Cyber Norms Operationalization in Cambodia and the ASEAN

Comparing cyber law in:

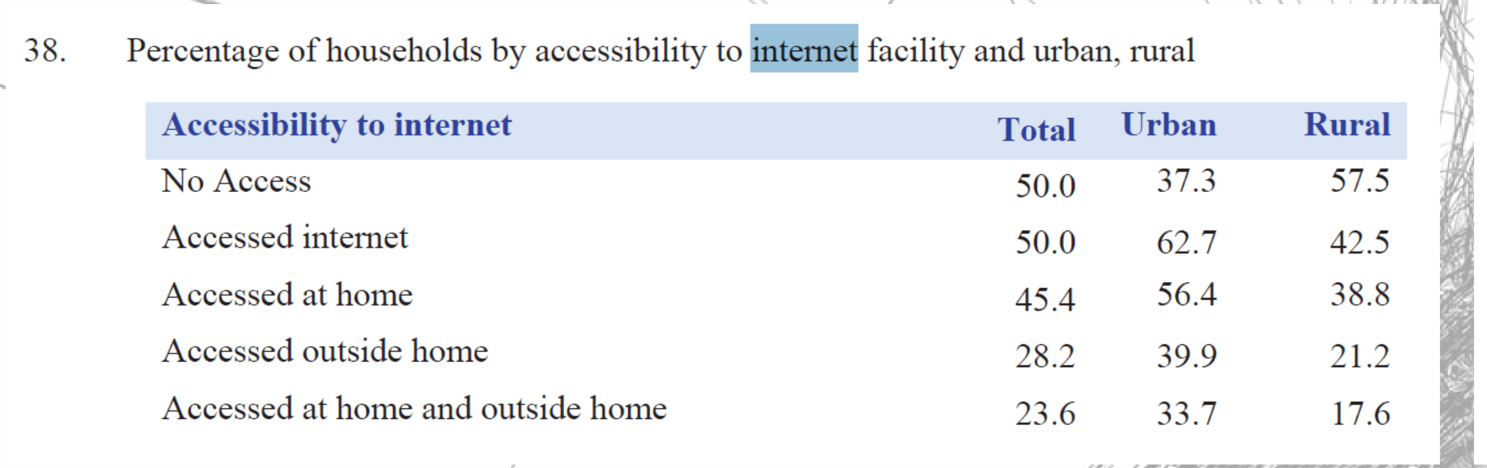
- Cambodia,
- Singapore,
- Vietnam,

As well as:

- The EU,
- China,
- The USA

Statistics: Internet Use

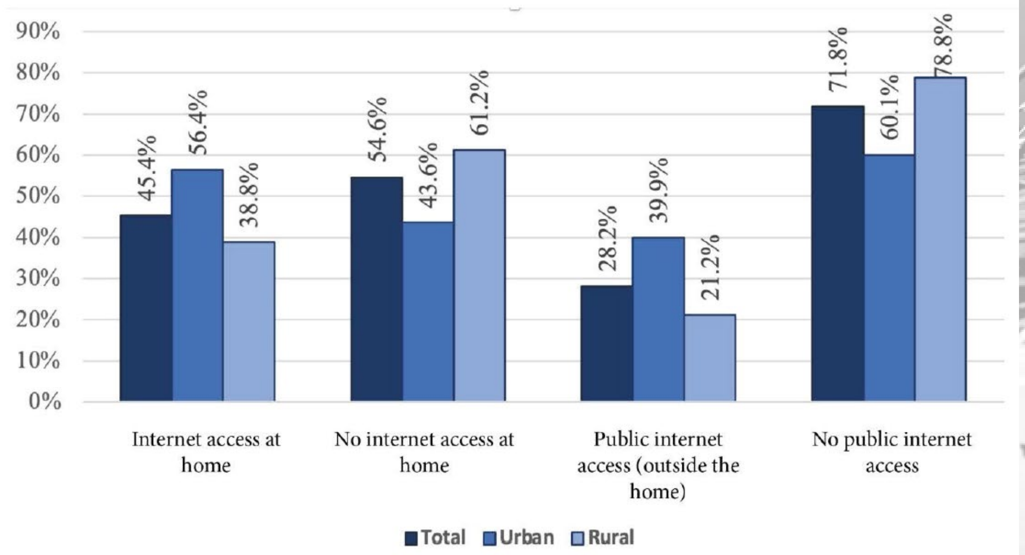
General Population Census of the Kingdom of Cambodia, 2019



38. Percentage of households by accessibility to internet facility and urban, rural

Accessibility to internet	Total	Urban	Rural
No Access	50.0	37.3	57.5
Accessed internet	50.0	62.7	42.5
Accessed at home	45.4	56.4	38.8
Accessed outside home	28.2	39.9	21.2
Accessed at home and outside home	23.6	33.7	17.6

