Internet Censorship in Thailand: User Practices and Potential Threats

Genevieve Gebhart* †1, Anonymous Author 2, Tadayoshi Kohno †

*Electronic Frontier Foundation †University of Washington
gennie@eff.org
yoshi@cs.washington.edu

Abstract—**The "cat-and-mouse" game of Internet censorship and circumvention cannot be won by capable technology alone. Instead, that technology must be available, comprehensible, and trustworthy to users. However, the field largely focuses only on censors and the technical means to circumvent them. Thailand, with its superlatives in Internet use and government information controls, offers a rich case study for exploring users' assessments of and interactions with censorship. We survey 229 and interview 13 Internet users in Thailand, and report on their current practices, experienced and perceived threats, and unresolved problems regarding censorship and digital security. Our findings indicate that existing circumvention tools were adequate for respondents to access blocked information; that respondents relied to some extent on risky tool selection and inaccurate assessment of blocked content; and that attempts to take action with sensitive content on social media led to the most concrete threats with the least available technical defenses. Based on these findings and in direct response to these problems, we make recommendations for shifting objectives in anti-censorship work, as well as for technical directions and future research to address users' on-the-ground needs.**

1. Introduction

The "cat-and-mouse" game of Internet censorship and circumvention cannot be won by capable technology alone. This ongoing struggle generally pits government-level censors seeking to block citizens' access to content against researchers and developers devising ways to circumvent such blocks. In the middle, users face the often-overlooked task of putting these circumvention tools into action and reconciling them with on-the-ground conditions.

The bulk of research on censorship circumvention focuses on the former two sides of this "game" and their deployment of increasingly sophisticated technologies against each other. On one side, government censorship policies have received in-depth study [28, 46, 54], and corresponding technical measurements of censorship are well developed [1, 14, 16, 47, 53]. On the other side, the security community has proposed novel circumvention methods in response [10, 25, 38].

The goal of circumventing censorship and attaining freer access to information, however, relies on those circumvention methods being available, comprehensible, and trustworthy to users. Only by meeting users' needs can circumvention tools realize their full technical capabilities.

With this goal in mind, the field lacks sufficient inquiry into the range of user perceptions of and interactions with censorship. How do users assess censored content? What is the range of their reactions when they encounter censorship? How does censorship affect the way they not only access but also produce information?

In addition to guiding more thorough anti-circumvention strategies, these questions about users and censorship can act as a lens into broader security issues. Users' perspectives on censorship have wide-ranging implications for security behaviors both on and offline [51, 55], especially in the politically repressive, low-resource environments in which common-sense censorship circumvention technologies are most needed. Looking at users' censorship circumvention strategies can produce insights into the vulnerabilities of those strategies and the varied content perceptions, risk assessments, and self-censorship practices that inform them. Overall, these questions can guide research priorities toward safer Internet use.

In order to address the gap in understanding around users and censorship, we report on the results of online surveys and in-depth interviews with users of the Internet in Thailand. This effort represents a cross-disciplinary collaboration among authors from information science, sociology, and computer security, as well as Southeast Asian studies. Using standard sampling methodologies, we surveyed 229 and interviewed 13 respondents until reaching a "point of saturation" at which new respondents did not reveal new information. These methods were approved through our institution's IRB to protect respondents' privacy and safety.

This deep dive into users in a particular setting—in this case, Thailand under military dictatorship—allows us to have a concrete, informed discussion about the risks and challenges real individuals face with existing technologies

[1] Genevieve Gebhart conducted this research at the University of Washington. She is now at the Electronic Frontier Foundation.

[2] The second author is a Thai citizen and preferred to remain anonymous.

in a repressive environment. We focus our investigation on Thailand for the superlatives it exhibits in information controls, government repression, and Internet use. Conclusions about our sample provide lessons for efforts to protect users in other politically repressive contexts, particularly in neighboring Southeast and East Asian states. The challenges and nuances of this extreme environment can also motivate the development of stronger security measures valuable to users in any setting.

We organize our findings around users' current practices, threats, and unresolved problems, as well as other pertinent observations. Here we preview the takeaways from each section:

- *Current practices.* Most respondents were able to access censored content with existing technical tools and ad hoc methods. However, respondents tended to search for new tools every time they encountered blocked content, an incident-driven strategy that left them vulnerable to malware and surveillance. Further, respondents did not always accurately assess the actors and methods behind blocked content. Respondents also took extensive precautions on social media to avoid consequences from their peers as well as from the government.
- *Threats.* Respondents faced direct, concrete threats on social media, primarily from politically motivated peers. Respondents' perceived, hypothetical threats revolved around uncertain, self-contradictory conceptions of government capacity and will. These vague perceptions nevertheless informed respondents' behavior. We also highlight threats that respondents may have overlooked, including government phishing and malicious proxies.
- *Unresolved problems.* Respondents' most urgent unresolved problems were with content assessment, tool selection, and safe engagement on social media.
- *Additional observations*. Both quantitative and qualitative evidence pointed to a correlation between how often respondents encountered blocked content and their tendency to self-censor. Further, blocked content had complicated meaning and symbolism even to respondents who did not want or need to access it. Finally, respondents did not exhibit exclusively pro- or anti-censorship attitudes.

Together, these findings motivate a discussion about shifting objectives in censorship work in particular and security research in general. Our findings demonstrate that fighting censorship requires more than access to blocked content; users must also be able to understand and safely engage with that content. Further, anti-censorship design needs to take into account both technical realities and user perceptions, as both play a role in shaping user behavior. However, given the finding that respondents could not be categorized as strictly pro- or anti-censorship, we recommend flexible rather than one-size-fits-all solutions.

With this deeper understanding of how censorship impacts a sample of real users, we recommend three directions to address respondents' three unresolved problems above: a browser extension to aid in content assessment, tool delivery strategies to help with tool selection, and changes to build plausible deniability into existing social media platforms. We hope these recommendations for future action, and the findings on which they draw, will inform a next generation of anti-censorship tools even more closely tied to real users' practices and challenges.

2. Background and Related Work

To provide the necessary context for our respondents' survey and interview responses, we offer brief background on Internet censorship in Thailand before situating our study within three areas of related work: user practices and needs, censorship circumvention and resistant systems, and the impact of censorship on user behavior.

2.1. Internet Censorship in Thailand

With unique censorship implementation and rationale, as well as an escalating environment of direct and indirect censorship, Thailand represents a valuable case study in how users interact with Internet censorship.

