យោបល់លើសេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យាព័ត៌មាន

Comments on the Draft Law on Cybercrime

ស្ថាប័ន៖ Name of Entity:	
ឈ្មោះ៖ Name:	
តួនាទី៖ Position:	
លេខទូរសព្ទ និងអ៊ីម៉ែល៖ Mobile and Email:	
កាលបរិច្ឆេទនៃការផ្តល់យោបល់៖ Date of Submission:	
ឯកសារយោង៖ Reference:	

អត្ថបទដើម **Original Text**	យោបល់ និងហេតុផល **Comments and Reasons**	សំណើកែលំអ **Proposal for Improvement**
Article 2: Scope This law applies to any cybercrime committed within or outside the territory of the Kingdom of Cambodia which infringes the security, public order, or interests of the Kingdom of Cambodia.	The terms "security," "public order," and "interests of the Kingdom of Cambodia" are overly broad and could lead to potential overreach or inconsistent application of the law.	Add terms "security," "public order," and "interests of the Kingdom of Cambodia" to Article 3.

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
Article 3: Definition 4. Unauthorized access means having no legal right, excuse or justification to access the whole or any part of a computer system	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 4. Illegal Access means a person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.
Article 3: Definition 6. Computer data means any representations of facts, information or concepts in a form that a computer system can process. This category includes texts, images, graphics, animation, symbols, audio, and video in digital or electronic form and any computer program that can cause a computer system to perform a function.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 6. Computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function
Article 3: Definition 7. Traffic data means any data related to communication using a computer system and generated by a computer system that forms a part of the chain of communication, indicating the communication's origin, destination, route, time, date, size, volume and duration, or	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	7. Traffic data means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
the type of service used for communication.		
Article 3: Definition 8. Computer system means an electronic device or a group of interconnected devices or related devices that perform automated data processing, including all types of devices capable of data processing, but not limited to desktop computers, laptop computers, and telephones.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 8. Computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data
Article 3: Definition 11. Computer data storage medium refers to any equipment or technology that can store computer data.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 11. Computer data storage medium refers to any article or material from which information is capable of being reproduced, with or without the aid of any other article or device
Article 3: Definition 12. Subscriber Information means any information contained in any form which establishes the subscriber's identity, such as name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity,	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 12. Subscriber Information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service;

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
including any temporarily assigned network address (including internet protocol address), and means and source of payment for such service (including any credit card or bank account number).		b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
Article 3: Definition 13. Seize means removing and retaining electronic devices or computer programs, making and retaining a copy of computer data directly on the premises, restricting access to the computer system or removing computer data in the accessed computer system, or taking a printout of the computer data output	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 13. Seize includes: (a) make and retain a copy of computer data, including by using on-site equipment; (b) render inaccessible, or remove, computer data in the accessed computer system; and (c) take a printout of output of computer data.
Article 3: Definition 15. Service provider means: − Any physical person or legal entity offering the users of its services the possibility to communicate using a computer system or telecommunication system. − Any other physical person or legal entity processing or storing	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 15. Service provider means: (i) Any public or private entity that provides to users of its service the ability to communicate by means of a [computer system OR information and communications technology device]; and (ii) Any other entity that processes or stores [computer data OR digital information] on behalf of such a communications service or users of such a service;

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
computer data for the persons or entities mentioned in the above paragraph or for the users of services offered by these persons or entities		
Article 3: Definition 17. Child pornography refers to any image that is transmitted through information technology, such as photos, video, animation, and audio, including electronic material that describes child pornography or depicts any act or activity involving a sexual organ or any part of the body of a child by any means, or other similar pornography of a child that stimulates sexual desire or causes sexual excitement	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 17. Child pornography shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct
Article 3: Definition 18. Cryptocurrency is a digital or virtual currency designed to work as a medium of exchange that uses strong cryptography to secure financial transactions and verify the transfer of assets. Cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems.	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See the U.S. Department of Commerce National Institute of Standards and Technology definition of cryptocurrency: https://csrc.nist.gov/glossary/term/cryptocurrency	Article 3: Definition 18. A digital asset/credit/unit within the system, which is cryptographically sent from one blockchain network user to another. In the case of cryptocurrency creation (such as the reward for mining), the publishing node includes a transaction sending the newly created cryptocurrency to one or more blockchain network users. These assets are transferred from one user to another by using digital signatures with asymmetric-key pairs.

