 50 enables the government to investigate the Online Service Provider at any time to access data for "*country's protection and security purposes and public interest*." B. The italicized phrase has no definition and can be widely interpreted. <u>Conclusion:</u> In the absence of any specified definition/limitation of the italicized term, Online Service Providers may be subjected to random inspections and investigations by governmental authorities.

Chapter XII Section 51	*In the event of requiring to act for the public interests, the Ministry can carry out the following with approval from the State Administration Council:* *(a) Temporarily prohibit any online service provider in Myanmar;* *(b) Temporarily control devices related to online service provider in Myanmar; and* *(c) Permanently terminate any online service provider in Myanmar.*	A. This clause may give the Ministry and the State Administration Council very wide powers. The term 'public interest' has not been defined and hence the garb of 'public interest' could be used to temporarily or permanently suspend the business of Online Service Providers. B. This provision may be interpreted to be beyond the realm of Section 77 of the Telecommunications Law which states: "*The Ministry may, when an emergency situation arises to operate for public interest, direct the Licensee to suspend a telecommunications service, to intercept, not to operate any specific form of communication, to obtain necessary information and communications and to temporarily control the Telecommunications Service and Telecommunications Equipment.*" C. Firstly, the Telecommunications Law describes a situation as an emergency condition existing and secondly makes such suspension in the temporary form to suspend a telecommunications service, to intercept, not to operate any specific form of communication. D. However, the Draft Cyber Security Law applies the temporary/permanent suspension not to any specific communication/s but of the complete business whereby the temporary or final ban can be given to the Internet Service Provider completely. The only justification to be given is 'public interest' which is not a defined term. <u>Conclusion:</u> For Online Service Provider, the above provision will apply and thereby there exist risks that governmental authorities may ask for the temporary or permanent stoppage of services due to 'public interest'.
Chapter XI Section 42	<u>*Section 42:*</u> *CCTV shall be installed in line with rules and regulations at places where many people are coming and going, public places, and places which need security.*	Section 42 creates a legal enabling provision for public location of CCTVs in public places which need security. <u>Conclusion:</u> Installation of CCTVs is not a cybersecurity issue and may be an issue of privacy and security which in that case should be under the Privacy Law.

Chapter XV Sections 61, 64, 65, 67, 70 and 72	*Offences and Penalties:* *Section 61: Online Service Providers who are convicted of failure to comply with provisions prescribed in this law shall be punishable for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.* *Section 64: Any person who is convicted of creating misinformation and disinformation with the intent of causing public panic, loss of trust or social division on a cyber space shall be punishable for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.* *Section 65: Any person who is convicted for creating a fake account, website and web portal with the intent of public panic, loss of trust or social division on a cyber space shall be punishable for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.* *Section 67: Any person who is convicted of buying and selling illegal currency such as digital currency, cryptocurrency on cyber space shall be punishable for a term not exceeding 3 years or a fine not exceeding 100 lakhs or both.* *Section 70: Anyone- with the intention of infringing state sovereignty, security, stability, rule of law, unity among ethnic groups- prevent others not to be able to use cyber resources, make the use of cyber resources difficult, attempt to penetrate the cyber network without permission, use more than allowed, put in the malware into computer with the intention of harming someone, shall be prosecuted under the Counter Terrorism Law.*	A. Section 61 of the Draft Cyber Security Law provides for a 3 year imprisonment for general non-compliance for Online Service Providers and the fine amount is MMK 100 lakhs. B. Section 64 makes it an offense for misinformation and disinformation with the intent of causing public panic, loss of trust or social division on a cyber space- this may be interpreted as *any social media news or disaffection towards the government* and arbitrary powers may be used to charge under this provision. Suggest a complete deletion of the provision. C. Similar to Section 64, Section 65 concerning fake news, and fake website and portal (without any formal definition) is open to interpretation and may give the authorities excess/ arbitrary powers to imprison any person based on this particular provision. D. The Central Bank of Myanmar (CBM) in its letter dated 3 May 2019 clarified that digital currencies such as cryptocurrency are not considered to be legal tender in Myanmar. The CBM to date has not issued any letter or notification which criminalizes or penalizes the usage of digital currencies. The CBM has just pointed out that transactional risks may be associated with the usage of such digital currency. The CBM may be the correct authority to penalize or criminalize the usage or transactions of digital currency and not the Ministry under this law. E. Section 70 in its interpretation and application can be deemed to be broad enough to include any act which may purportedly infringe state sovereignty, rule of law, unity, and stability of the Union by the usage of any cyber resource or network. The prosecution would take place under the Counter Terrorism Law where, based on the specific nature of the offense, the penalties may range from life imprisonment to death

	Section 72 states that the Department, with the approval of the Steering Committee, shall take any of the following actions against a violator who is convicted of failure to comply with Section 44 and 48: *a) Warning;* *b) Sentencing a fine;* *c) Temporary suspension of service provision within Myanmar for a particular term;* *d) Banning service provision within Myanmar or revoking the business license.*	penalty. Therefore, this particular provision may be deemed as excessive in its application especially since the nature of *infringing state sovereignty, security, stability, rule of law, unity among ethnic groups* is open to interpretation and may be interpreted in a broad manner to prosecute. F. With respect to Section 72, the Internet Service Providers who fail to cooperate/collaborate with the authorities (required under Sections 44 and 48 of the Draft Cyber Security Law) have a penalty that extends up to banning. This is again a seemingly restrictive provision penalty. <u>Conclusion:</u> The penalizing provisions of the Draft Cyber Security Law seem to be excessive and also include imprisonment terms.
Chapter V Section78 read with Chapter VI Section 89	<u>*Section 78:*</u> *Existing and Ongoing Electronic Identification Permit License (Digital Signature) Services, Online Services and Cyber Security related Services before the enforcement of this Law shall register and apply for the license in accordance with this law within one year from the date this law was enacted.* <u>*Section 89:*</u> *The Electronic Transactions Law (State Peace and Development Council Law No. 5/2004) is repealed by this law.*	A. Firstly, the Electronic Transactions Law has been repealed by this law and it is stated that licenses for electronic identification permit/digital signatures will be governed under the Draft Cyber Security Law. B. However, there is a lack of clarity on the entire regime of e-signatures/digital signatures, for instance what is the scope of e-signatures under the law, which are the documents on which e-signatures may be applied, are there any specific exceptions (for instance Section 5 of the Electronic Transactions Law), what would be the impact of previous documents which have been executed on the basis of the previous law. <u>Conclusion:</u> There exists a complete lack of clarity on such provisions and the effect of the application of the present draft in so far as all the aspects of the Electronic Transactions Law is concerned with respect to the use/operation of e-signatures and digital signatures. There is also a lack of clarity regarding whether e-signatures can be used freely or whether some form of certification will need to be given by the *Electronic Identification Permit License Holder.* It is also not clear what the functions of this license holder is under the Draft Cyber Security Law.

Chapter XVI Section 85	<u>*Section 85*</u> *The offences of this law are recognized as cognizable offenses and can be charged by the Myanmar Police Force.*	All the offences stated under the law have been made cognizable offenses and the police can charge and arrest without a warrant or a sanction from the court. <u>Conclusion:</u> There is a possibility of excess powers being used under this provision to arrest those purported to be non-compliant with the law. There is a possibility of misutilization of this provision and charging individuals arbitrarily under this provision.