Internet censorship in Thailand was formally legislated with the Computer Crime Act of 2007. Among other provisions, this act criminalized the concealment of one's IP address, a key element of technical censorship circumvention strategies, thus ushering in "much more draconian Internet censorship than in China, Saudi Arabia, Iran, or even Vietnam" [56]. The act has faced international criticism in particular for the broad discretion it gives the government to interpret what does or does not constitute a computer crime violation [49].

Since then, the volume, range, and methods for restricting blocked content have accelerated. Tests in 2006, 2010, and after the most recent military coup in 2014 found that implementation of censorship was highly inconsistent among Thai ISPs in terms of content filtered, mechanisms used to filter it, and block pages visible to users as a result [40, 41, 48]. Such large-scale variation poses a challenge to technical measurements, making user testimony particularly valuable.

The defining characteristic of censorship in Thailand is lèse majesté, a Thai law that criminalizes insulting, threatening, or defaming Thailand's monarchy, particularly the late King Bhumibol. With 70 years on the throne and anywhere from an estimated 18 to 53 billion USD in personal wealth, he was among the world's longest-reigning and wealthiest monarchs. In combination with the Computer Crime Act, lèse majesté is invoked both to block online content and criminalize those who create and disseminate it [7], with recent punishments of up to 30 years' imprisonment [21].

At the time of this study in February and March 2016, the aging King's health was in decline and a divisive royal succession loomed. Since the conclusion of this study, the King passed away in October 2016, with the controversial crown prince taking the throne about six weeks later. Shortly after, in December 2016, the Computer Crime Act underwent serious amendments that encouraged even broader and more ambiguous interpretation of computer crime offenses, increasing its potential for abuse against dissidents [15].

Throughout this time, the current military regime, which took power in the 2014 coup, has instituted an expansion of what constitutes a lèse majesté violation online. Recent offenses range from insulting the late King's dog to clicking "like" on Facebook content deemed defamatory to the monarchy [23], with monitoring and reporting coming from politically motivated citizens as well as government authorities.

Thailand boasts an active population of content-producing social media users, with the capital city of Bangkok hosting more Facebook users than any other city in the world [13]. Widespread censorship of user-generated content—via both mass surveillance from the government and "surveillance by the masses" from peers on social media—poses a serious, everyday threat to the regular Internet users who make up our sample, as they risk unknowingly violating vague and constantly changing legal and social standards [30].

2.2. User Group Practices and Needs

Previous research demonstrates the value of studying specific user groups' security practices and needs in depth. A growing body of work, for example, examines journalists' general practices and security-related needs [37]. In Thailand in particular, Hamnevik and Persson [19] investigate the strategies journalists use to uphold their codes of ethics under censorship.

Additionally, targeted user groups like activists [36] and NGOs [18, 31] have emerged as subjects of research on politically motivated attacks. An especially rich area of literature focuses on Chinese activists' interactions with government censorship and discourse [20, 34].

We build on this work by investigating another distinct demographic. While a user group defined by country is broader than a particular profession like journalists or activists, capricious enforcement of Internet regulations in Thailand puts even everyday users at significant risk for targeted censoring, surveillance, and attacks. Only by engaging with this user group can we better understand what threats may manifest *in their environment* and how best to respond to them.

2.3. Censorship Circumvention Tools and Resistant Systems

Existing systematizations classify technical aspects of censorship circumvention tools, resistant systems, and blocking criteria [27, 29], with Leberknight et al. [32] further discussing design features and sociopolitical perspectives. Region- and country-specific tools like Alkasir [2] have also been subjects of previous study. Previous empirical work in this space also aims to ground censorship circumvention in observation of real censors and attacks on resistant systems [52].

However, a narrow focus on technical tools and systems may miss the other circumvention strategies that users employ to get to the information they want. For example, Khattak et al. [26] find that, immediately after encountering blocked pages, Pakistani users tended to search for and shift to alternative, unblocked content providers rather than attempt to find or use technical circumvention tools. We aim to provide a more thorough account of the range of methods users employ in response to censorship.

2.4. Censorship's Impact on User Behavior

A strong body of user-focused research establishes how Internet censorship regulation can discourage users' practices of contributing to content [51], alter their trust in online sources [17], motivate them to self-censor criticism of ruling governments [57], and impact discussions on social media [9]. Previous work highlights "networked authoritarianism" [35]—a characterization with acute applications to Thailand's Internet environment—as one political setting in which censorship carries such impacts. Pearce and Kendzior [44] describe a networked authoritarian regime as synonymous with Deibert and Rohonzinski's [11] "next-generation" Internet censorship and information controls, using not only outright blocking but also legal and social manipulation to control information.

Users' perceptions of censorship play a nuanced role in these networked authoritarian processes and self-censorship outcomes. Wang and Mark [55] examine Chinese users' attitudes toward censorship based on direct experience with, rather than abstract ideas about, information controls. Building on this work, we focus on real users' tangible interactions with, as well as broader attitudes about and assessments of, Internet censorship.

3. Questions and Motivations

In response to the bodies of literature described above, we pose three questions.

First, how, if at all, do users of the Thai Internet assess Internet censorship? How users understand censorship—from the censors behind it to its social desirability to its significance in their daily lives—gives crucial context to the actions they take in response.

Second, how, if at all, do users of the Thai Internet access blocked information? Where users report risky, misinformed, or inconsistent reactions to censorship, there may be opportunities to address unresolved problems and needs.

Third and finally, to what extent is censorship associated with or experienced alongside self-censorship? We focus specifically on self-censorship that reflects a fear of the law, government, or politically motivated actors. Inquiry into users' actions with, not just access to, information can motivate more comprehensive responses to the range of censorship-related challenges they face.

4. Methods

To address these questions, we conducted a two-phase study: a large-scale anonymous online survey, followed by individual in-depth interviews.

4.1. Human Subjects and Ethics

Because survey and interview responses could carry criminal liability, we obtained IRB approval before undertaking any research activities involving human subjects. The survey's introductory page included consent information in both English and in Thai, and verbal consent was established at the beginning of all interviews. We asked respondents to answer only questions they were comfortable answering, and to not share any information that could put them at risk. We stored survey and interview data on encrypted hard drives, and did not record or store any identifying metadata. Respondents were free to withdraw their survey and/or interview responses at any time.