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
Article 3: Definition 19. Cybercrime refers to the use of information technology to harm computer systems, computer data, websites, and/or technology, or to harm or commit crimes against individuals or entities, whether directly or indirectly through the use of computer systems, computer data, or information technology	Definitions should adhere to multinational standards in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 3: Definition 19. Cybercrime is not a defined legal category, but includes: (a) offences aimed at computers, computer or communications systems, their users or the data they contain; and (b) more traditional offences committed using these systems, especially if technologies have significant effects on how the crime is committed or investigated
Article 5: Competent authority to investigate cybercrime Where necessary, judicial police officers in charge of anti-cybercrime may collaborate with national or international technical experts to investigate said offenses.	International cooperation on cybercrime carries significant risks, including the potential for surveillance abuses to be outsourced to foreign entities, thereby circumventing domestic legal restrictions and oversight mechanisms. This not only undermines the sovereignty of Cambodia by allowing external actors to exert influence over its surveillance practices but also poses a threat to the privacy and civil liberties of its citizens. Such cooperation can lead to a situation where the host country leverages the resources and authorities of third-party nations to conduct surveillance on its own population, effectively bypassing national safeguards designed to protect individual rights. This erosion of sovereignty and privacy underscores the need for stringent legal frameworks and due process protections to govern international cybercrime collaborations, ensuring that they do not become a conduit for expanding the surveillance state.	Where necessary due to imminent security threats, judicial police officers in charge of the anti-cybercrime unit may collaborate with national or international technical experts to investigate said offenses, provided such collaboration is approved by a judge, limited in time and scope, and conducted with appropriate notice to relevant parties unless such notice would jeopardize the investigation.

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
Chapter 3: Obligation and Responsibility of Service Providers (Articles 8-10)	Lacks specific safeguards for data protection, user privacy, and transparency in data access. Key issues include broad authority for data access, insufficient detail on data protection measures, lack of transparency requirements, no provisions for data breach notification, and unclear limits on cooperation with law enforcement.	Add a new Article 11 titled "Data Protection and Transparency" that requires implementation of strong data security measures including encryption; access to data only with a valid court order; maintenance of access logs and annual transparency reporting; 72-hour data breach notification (GDPR); appointment of data protection officers; user notification of data access unless prohibited; regular security audits and data minimization practices; and clear limits on cooperation with law enforcement.
Article 10: Confidentiality Service providers shall maintain the confidentiality of computer data, traffic data and subscriber information as stipulated in this law unless authorized by a court order	Additional detail is needed in this section may be warranted. The cybercrime law should attempt to enhance the defensive cybersecurity posture of all technology systems in Cambodia.	Article 10: Confidentiality Service providers shall maintain the confidentiality of computer data, traffic data and subscriber information by adhering to internationally recognized cybersecurity and encryption standards unless authorized by a court order.
Article 12: Preservation of computer data and traffic data 4. The service providers or the persons who own the data as outlined in Paragraph 1 are obliged to effectively preserve such information confidentially and not disclose or take any action that may disclose the preservation of such data to the subscriber or the suspect	Articles 13 and 15 also have similar wording about disclosure. The original text runs counter to the transparency reports that companies issue on government warrants and requests for data. For an example, see https://transparencyreport.google.com/user-data	The service providers or the persons who own the data as outlined in Paragraph 1 are obliged to effectively preserve the confidentiality of such information and should disclose such data to the subscriber, the suspect, or in publicly available transparency reports once the investigation has concluded.