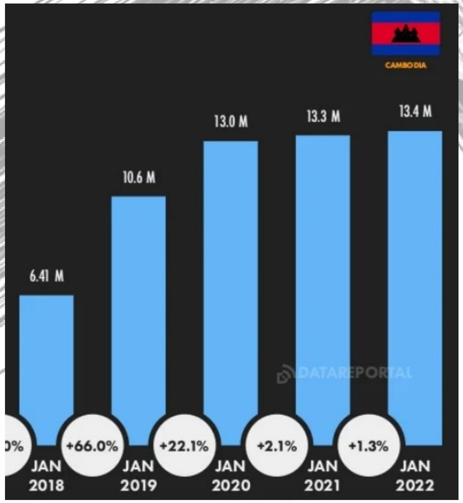
Figure 10.3.6 Percentage distribution of households by type of internet access and area, Cambodia, 2019

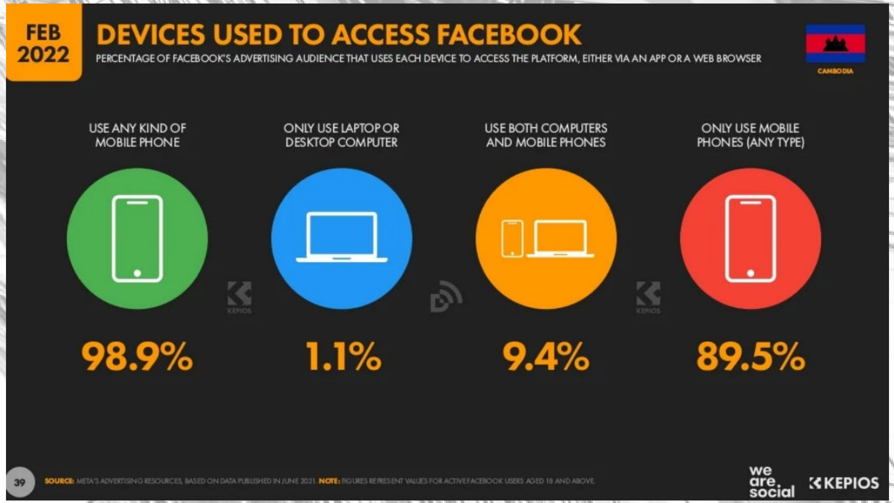


Jan. 26, 2022 Datareportal / wearesocial / Kepios Aggregation (citing GWI Q3 2021)

Percentage of Internet Users as a Percent of the Total Population:

Southeast Asia:	72%
Oceania:	73%
Eastern Asia:	73%
Cambodia:	79%
North America:	92%
Western Europe:	94%





FEB 2022

DEVICES USED TO ACCESS FACEBOOK

PERCENTAGE OF FACEBOOK'S ADVERTISING AUDIENCE THAT USES EACH DEVICE TO ACCESS THE PLATFORM, EITHER VIA AN APP OR A WEB BROWSER

SOURCE: META'S ADVERTISING RESOURCES, BASED ON DATA PUBLISHED IN JUNE 2021. NOTE: FIGURES REPRESENT VALUES FOR ACTIVE FACEBOOK USERS AGED 18 AND ABOVE.

Image: https://www.alongdustyroads.com/posts/mobile-sim-card-at-phnom-penh-airport-cambodia

Cambodian Law

- 2015: Telecomm. Law
- 2018: Interministerial Prakas (disinformation)
- 2019: eCommerce Law
- 2021: National Internet Gateway
- 2021: Subdecree 252 (gov't data sharing)

- Jurisdiction by MPTC, in collaboration with ministries of Information, Interior, Commerce
- Many specific regulations acknowledged TBD
- Central administration of internet (NIG)
- Appears to envision strong prosecutorial discretion.

Areas for Legal Development

- Cybercrime Law (draft leaked 2020; no passage yet)
- Data Privacy (consumer protection)
- National Policy on the Development of the Digital Sector, 2030
- ASEAN Masterplan, 2025

- Cybersecurity?
- Technical standards?
- Social media?
- Other governance on corporate conduct over the internet?
- Additional administration?

Singaporean Law

Personal Data Protection Act (PDPA) (2012); Similar in many ways to the EU GDPR. Comprehensive (123 page document) Key differences:

- Requires statement of purpose
- Treats all data the same; no distinction between PII and other data.
- Does not apply to public agencies and affiliates
- No provisions for pseudonymization
- Regards only individuals in Singapore, not outside
- Data subject rights of access less comprehensive

Areas for Legal Development

- 2020 amendments (effective 2021) brought significant updates that narrowed the gap between the PDPA and GDPR, including:
  - Mandatory data breach notifications
  - Civil cause of action for damages, where 1) harm, and 2) violation of the PDPA
  - Expanded definitions of “deemed consent” (where consent is not expressly given, but can be inferred)
  - Expanded enforcement and evidentiary powers for the Personal Data Protection Commission
- Common law jurisdiction; judicial decisions refine the law.

Vietnamese Law

Law on Cyber Information Security (2018):

- Data localization requirement for all internet services that collect Vietnamese customers' data. That data must be physically stored in Vietnam.
- Offshore data collectors must designate a local office or representative in Vietnam.
- Ministry of Information and Communications may demand deletion of content and conduct an audit with 12 hours' notice.
- Certain content illegal: incitement against the state, distortion of history, disturb public order, slander, etc.

