Privacy and State Surveillance in Southeast Asia

K.S. Park

Professor, Korea University

Director, Open Net

It is easy to say that digital authoritarianism and digital populism are the two sides of the same coin but people often forget that such statement is ironic because populism requires support of the masses no matter how transient and misinformed it may be and authoritarianism at its core suppresses the will of the masses by force and pre-existing institutions. What makes possible this irony is the state's ability to conduct and justify surveillance on people - an ability to identify and orient judicial and social attacks toward dissident activists and journalists. There are three layers of state laws that affect the state's surveillance capacity.

- The first layer consists of **data availability**. Mandatory data retention laws fall under this category. Also, mandatory data localization laws also enhance data availability to the state by obviating the need for going through MLAT process for accessing foreign-based data.
- The second layer consists of **data identification**. Mandatory identity verification laws fall under this category. Also the laws allowing warrantless "unmasking" of data significantly enhance the state ability to target dissidents.
- The third layer consists of **data acquisition**. The laws allowing access to private data without judicial approval violate international standards of privacy or lower the bar of judicial approval to the extent that it is meaningless. In this presentation, I will discuss the laws and proposed laws of Myanmar, Indonesia, and Viet Nam against the framework.

Privacy - Basics

- Intrusion into privately held area → privacy infringement
- Revealing privately held information → privacy infringement
- Exception: to save life, protect security, reveal corruption
- How about "to investigate (or prevent) crime"? OK --→but if **the state is doing it**, presumption of innocence requires special procedure
- → Warrant Doctrine: special protection when State is infringing individuals' privacy for criminal punishment

→Warrant = "Probable cause" certified in writing by a responsible official independent of prosecutorial interest

→Due process = Presentation of warrant upon execution so that the target can be at least notified of the fact/reason for infringement Cf. normal due process requires advance notice so the target can rebut but criminal investigation is urgent.

But what is private?

- US: "reasonable expectation of privacy"
- Warren-Brandeis article: "right to be left alone"
- Prosser – 4 categories (intrusion, disclosure, commercial use, "false light",

but only 2 considered legitimate descendant of Warren-Brandeis version of privacy (I think 1 are legitimate, too)

- US: categorical (black & white 3rd party doctrine) – Supreme Court:

"metadata acquisition not surveillance, not need warrant" → US Congress changed law

- EU: incremental - e.g. Gay pride march not considered voluntary giving up of privacy
- US: becoming more incremental – Jones, Riley, Carpenter
- Anyway, when it comes to criminal investigation, EU=US –e.g.

French police collecting info at gay pride march will not need warrant.

Surveillance - Basics

- Surveillance = privacy infringement by INTRUSION
- When is surveillance justified?
  - When State does - **Warrant doctrine**
  - When Private parties do – to reveal corruption
- Why is warrant required? Gov't intrusion of any right requires **due process**
- Levels of state surveillance
  - Content v. Metadata (data required to be disclosed for communication or disclosed necessarily as a byproduct of communication)
  - Stored v. Real-time (Is intrusion to access not-yet-existing data more infringing or less infringing?)
  - Accuracy: GPS data vs. IP address vs. Mobile AP data
  - → Various levels of approval standards for **wiretapping >> search and seizure of content >> real-time metadata >> stored metadata (>>identity of communicating party?)**

Snowden revelations – mass surveillance

- Prism – "backdoor" into databases of Big Techs.
- What is the problem with Prism?

- Warrantless
- Mass surveillance (v. individualized suspicion)
- Domestic US persons (likely to include but not always)
- Lack of Notification

- Yahoo's Terms of Use: share if "required to do so by law"

→No expectation of privacy? → how about "on request"?

Apple v FBI – What do with dual-use technologies

Is it private information? Yes

Is there justification for breaching privacy? Yes, known terrorist potentially harboring info on other terrorists

Is FBI physically capable of doing that? No

So FBI tried to obtain a court order compelling Apple to break the iPhone for them.

(1) Can court force you (an innocent third party) to cooperate by affirmative act like painting a picture?

(2) Why did Apple oppose? Virality of information Do you agree?

Do people have right to use encrypted communication? Is there a limit on state's ban on encryption?