4.2. Sample and Recruiting

Our goal in sampling was to investigate the widest possible range of user assessments of and reactions to censorship in Thailand. We aimed to capture such maximum variation (rather than, for example, representation or generalizability) as a robust counter to the inherent limitations of survey bias on gathering and interpreting empirical qualitative evidence. With this in mind, any user of the Thai Internet was eligible to participate in the study, regardless of nationality or location. The only eligibility requirements were that respondents 1) had spent the majority of the past year in Thailand, and 2) were over 20 years of age (the age of adulthood in Thailand). Notably, nationality did not have a statistically significant effect on any survey responses.

These minimal eligibility requirements meant we had the opportunity to survey users across the spectrums of support for censorship (both "pro" and "anti") and use of circumvention tools (both users and non-users). This variation facilitates this study's strength in characterizing a range of actual Internet users' complex, individual experiences. For example, non-users' perspectives shed light on how people become aware of new technology, what leads them to accept or reject it, and what design or implementation changes may encourage adoption [5].

We recruited survey respondents primarily through snowball sampling methods [6]—that is, a sampling technique in which initial subjects recruit other subjects by sharing the survey link. Snowball sampling is most appropriate for difficult-to-recruit populations that require a high degree of trust. For the extremely sensitive topic of Internet censorship in Thailand, snowball sampling increased the likelihood that respondents would receive the survey from a trusted source and thus feel safer providing candid responses.

To recruit initial subjects, we distributed the survey link as widely as possible via social media (Facebook, Twitter), academic blogs (New Mandala), relevant listservs (TLC, Wikimedians in Thailand), professional groups (Librarians in Thailand, Thai Journalists Association), online interest groups (Blognone), and online news outlets (Prachathai). We also distributed the survey to the authors' contacts and colleagues. In all cases, survey introductory text encouraged subjects to share the link within their own networks. To make it possible to isolate compromised responses in case of any "hijacking" from extreme users or even police or government actors, we used distinct URLs for each distribution method.

Interview recruitment flowed from the survey, with the final survey question asking respondents to provide their email address if they were willing to participate in an interview. Of 229 survey respondents, about 38 percent (n=87) provided email addresses, with about 59 percent (n=135) giving no response and 3 percent (n=7) making a distinct statement of refusal (e.g., "Too dangerous" or "Should you come to Thailand and provide safe space and face-to-face, I would consider it."). We found no statistically significant differences in interview willingness across gender, nationality, or location.

4.3. Self-Selection and Bias

While this study's snowball sampling method achieved its goal of capturing high variation among a broad range of users of the Thai Internet, it was not representative of that overall group. Triangulation among multiple methods built several points of self-selection into the study: respondents first self-selected to view and complete the survey, then to provide their contact information for interviews, and then to reply to the authors' emails to request and schedule interviews. Further, due to inherent limitations in survey distribution, potential respondents may never have seen the survey.

These stages of self-selection likely contributed to demographic skew, which we describe in more detail in Section 5.1 below. In particular, these methods may have filtered out those with concerns about the consequences of their participation in the study, who did not trust the survey or the academics associated with it, or who were not sufficiently interested to invest increasing amounts of time.

Finally, the imperative of minimizing human subjects' risk while collecting reliable information about a sensitive topic limited the specificity of information we could safely solicit from respondents.

4.4. Procedures

Both the survey and interviews remained open until a "point of saturation" at which additional surveys and interviews no longer revealed new themes [33].

4.4.1. Survey Procedures. Survey text[23] was in both English and Thai, with multiple native Thai speakers verifying the Thai translation. The survey was open for two and a half weeks in February 2016 on our university's custom survey platform. This platform uses a code translation method that allows for secure identification and withdrawal of responses. We also chose the platform for its association with our institution, which was intended to further convey to respondents our academic affiliation and aims.

The first section of the survey made no mention of censorship or blocks, and instead asked questions about where and how respondents accessed the Internet. This section concluded with a neutral, open-ended question to probe for what respondents found most important about using the Internet in Thailand. Following questions included: what kinds of blocked content respondents encountered and how frequently; whether and how respondents had ever attempted to access blocked content; whether and where respondents had ever posted content that was later blocked; open-ended questions about change and restriction on the Thai Internet; and a multiple-choice question about whether respondents had ever self-censored for fear of the law.

4.4.2. Interview Procedures. Based on the content of their survey responses, we aimed for maximum variation in choosing willing survey respondents to contact for interviews. Interviews were conducted over Skype or the phone in the respondent's language of preference (English or Thai). Interviews were audio recorded with respondents' consent, transcribed, and then destroyed within 45 days.

Although interviews included follow-up questions specific to each respondent, we followed a semi-structured interview protocol[4] to ensure that the same basic lines of inquiry were pursued in each interview. In addition to follow-up questions about survey responses, interviews explored: the strengths and shortcomings of respondents' censorship circumvention strategies, if any; respondents' conceptions of better tools; respondents' awareness of and experience with citizen informants; and management of public online presences like social media pages.

4.5. Analysis

Our mixed-methods approach takes advantage of the strengths and weaknesses of survey and interview methodologies. While the online survey allowed us to reach a wider range of respondents, it did not allow for follow-up questions or in-depth discussion. The interviews, on the other hand, gave respondents an opportunity to reveal stories and opinions they may not have been comfortable sharing in writing, but introduced an additional layer of self-selection. Combining these methods results in a more comprehensive evaluation of user practices and perspectives than either method could produce alone.

Quantitative data from closed, multiple-choice survey questions lent itself to statistical analysis to probe for trends, correlations, and statistical significance, which we report inline where appropriate.

Qualitative data came from both open-ended survey questions and interview transcripts. We employed a grounded theory approach to thematic coding [43], an iterative process of developing, testing, and modifying emergent themes or "codes" from the data. Two of the authors—one natively fluent in English, one natively fluent in Thai, and each proficient in both languages—independently coded all qualitative survey responses and interview transcripts. During this process, all Thai-language survey and interview responses were translated into English and verified by multiple native speakers. After reaching consensus and revising codes where necessary, we developed a final codebook to apply to the data. Top-level codes are reflected in the thematic sections and subsections around which we report our findings in Section 5.