Areas for Legal Development

- Level of actual enforcement is unclear.
- Guidelines and regulations on actual implementation still under review.
- November, 2021 draft amendment:
  - Would remove localization and local office requirements!
  - Introduce new provisions on data centers
  - Govern online gaming, including a 60-minute screen-time limit on players 18 and younger, for certain games.
- Pressure by both local and foreign business community to enact business-friendly laws.
- Illegal content includes many categories, but all are relatively vague (“cyber-humiliate”). Likely to remain in place.

EU Law

GDPR (General Data Protection Regulation):

- Ex-ante regulation requiring collection and use of PII only as necessary
- After data is used for stated purpose, it must be deleted
- Data subject given specific rights (art. 15)
- Security requirements, but left to the judgment of the collector; to be evaluated in a dispute
- Limits on transfer outside the European Economic Area
- EU wide administrative authority
- Businesses tending to seek certificates of GDPR compliance by technical experts

Areas for Legal Development

- Draft regulation (July 2021) on AI use by EDPB and EDPS would seek to limit “intrusive uses of AI,” social scoring (e.g. for finance or social media’s content moderation), use of biometric data; proposes additional administration, registration of AI tools, and “sandboxes” for study.

- EU Declaration on Digital Rights and Principles for the Digital Decade (Jan. 26, 2022) articulates broad vision for integrated future EU policy direction on human rights and the internet. Without spelling out each right, it manages to incorporate most of them.

- Armed Conflict in Ukraine: developing situation may see new developments in cybersecurity that will need to be addressed.

Chinese Law

Golden Shield

- Comprehensive surveillance by government of citizens both online and offline;
- Use of data to analyze citizen behavior;
- Firewall prevents access to prohibited sites;
- Use of VPNs prohibited.

PIPL (Previously PIPS), 2021:

- Seeks to limit effects of deleterious corporate data practices on Chinese citizens;
- Pervasive data breaches had led to pervasive cybercrime; in one case a poor university student was scammed and died of a heart attack that night.

Areas for Legal Development

- Influence: Reports of backroom policy by Chinese government on foreign corporations operating in China (e.g. Google), placing conditions on extraterritorial conduct
- Belt and Road initiative proposes a number of objectives:
  - Market access to greater supply of ICT rare earths
  - Use of political and economic influence to demand data-sharing
  - Hypothesized backdoor between Chinese corporate data collection and Chinese government;
- Influence of Chinese ICT Sector (e.g. Huawei, Apple*)
- Taiwan semiconductors dependent on continued status quo.

U.S. Law

Common Law, Market-Centric

- Law is split between statutes (passed by legislature), regulations (passed by executive administrative agencies), and courts (which interpret the details of the first two)
- With some exceptions, generally enforced through ex-post civil/tort liability
- National Institute of Standards and Technology (NIST): provides non-binding guidance

Decentralized; Federalism:

- Federal government watches over some sectors (banking, national security);
- Data protection and cybersecurity left to the states

Areas for Legal Development

Congress (Art. 1)

- Murmur of imposing ‘common carrier’ status on social media platforms, treating them as the de-facto exclusive option for public engagement.
- Strong movement for oversight and limitation of the power of “Big Tech.”

Executive (Art. 2)

- Heavily oriented towards national security, military, intelligence.
- CISA updates cybersecurity standards within the government itself, but does not bind the public.

Judiciary (Art. 3)

- Internet law constantly being refined and updated through continual tort litigation;
- Litigative society may benefit deep pockets and impose legal access barriers;
- Judicial philosophies may influence substantive law.

States are also developing laws

International Law and Initiatives

- Budapest Convention on Cybercrime (2001);
- Internet Governance Forum proposes best practices;
- Civil Society digital constitutionalism (e.g. IO Foundation) and further best practices;
- Continuing jurisprudence by special rapporteurs on privacy, expression, etc. by the OHCHR;
- Tallinn Manual by NATO, and continuing studies by the ICRC on the effects of cyberwarfare on civilians, etc.
- Innumerable SDG initiatives incorporating data and internet access/use.

Areas for Legal Development:

- No international conventions specifically addressing:
  - Digital human rights/human rights on the internet
  - Data protection
  - Tech ethics and AI development
  - Budapest convention likely in need of several optional protocols at this point
- Continuing GA declarations which chip away at formalizing digital human rights;
- Faith in international institutions and globalism appears to be decreasing, nationalism and factionalism increasing;
- “Cyber sovereignty” vs. “open, free, global, interoperable, reliable, and secure” internet
- UN’s role in a tripolar model of cyber / data policy?
- Cambodia, ASEAN, global south trajectory presently not entirely fixed.

Q?

A?

1. How could cyber and data law affect relations between nations?

2. Should the world harmonize laws, or would that intrude on culture and sovereignty?

3. What could be the benefits of various models?