INTERNET CENSORSHIP IN THAILAND
การเซ็นเซอร์อินเทอร์เน็ตในประเทศไทย

Although Internet censorship in Thailand is among the world's most aggressive and capricious, we still do not fully understand its impact on users.

Research Questions & Mixed-Methods Answers

Despite the widespread effects of Internet censorship in Thailand, the research community still lacks a thorough understanding of how it impacts users. In particular, how do users of the Internet in Thailand:

- **ASSESS** censorship?
- **ACCESS** censored content?
- take **ACTION** with information?

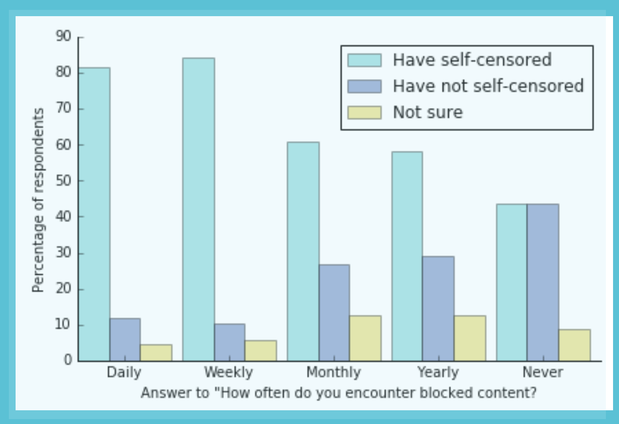
With IRB approval, we address these questions through statistical and qualitative analysis of 229 online surveys and 13 in-depth interviews with regular, everyday users of the Thai Internet.

User Practices, Threats, & Unresolved Problems

62% of respondents reported attempting to circumvent Internet censorship with technical tools like proxies, VPNs, and Tor, as well as more "ad hoc' methods. These tools and strategies were technically adequate to circumvent Thai censorship. However, respondents' selection of censorship circumvention tools was **risky** and **incident-driven**, leaving them vulnerable to surveillance, malware, and other attacks.

Moreover, respondents were sometimes **unable to distinguish** among government censorship, geoblocking, paywalling, and other types of inaccessibility, making it difficult to determine what and how much their government is censoring.

70% of respondents reported **self-censoring** online for fear of the law. This self-censorship was correlated with exposure to censorship. Creating and sharing content on social media was the most urgent, concrete threat that users faced, but was also the area where they most **lacked the technical means** to protect themselves.



Recommendations & Broader Implications

Content Assessment

- Users need need more information about content both *before* and *after* they load a website.
- Is it blocked? By whom? Where is it hosted? Does is pose a surveillance risk?

➢ Combination of **browser extension** and **private information retrieval (PIR)** from an external database to gather more information and infer how and why content is blocked.

Tool Selection

- Users need flexible, readily available tools from trustworthy sources.
- We must deliver tools to users *before* they need them in order to avoid risky, reactionary searching behavior.

➢ Official, **browser-affiliated** tools.

➢ **Flexible, adaptive** tools that change based on desired content and user priorities.

Social Media

- Recommendations to existing social media platforms toward safer engagement and *more* use.

➢ **Anonymity** – Display a count of likes rather than the identities of likers.

➢ **Impermanence** – Likes, comments, and other interactions self-destruct after they have served their social purpose.

➢ **Control over content** – Comments can be set to be un-share-able and un-like-able.

Beyond Thailand, this **area-focused engagement** with **real users** in an extreme environment can motivate the **empirically grounded** development of **stronger security measures** valuable to users in any setting.

Advisor: Professor Tadayoshi Kohno
UW CSE Security & Privacy Research Lab

Genevieve Gebhart
Master of Library & Information Science
Capstone 2016

Information School
UNIVERSITY of WASHINGTON