TABLE I
INTERVIEWEE DEMOGRAPHICS

No.	Gender	Age	Nationality	Occupation
1	M	20-29	American	Professor
2	M	60-69	American	Researcher
3	M	60-69	Dutch	Researcher
4	F	30-39	Thai-American	Lifestyle journalist
5	M	20-29	Thai	Researcher/musician
6	M	20-29	Thai	Undergraduate student
7	F	30-39	Thai	PhD candidate
8	M	20-29	Thai	Government employee
9	F	20-29	Thai	Researcher
10	F	20-29	Thai	News researcher
11	M	40-49	Thai	Professor
12	M	20-29	Thai	Student
13	M	20-29	Thai	Graphic designer

[3] A copy of the survey instrument can be found at https://catalyst.uw.edu/webq/survey/gennie/323533.

[4] A copy of the interview protocol can be found at http://seclab.cs.washington.edu/pubs/IEEE-EuroSP-Gebhart-EtAl-2017-Interview-Protocol.pdf.

5. Findings

After an overview of respondents and their demographics, we present our findings in four categories: current practices, experienced and perceived threats, unresolved problems, and additional observations.

5.1. Respondents Overview

The survey was closed with a total of 245 responses out of 691 total views, for an approximate 35 percent response rate. Of these, 16 responses were removed (15 for ineligibility, and 1 at the request of the respondent) for a final sample of 229. Our snowball sampling method resulted in a skew toward young, educated respondents, with an average age of 38 and 92 percent (n=210) having attained at least a bachelor's degree. Males (62%, n=142) and non-Thai nationals (32%, n=74) were also overrepresented. Nationality, however, did not have a statistically significant effect on any survey responses.

Respondents reported a range of professions, with agriculture (n=2) and housekeeping (n=2) represented alongside journalism (n=6) and librarianship (n=5). The most common occupations were university- and technology-affiliated: students (n=29), academics (n=27), independent contractors or freelancers (n=22), and technology-related positions (n=19), followed by private sector employees (n=18) and government employees (n=16).

We contacted 38 survey respondents for interviews, of which 13 were interviewed (see Table 1 on previous page).

5.2. Current Practices

Respondents' current practices reveal general satisfaction with censorship circumvention tools' ability to access blocked content, but also concerning trends about inaccurate or misinformed conceptions of the functions various tools offer and the actors behind blocked content. Respondents also self-censored and took extensive additional precautions on social media.

5.2.1. Accessing Blocked Content. Respondents reported that they were able to get around blocks using not only technical tools but also ad hoc methods (see Table 2). About 63 percent (n=144) had attempted to circumvent blocks before. Of those, about 90 percent (n=132) said their attempts were successful, indicating that existing tools were capable of circumventing the government's current censorship strategies.

Eleven respondents reported failure, with only three methods: proxies (n=2), VPNs (n=2) and alternative searches (n=3). (Four did not report any method.) All had a bachelor's or master's education, and did not differ from average respondents in the number of years they had been using the Internet or the amount of time they spent on the Internet per day. Those for whom proxies or VPNs failed expressed frustration with finding instructions, learning how to use the tools, and slow performance.

TABLE 2
CENSORSHIP CIRCUMVENTION TOOLS AND STRATEGIES
Percentages are out of 144, the number of respondents who reported attempting circumvention. Because respondents generally listed more than one tool/strategy, they will add up to more than 100%.

Tool/strategy	Notes/examples	#	%
VPN	Hola (3), HideMyAss, Hotspot Shield, Zenmate, Softether	54	32.64
Proxy	ProxyChain, oProxy, TurboHide, Privoxy, Lantern, free proxies in general	47	32.64
Tor	---	34	23.61
Google Translate	---	9	6.25
Search for different source	Includes copy-paste searching	7	4.86
Cache	---	6	4.17
Wait until physically abroad	---	4	2.78
Mobile sites	---	3	2.08
Mobile apps	e.g., specific news sources' apps	2	1.39
Internet Archive	---	1	0.69
RSS Feeds	---	1	0.69
Change domain	e.g., "example.fr" instead of "example.com"	1	0.69
Change ISP	Generally via mobile network	1	0.69
Change search to English	English-language content less strictly monitored than Thai	1	0.69
Use workplace computer with servers abroad	---	1	0.69
Ask friends abroad to find content	---	1	0.69

Significantly, women were less likely to attempt to circumvent censorship (Fisher's exact test, $p < 0.01$), and more likely to fail if they did (Fisher's exact test, $p < 0.01$). These conclusions rely on a relatively small sample of only 35 female respondents who attempted to circumvent censorship. However, even the small size of this sample is indicative of the underrepresentation of women in circumvention efforts among respondents.

These findings suggest that access challenges came not from tools' technical ability to circumvent censorship, but rather from how readily available and understandable they were to respondents.

5.2.2. Risky Tool Selection. Although respondents found existing circumvention tools effective, their strategies for selecting such tools were risky and incident-driven. Some respondents reported searching for and selecting new tools every time they encountered blocked content. This reveals a substantial opportunity to improve tool delivery, which we discuss in more detail in Section 6.

While a few survey and interview respondents described learning about proxies and VPNs from academic or media advocacy groups, most relied on repeated Google web searches. Trust in Google played a key part in this practice.

Interviewee #6 said:

"First thing I just go onto Google and search 'proxy server.' Click, click, I get it, and that's what I go through. I kind of trust Google to have the best ones on top, since the SEO will push those to the top. So I'll do the first two that are not ads."

Experiences of strict repression also motivated respondents to adopt stronger resistance tools. Interviewee #9 learned to use Tor when Facebook was briefly blocked after the 2014 coup. This use of an anonymous service to log into an individually identifiable social media account is not necessarily a contradiction, as Tor protects one's browsing habits, location, and identity from ISPs and other upstream surveillance [12]. In this case, Interviewee #9 perceived Tor as the strongest, most complex tool available to overcome an unusual, crisis-indicating block of Facebook. After Facebook was unblocked, she stopped using Tor due to the time and effort required.

Survey responses confirm, however, that this brief Facebook block drew attention to censorship, with several respondents describing it as the situation in which they felt most restricted on the Internet. Further, restrictive Internet experiences were not limited to the domestic Thai context; a Thai survey respondent reported using a VPN in Thailand only after he adopted it while traveling in China.

Interviews also suggest some relationship between desired content and selected tools. For example, Interviewee #13 adopted VPNs in an effort to improve gaming speed. Interviewee #4 also described using VPNs while prioritizing performance over anonymity or other concerns, using a VPN for video streaming and a proxy for other content:

"It used to be that Netflix was not allowed in Thailand. So the only other thing you would do is use a VPN. But for a normal website you would just use a browser-based proxy."