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
Article 14: Search and seizure of computer data	- Handling of privileged information: The article doesn't address how to handle potentially privileged or sensitive information. Oversight and accountability: The article lacks provisions for independent oversight of search and seizure operations.	Provisions for handling privileged information[1] Mechanisms for independent oversight of search and seizure operations[2]
Article 15: Real-time collection of traffic data 3. This Article shall apply only to investigations related to serious offenses.	Specificity and Clarity	Clearly define "serious offenses" that warrant interception.
Article 16: Interception of content data 3. This Article shall apply only to investigations related to serious offenses or crimes related to national security.	Specificity and Clarity	Clearly define "serious offenses" that warrant interception.
Article 17: Complaint and transitional fine	The initial appeal to the Minister of Interior, rather than an independent body, may not fully satisfy the requirement for an effective remedy.	Establishing an independent review body for initial appeals[3].
Article 26: Illegal data distribution by competent officers	The article doesn't address situations where disclosure might be in the public interest.	Additional provisions for disclosure of data for the public interest. (Whistleblower protection)
Article 32: Cryptocurrency	This should be addressed through comprehensive Cryptocurrency regulation, preferably through ASEAN cooperation. See Singapore's Payment	Removed

[1] UN Human Rights Council Resolution on The Right to Privacy in the Digital Age (A/HRC/RES/34/7), paragraph 5(f)
[2] UN Human Rights Council Resolution on The Right to Privacy in the Digital Age (A/HRC/RES/34/7), paragraph 5(d)
[3] ICCPR Article 2(3), and UDHR Article 8

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
	Services Act (PSA), Securities and Futures Act (SFA), and the Monetary Authority of Singapore for regulation examples.	
Article 34: Unauthorized access	- The article does not provide exceptions for legitimate security research or ethical hacking, which could inadvertently criminalize activities that are beneficial for overall cybersecurity.	• Including exceptions for legitimate security research and accidental access.
Article 35: Violation of authorized access	- This article doesn't consider the sensitivity or classification of the data accessed. There are no provisions for situations where unauthorized use might be justified (e.g., emergencies, whistleblowing).	• Create different levels of punishment that match how serious the offense is or how sensitive the information is. For example, misusing basic personal data might result in a smaller fine, while misusing highly confidential government information could lead to a much stricter penalty. Adding provisions for justified unauthorized use in specific circumstances.
Article 36: Unauthorized data interception	There are no explicit exceptions for legitimate activities that might involve data interception, such as authorized network monitoring or cybersecurity research.	Including exceptions for legitimate activities, such as authorized network security monitoring or research.
Article 37: Illegal computer program or device	An explicit exemption should be given for authorized testing or protection of a computer system. Commonly referred to as exemptions for white hat or ethical hackers, these polices enable security professionals to discover bugs and report the issue to the owner of the computer system before malicious cyber forces exploit the vulnerability. These professionals provide a valuable service in ensuring the security and confidentiality of IT systems.	Ethical hackers conducting authorized security research within a clearly defined scope, who promptly report discovered vulnerabilities and comply with international human rights standards, shall be protected from criminal and civil liability, provided their activities are conducted in a manner that respects data confidentiality and minimizes harm.

អត្ថបទដើម Original Text	យោបល់ និងហេតុផល Comments and Reasons	សំណើកែលំអ Proposal for Improvement
Article 38: Computer data interference	Unintended consequences: It could potentially criminalize some forms of legitimate system administration or security testing.	Including explicit exceptions for legitimate system administration, security testing, and research activities.
Article 39: Computer system interference	Unintended consequences: It could potentially criminalize some forms of legitimate system administration or security testing.	Including explicit exceptions for legitimate system administration, security testing, and research activities.
Article 43: Defamation	Potential for misuse: without clear definitions and safeguards, this article could potentially be used to suppress legitimate criticism or dissent.	Including provisions for prompt retraction or correction of false statements as a mitigating factor.
Article 47: Computer-related forgery Any person, without right , engages in the input, alteration or deletion of computer data or the restriction of the access to such computer data, resulting in inauthentic data , with the intent to be used for legal purposes shall be punishable by a term of imprisonment from 2 (two) years to 5 (five) years and a fine from 10,000,000 (ten million) to 25,000 000 (twenty-five million) Riels.	"Computer-related forgery" should adhere to the multinational standard definition in order to improve clarity and increase likelihood of international cooperation in prosecuting cybercriminals. See 2023 draft of the UN Cybercrime Treaty, The Council of Europe Budapest Convention on Cybercrime, or The Commonwealth Model Law on Computer and Computer Related Crime.	Article 47: Computer-related forgery The input, alteration, deletion, or suppression of computer data committed with the intent to defraud and without right, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.