Indonesia

- Data availability – "In order to prove the truth, the use of telecommunications facilities at the request by users of telecommunications services, the providers are obliged to record the use of telecommunications facilities used by the users, and to record the information in accordance with laws and regulations." (Article 41, Telecommunications Law" – mandatory data retention
- Data identification – mandatory registration of "electronic system operators" (Article 2 MR5) – any web/app mediating communication among ppl "to provide, manage, and/or operate communications services including but not limited to short messages, voice call, video call, electronic mail, and conversation in network in the form of digital platform, network services and social media;" – no anonymity for intermediaries

- "Private Sector ESO provides access to Traffic Data and Electronic Systems User Information (Subscriber Information) requested by Law Enforcement Authorities in the event that the request is officially submitted to the Private Sector ESO Contact Person.(Article 36, MR5) – **no anonymity for users**

- Data acquisition – "For the purposes of the criminal justice process, telecommunication service providers may record the information sent and/or received by telecommunication service providers and provide the information as needed, by: (1) Written request from General Attorney and/or the Chief of Indonesian Police for specific criminal acts; (2) Request from investigators for specific criminal acts in accordance with applicable law." (Article 42, Telecommunications Law) – warrantless interception, also Article 36 warrantless acquisition of traffic data
- Data restriction – government demand "urgent" 4 hrs/non-urgent 24 hours takedown (Article 15, MR5) – "prohibited content" – definition "a. in violation of the law and regulation; b. causing public unrest and disturbance of public order; and c. providing information on the method or providing access to prohibited Electronic Information and/or Electronic Document." – but meaningless because once Minister finds it prohibited, ESOs have absolute duty to take down.

Myanmar

- 2022 Myanmar Cybersecurity Bill: ban use of virtual private networks (VPNs), abolish the need for certain evidentiary proof at trial, and require online service providers to block or remove online criticism of junta leaders.
- **Data acquisition:** 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.
- **Data restriction**: Requires Digital Platform Service providers to block or remove content about which there is a "legitimate complaint" that the content "damages a person's social standing and livelihood." It would not require the information to be false or require a court order. - "misinformation and disinformation," information "causing hate, disrupting the unity, stabilization and peace," and statements "against any existing law."
- Prevalent use of Western-originated surveillance technlogies

Viet Nam

- **Data availability and data acquisition**: Decree 53 of the aforementioned Cybersecurity Law came into effect on October 1 2022, clarifying the rules that mandate all domestic companies and many foreign companies, including social media platforms, telecommunications services, payment providers, and gaming platforms, to store user data information locally and provide it to authorities upon request. (subscriber identifying information, for 24 months upon request)
- **Data Restriction: Article 26** *Guarantees relating to information security in cyberspace* - Any domestic or foreign enterprise which provides services on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [*cyberspace service provider*] has the following responsibilities: To prevent the sharing of information and to delete information with the contents prescribed in clauses 1 to 5 inclusive of article 16 of this Law on services or information systems directly managed by any agency or organization no later than twenty four (24) hours after the time of a request from the CTF under the Ministry of Public Security or from a competent agency under the Ministry of Information and Communications, and to save/maintain system logs in order to serve investigation of and dealing with breaches of the law on cybersecurity within a [specified] period [to be] stipulated by the Government (2018 Cybersecurity Law) Information deemed particularly sensitive may be taken down within three hours.
- **Article 16** *Prevention of and dealing with information in cyberspace with contents being propaganda against the Socialist Republic of Vietnam; information contents which incite riots, disrupt security or cause public disorder; which cause embarrassment or are slanderous; or which violate economic management order*
- **Article 17** *Prevention of and combatting cyberespionage; and protection of information classified as State secret, work secrets, business secrets, personal secrets, family secrets and private life in cyberspace*
- Prevalent use of Western-originated surveillance technlogies

Takeaways

- Germany's NetzDG – a response to disinformation – inspired administrative censorship regimes in Southeast Asia
- Data sovereignty and data localization in other parts of the w orld buttressed data availiability initiatives in Southeast Asia
- Online safety bills in UK, Canada, Australia may end up justify ing anonymity-restrictions in Southeast Asia
- Sale of 'dual-use' technologies by advanced countries should be regulated.
- Substance is of course more important, however, form should be always used with care.