Overall, tool selection did not take place in a vacuum, with respondents making on-the-spot, sometimes inaccurate assessments of security characteristics, performance, risk, and desired content.

5.2.3. Inaccurate Content Assessment. Users in Thailand may encounter content blocked by various actors beyond the government, and respondents were not always sure what actor was responsible for a particular block. Content owners may restrict content on copyright or licensing grounds, and content providers and platforms (like Netflix) may not make content available in certain countries (also known as "geoblocking"). Users who cannot distinguish among these blocking actors cannot accurately determine what content their government—arguably the most significant adversary among blocking actors—considers sensitive.

Using respondents' words and categorizations from responses to an open-ended survey question about what blocked content they had encountered, Table 3 presents categories of blocked content and how often respondents reported them. Note that this is not a representation of what or how much content the government censors, but rather a measure of how frequently survey respondents reported encountering categories and instances of blocked content.

TABLE 3
CATEGORIES AND INSTANCES OF BLOCKED CONTENT
Percentages are out of the entire sample of 229. Because respondents generally listed more than one category, they will add up to more than 100%.

Category	Notes/examples	#	%
News		113	49.34
-- Domestic	Thai e-News (2)	2	0.87
-- International	The Daily Mail (58), Asia Sentinel (2), The Guardian (2), The New York Times (2), Business Insiders, Wall Street Journal	69	30.13
Pornography	Pornhub, X-ART, ImageFap, free pornography in general	55	24.02
Lèse majesté	---	43	18.78
Politics	---	40	17.47
Music, video	YouTube (14), Netflix (6), Vevo, Ustream	36	15.72
Criticism of govt/military	---	25	10.92
National security	---	11	4.80
Blogs and individual authors	Political Prisoners of Thailand (4), Andrew MacGregor Marshall (4), Andrew Drummond (2), Saksith Saiyasombut	11	4.80
Social media	Links from/posts on (4), forums/webboards (4), Facebook after the coup (2)	10	4.37
Political opposition	Thairedshirts.org	7	3.06
Filesharing	---	6	2.62
Gaming	Tropico 5	4	1.75
Gambling	Links from sports sites	4	1.75
Ads	---	3	1.31
Southern insurgency	Content concerning ongoing Muslim insurgency in Thailand's south	3	1.31
Research	---	3	1.31
Defamation	---	2	0.87
Circumvention tools	---	2	0.87
"None"	---	2	0.87

Most respondents listed only government-blocked content, with some even specifying whether the blocks came from government agencies, ISPs, or licensing or copyright restrictions. When blocks led to clear government block pages—typically pages with a Ministry of ICT or police seal accompanied by a statement that the website was "inappropriate" and had been blocked—respondents were confident that the blocking actor was the government. But beyond those recognizable landing pages, some respondents were unsure what else the government might be blocking or what that would look like. About 10 percent of respondents (n=23) expressed uncertain or incorrect assessments of blocking actors with regards to media (n=21) and research content (n=2).

While the Thai government does block or has blocked all respondent-reported categories, specific instances vary and may contribute to user confusion among government censorship, geoblocking, licensing, and other reasons for content to be inaccessible. For example, respondents who reported YouTube clips and Netflix as blocked were likely running into geoblocking. However, memories of government censorship of Youtube in 2006 and 2007 may have influenced respondents' assessments of current geoblocking. One survey respondent explicitly attributed increased accessibility of Netflix to Thai allowances:

"There's more censored information, but Thailand is also slowly allowing locals to gain access to foreign websites (e.g. Netflix)."

Respondents also inaccurately conflated paywalled academic research content with recent military restrictions on academic freedoms and speech:

"Content that the law deems inappropriate is still blocked, including research under copyright. ***(เนื้อหาที่กฎหมายกำหนดว่าไม่เหมาะสมซึ่งเข้าถึงไม่ได้อยู่แล้วก็ยังคงปิดกั้นอยู่ รวมถึงงานวิจัยที่ติดลิขสิทธิ์ด้วย)"***

One would-be survey respondent even perceived the unavailability of this study's survey as government censorship. Having attempted to access the survey after it was closed, he emailed the authors to express concern that the survey had been blocked by the military government.

Interview responses elaborated on the nature of this uncertainty. When asked how she assesses what content is blocked and who has blocked it, Interviewee #9 said:

"I have no idea. But I just assume that maybe it's a government block. I don't know what websites are blocked or who blocks them. But I see from Facebook that there are blocks happening. ***(ไม่ทราบเลยแต่ว่าแค่คิดไปเองว่าเอออาจจะเป็นรัฐบาลบล็อกอะไรยังเงี้ยไม่ทราบเลยว่าเว็บไซต์ไหนโดนบล้อกหรือใครบล็อก แต่เห็นจากในเฟซบุ๊คว่ามีการบล็อกเกิดขึ้น)"***

Survey and interview responses also pointed out inconsistent and unpredictable government motivations for censorship, which could contribute to difficulty assessing who is blocking what content and why. Various respondents called blocked content "random," "blocked for no reason," and "benign," and observed that "the block comes up when you least expect it." One respondent simply summed up blocked content as being "about things that the government dislikes. (***เกี่ยวกับเรื่องที่รัฐบาลไม่ชอบใจ***)"

Without explicitly asking survey respondents to list blocking actors in addition to blocked content, this finding remains ambiguous. Nevertheless, this pattern suggests that user perception and experience of blocked content can be similar regardless of actor. Further, respondents did not have formal resources to help them determine the actors and methods behind blocked content, a problem we revisit in Section 6.

5.2.4. Social Media Precautions. Respondents reported taking extensive precautions on social media to protect themselves from both the government and politically motivated peers. Lacking technical protections, respondents focused on social management and self-censorship.

Some observed government censorship shifting away from direct blocking as users increasingly move toward social media:

"Fewer websites are blocked because there are different communication channels that are hard to block, like social media such as Facebook. ***(เว็บไซต์เหมือนจะถูกบล็อคน้อยลงเพราะว่ามีช่องทางอื่นในการสื่อสารที่บล็อคได้ยาก เช่น โซเชียลมีเดียส์ เช่น เฟซบุ๊ค)"***

In addition to monitoring privacy settings and limiting one's "friends" or "followers," respondents employed several self-censorship strategies on social media, including: avoiding posting content about controversial topics; posting content for a "trial period," monitoring peer response, then taking it down or revising it if necessary; using abbreviations and nicknames to refer to royal and political figures; and carefully considering what they like, share, or otherwise repost.

Interviewee #11 described his thought process:

"If it's something about the monarchy, I have never posted or shared or liked it at all, because I know that if I do something like this in Thailand it's very dangerous—anything about the monarchy or the stability of the government. I have never expressed opinions or even clicked 'like' on other people's posts because it's so dangerous. ***(ถ้าเป็นอะไรที่เกี่ยวกับสถาบัน ผมจะไม่เคยโพสหรือแชร์หรือว่ากดไลค์เลยเพราะรู้ดีว่าถ้าทำอะไรพวกนี้ในไทยนี่อันตรายมาก อะไรที่เกี่ยวกับสถาบันหรือว่าความมั่นคงของรัฐบาล ผมจะไม่เคยแสดงความเห็นหรือแม้ถ้ากดไลค์โพสที่คนอื่นโพสเพราะว่ามันอันตราย)"***

Respondents who managed group pages or other public forums also censored others in order to mitigate their own risk as intermediaries. Interviewee #4 referenced popular online newspaper *Prachathai*'s notorious intermediary liability case in describing her own monitoring efforts as a Facebook group administrator:

"For a while I managed a Facebook page for journalists, and we had to put in a pretty strict word filter just in case anyone was going to write anything lèse majesté-related and we couldn't remove it in time. Because our prime minister has already said, this moderator for a Thai newspaper hadn't removed these insulting remarks to the monarchy and she was sentenced to several years in jail."

This finding highlights the censorship-related threats that remain even after users have achieved passive access to content. Instead, respondents felt most at risk when they tried to actively create and share information.

5.3. Threats

The threats that respondents described fell into two distinct categories: experienced threats and perceived threats. The threats that respondents had directly experienced were almost exclusively related to their peers and social media. Perceived and hypothetical threats, on the other hand, revolved around unclear conceptions of government capacity and will. We also identify overlooked threats, which respondents implied but did not directly recognize in their responses.

5.3.1. Experienced Threats. Although peer monitoring and reporting posed the most immediate threat to respondents, this was the area where they most lacked the technical means to protect themselves.

Descriptions of actual experiences and threats came out primarily in interviews. These threats included simply getting "unfriended" on Facebook, having one's posts blocked or removed, public shaming, and being reported to administrators, platform providers, or local authorities. Interviewee #5 described an experience with public shaming:

"It was an article about someone online who had mocked the king's dog, the one that's very famous and they make movies about it. And he got lèse majesté for that. Everyone finds it ridiculous, but no one talks about this kind of thing. So I wanted to say that this is ridiculous, and the words that I put online were pretty satirical, and to this royalist friend it seems like I'm mocking the king. He shared it on his own Facebook account, and he was like, 'I cannot accept this kind of behavior from someone I know. If you don't like the king, you need to get out.' His post gained 150 likes. I felt pretty bad about it."

Although respondents also had concerns about the Thai social forum Pantip, popular mobile messaging app LINE, and comment sections of news sites, Facebook was the most common thread among several aspects of censorship and self-censorship. On Facebook, respondents ran into blocked links, had their own content blocked by group administrators and even Facebook itself, and were reported on or exposed by peers. Of the 15 survey respondents who reported having posted something online that was later blocked, 9 were censored on Facebook.

Facebook's popularity among Thai Internet users poses a challenge to widespread adoption of alternative, censorship-resistant social media platforms, but also presents opportunities for simple but powerful changes to protect users. We discuss related recommendations in more detail in Section 6.

5.3.2. Perceived Threats. Respondents who feared government surveillance described general, hypothetical concerns and threats that they had not directly experienced. Only one survey respondent reported having been summoned for "attitude adjustment for the military government," and no interview respondents reported having experienced direct concrete threats. Thus, these findings cannot specify the technical realities of government adversaries' capacity and will. Rather, we report how respondents perceived government capacity and will, and these perceptions' powerful role in shaping online practices.

While respondents consistently described government monitoring as a serious threat, uncertainty and self-contradiction about the exact nature of that threat dominated responses:

"Although speeds have increased, recently paranoia has increased as well. I can't help feeling it is all being monitored. Whether that is real or not, I am not sure…but it is a daily concern and shouldn't be."

Few respondents directly cited the widely publicized stories of high-profile activists, journalists, dissidents, or academics whom the military government has summoned, arrested, and jailed. Instead, their fears revolved primarily around knowledge of friends' and family members' experiences with arrest, imprisonment, "attitude adjustment," theft or seizure of devices, military summons, police violence, and disappearance.

Respondents were most concerned about using public wifi, the prospect of a single international gateway, and man-in-the-middle (MITM) attacks on proxies and Tor.

Public Wi-Fi. Respondents felt watched and unsafe while using public wifi at airports, coffee shops, and other public spaces where users are required by Thai law to register their identity before using a network. Interviewee #12 said:

"I don't feel safe to give my ID to just use the wifi. It's like they can track what I'm doing. Let's say you give someone your personal ID, for example passport ID, to use wifi, so they can associate all of the action that you are doing with that wifi to you. So I have a feeling that they can track us whenever they want."

None, however, reported knowledge of any attacks or consequences as a result of using public wifi.

Single Gateway News. Respondents also reported feeling more restricted online after government plans for a single international Internet gateway were leaked in October 2015. Although respondents were concerned about the expanded censorship and surveillance capabilities a single gateway would allow, they had doubts about the government's ability to implement it. Interviewee #7, while sure about current government capacity, was uncertain about the future:

"As far as I know, the government has an interest in surveilling the public. But right now they do not have sufficient capacity—I am not sure in the future. Once the government has the ability to eavesdrop on the public, will Thailand have a 'great firewall' like China? I'm afraid it will be like that—a single gateway. ***(หที่ทราบมาก็คือรัฐบาลมีความสนใจที่จะดักฟังประชาชนแต่ว่าตอนนี้รัฐบาลยังไม่มีศักยภาพเพียงพอที่ผมไม่แน่ใจว่าในอนาคตหลังจากที่รัฐบาลมีความสามารถที่จะดักฟังประชาชนแล้วเนี่ยประเทศไทยจะมีเรดไฟร์วอลเหมือนประเทศจีนรึป่าวซึ่งผมกลัวว่ามันจะเป็นแบบนั้น ซิงเกิ้ลเกทเวย์)*** *"*

Man-in-the-Middle Attacks. Overall, respondents were aware of but uncertain about the possibility of surveillance via censorship circumvention and anonymity tools. Several interviewees asked the interviewers about the protections various censorship resistance tools offered. Interviewee #6 asked:

"Here's a question I wanted to ask you. Will they [the government] be able to track me when I use a proxy?"

Others were more concerned about commercial or criminal interception than government surveillance. Interviewee #11 was the most vocal:

"If it's from the government, I'm not very interested. I don't really care. Because I don't care or I'm not afraid that I'll be tracked by the government. But I am more afraid that some man in the middle will want to know more about my usage behavior. I care about privacy more, that I might have to reveal something to the proxy, more than I care that the government or someone will track where I go. (ถ้าเป็นจากรัฐบาล ผมไม่ค่อยจะสนใจ ไม่ค่อยแคร์ เพราะว่าผมไม่ค่อยสนใจ หรือไม่ค่อยกลัวว่าจะถูกแทรคจากรัฐบาล แต่กลัวมากกว่าว่าจะทำให้ใครบางคนที่อยู่ตรงกลางเค้าอยากจะรู้ พฤติกรรมการใช้งานของเรามากกว่าแคร์เรื่องของไพรเวซี่ที่จะต้อง เปิดเผยอะไรบางอย่างให้กับตัวพรอกซี่มากกว่าแคร์ว่าจะโดน รัฐบาลหรือใครก็ตามแทรกได้เราว่าไปที่ไหน)"

Two interviewees were knowledgeable about the Tor network's structure of routing Internet traffic through random "nodes" before running through an "exit node" to the open Internet, and were most concerned about the risk of malicious exit nodes. However, even these technically savvy respondents shared general uncertainty about government capabilities.

5.3.3. Overlooked Threats. Finally, we report censorship-related threats that respondents overlooked but that are feasible given the history and known capabilities of Thai government adversaries: government phishing via block pages, Tor fingerprinting, and malicious proxies.

Notably, these threats would all function to select and surveil users who attempt to access blocked sites or use circumvention and anonymity tools. While no formal consequences for simply attempting to access blocked sites are on record [22], such measures would be a logical next step in the expanding crackdown on lèse majesté, and thus are worth monitoring and preparing for.

Government Phishing via Block Landing Pages. Some respondents inaccurately assessed the actors behind various blocked content. Respondents reported mostly false positives (i.e., thinking that geoblocking or website shutdown was actually government censorship), but with a concerning potential for false negatives (i.e., thinking that state blocking was actually benign). The government has already taken advantage of this uncertainty to phish and otherwise deceive users with block pages. After the 2014 coup, the Thai Royal Police temporarily linked a clumsy-but-effective phishing application to a government block page to gather users' email addresses and gain application-level access to Facebook profile information [39]. An even more convincing phishing effort would not be outside government capabilities.

Tor Traffic Fingerprinting. While some respondents were concerned about malicious Tor exit nodes, none discussed the related threat of Tor fingerprinting [42]—that is, sniffing encrypted traffic patterns via traffic analysis to determine what site(s) an anonymous user is visiting.

Malicious Proxies. Given some respondents' risky tool selection habits, the government has an opportunity to covertly promote a bogus proxy. Thailand already blocks proxy services and resources to a limited extent, indicating some government awareness of proxy use in the country. Further, the government could take advantage of users' incident-driven tool selection and orchestrate stricter censorship to drive users to a malicious tool.

5.4. Unresolved Problems

Throughout surveys and interviews in particular, respondents pointed out security problems that persisted despite the technologies and strategies they already employed.

5.4.1. Blocked Content Assessment. When discussing confusion around identifying blocking agents and mechanisms, respondents requested a tool to help them better classify websites before they visit them. The goal was to assess what kind of inaccessibility they were encountering (e.g., government censorship, geoblocking, technical problems, website takedown, etc.), particularly with regards to where content is hosted, whether or not it may be blocked, and what actors or processes might be responsible for the blocking. Interviewee #2 specifically wanted "some knowledge of whether or not I'm being tracked" on a particular website. Without a clearer understanding of censors and causes of blocking, users could not select appropriate tools, accurately understand what and how much their government and censoring, or assess the dangers, if any, that accessing blocked content might pose.

5.4.2. Circumvention Tool Selection. Respondents' common reactionary strategy of searching for a new proxy or other tool every time they encountered blocked content gave them more opportunities to be compromised by malicious or unreliable tools. Interviewees were aware that this was not an optimal strategy, but did not perceive any better, immediately available alternatives. Several interviewees asked interviewers for tool selection advice, with questions about malware, suspicious ads, and trustworthy sources beyond Google searches.

5.4.3. Safe Social Media Engagement. With social media posing the most common directly experienced threat to respondents, their outstanding needs largely concerned protecting interactions in that medium. When writing and speaking about monitoring on social media, respondents were especially concerned about the permanence of their online interactions. Interviewee #4 described her concerns about one-to-many communication that leaves "traces":

"I am most worried about any sort of interaction that leaves a trace. That includes clicking 'like' on Facebook posts all the way to posting comments. Messaging software that is secure, messages that disappear—that would make it easier for me to communicate. Snapchat is not a big thing in Thailand, but I wonder if the anonymity of it is boosted."

Few respondents pointed out encryption as a useful current or potential protection. Passwords, whether to online accounts or for encryption keys, were not generally seen as an effective defense against government force; Interviewee #12 described friends who, when responding to military summons for "attitude adjustment," were forced to give authorities their social media credentials.

5.5. Additional Observations

Surveys and interviews revealed additional aspects of respondents' relationships with Internet censorship. These observations contribute more dimensions to a discussion about the most appropriate responses to respondents' censorship-related security problems.

5.5.1 Censorship and Self-Censorship. Both quantitative and qualitative survey evidence suggest a correlation between the censorship that the government imposes on users and the censorship that users impose on themselves. Nearly 70 percent (n=160) of all respondents reported having decided not to post something online for fear of the law. Multiple-choice survey responses indicate those who encountered blocked content more often were statistically significantly more likely to be part of this 70 percent (Goodman-Kruskal's gamma, 95% CI [0.247, 0.595], gamma = 0.421, $p < .05$). This pattern shows not only statistical significance but also ordered correlation, with self-censorship increasing as exposure to blocked content increases.

Interviews and surveys elaborated on this potential connection between censorship and self-censorship. One survey respondent wrote:

"There are too many blocked sites. It feels like being monitored at all times."

Interviewee #1 further described the connection:

"The effect of political blockages is really pretty dramatic. I think less so the overt blockage, but rather self-censorship and how that affects how people access information."

Neither number of years on the Internet, amount of time spent online per day, nor the experience of having one's own content censored, exhibited the same explanatory significance for self-censorship as did frequency of exposure to blocked content. Nationality was also not a statistically significant variable to explain self-censorship; Thai respondents were not statistically significantly more likely to self-censor than foreign respondents.

This correlation between self-censoring behavior and exposure to censorship, however, still does not entirely explain tendencies to self-censor. Even respondents outside of Thailand, who presumably do *not* encounter Thai Internet censorship and geoblocking regularly, were as likely to self-censor as those in Thailand. Interviews with respondents both in and outside Thailand confirm this pattern, which further triangulates with reports of the Thai government intimidating Thai citizens abroad. With a small sample (n=27) of respondents answering from outside the country, however, the role of location in self-censorship merits further investigation.

5.5.2. Blocked Content's Symbolism. Patterns in survey responses indicate that blocked content was symbolic and meaningful even for respondents who did not want or need to access it. This underscores this paper's overall assertion that users' interaction with censorship goes beyond attempts to access blocked content: censorship affected the behavior of even those respondents with relatively little interest in blocked content.

The British tabloid the Daily Mail, which was blocked wholesale shortly after the 2014 coup for publishing a sensitive video of the Crown Prince and his then-wife at a birthday party for their dog, provides a case study. The Daily Mail dominated survey responses regarding blocked content, with about 25 percent (n=58) of respondents listing it as an instance of blocked content.

Of those respondents who mentioned the Daily Mail, half (n=26) listed no other website or type of website, appearing to use the Daily Mail as shorthand for censorship in general. For example, in response to a question about how the Internet in Thailand has changed over time, one respondent wrote:

"Pretty much the same, except for the Daily Mail."

Interviews further revealed the Daily Mail's status as a symbol of web censorship in Thailand. Interviewee #5 said:

"But after the coup, I forgot what led to the block, but we can't access Daily Mail anymore. It's one of those sites that we think of right away when we think of blocked sites. It's the first thing that comes to mind. It really represents something. I don't know why."

A survey respondent took this association further to associate the Daily Mail with a right to access foreign news:

"The Daily Mail is a normal news website. But it's our right to get news from other countries, not just domestic news agencies. ***(เดลี่เมล์ก็เป็นเว็บไซต์ข่าวธรรมดา แต่มันคือสิทธิ์ที่เราจะรับฟังข่าวจากต่างประเทศ ไม่ใช่เพียงแค่สำนักข่าวจากในประเทศเท่านั้น)****"*

Surveys and interviews also surfaced the "mythical" nature of the Daily Mail. Of the 58 survey respondents who listed it as an instance of blocked content, nearly a quarter (n=13) had never attempted to circumvent censorship. Further, of thirteen interviewees, only one had ever visited the Daily Mail's website before it was blocked.

This "mythical" status was not limited to the Daily Mail, but rather was a common conception of blocked content in general. Interviewee #8 spoke about a “legendary” political opposition website Kon Mueng Gan:

“Kon Mueng Gan—it sounds like a legend because it was closed down and I haven’t been able to retrieve the archives since. But it has always been mentioned in blogs and journals.”

Interviews also revealed the significance of what is not blocked. Interviewee #3 expressed surprise that newspapers Prachathai and Khao Sod were not censored more aggressively. Interviewee #8 speculated that the government let them and other alternative groups remain accessible in order to “keep track of what the opposition is doing.”

5.5.3. Disapproval of Censorship and Desire for Other Information Controls. Most survey respondents disapproved of existing government censorship, but those same respondents also expressed desire for other types of information controls. Both survey and interview respondents voiced frustration with “uncontrolled,” unreliable content on the Internet, including fraud, hate speech, rumors, and commercial promotion of off-market pharmaceuticals, weapons, and other unregulated goods.

Several respondents blamed increased use of social media in Thailand, with one survey respondent referring to it as a “double-edged sword”:

“Internet users in Thailand use social networks more and more, both the older and younger generations. But it's a double-edged sword because of the risk of fraud and political conflict becoming more widespread.
(ผู้ใช้อินเทอร์เน็ตไทย ใช้งานเครือข่ายสังคมเพิ่มมากขึ้น ไม่ว่าคนรุ่นเก่ารุ่นใหม่ก็ใช้แต่ก็เป็นดาบสองคม เพราะเสี่ยงต่อมิจฉาชีพและความขัดแย้งทางการเมืองก็เกิดขึ้นอย่างกว้างขวาง)”

Survey responses further indicate that current government censorship did not align with users’ demands for some level of information screening. One Thai survey respondent wrote:

“ICT laws are used to suppress expression but are never used to stop the fraud.”

Interviewee #7 placed these motivations in terms of the government protecting itself rather than protecting users:

“I feel that the government might want to make us follow the law in order to protect themselves. ***(คือรู้สึกว่ารัฐบาลอาจจะต้องทำตามกฎหมายอ่ะคะเพื่อป้องกันตัวเอง)”***

Overall, responses suggested potential support of—or even demand for—censorship or restrictions of some kinds of content. In this way, respondents did not fall into entirely pro- or anti-censorship camps.

6. Discussion

In addition to informing broader implications and conclusions, the results above serve as a foundation for reflecting on the technical directions and future research that will best serve users of the Internet in Thailand.

6.1. Broader Implications

Here we discuss how objectives in anti-censorship research can shift to better serve users: by prioritizing engagement as well as access, designing with user perceptions as well as technical realities in mind, and aiming for flexibility rather than “one-size-fits-all” solutions.

6.1.1. Objectives Beyond Access. Existing technology was generally adequate to circumvent censorship in Thailand and give respondents access to blocked content. Threats and problems came when they attempted to safely select tools and understand, create, and disseminate information in a censored environment. This echoes Al-Saqaf’s [2] critical conclusion that circumvention tools’ “ability to unblock websites is insufficient to address…the many new forms of Internet censorship.” Instead, the security community must broaden its objectives in censorship work to not only help users access content, but also protect users when they engage with that content. Technology alone cannot solve this problem that finds its roots in broader systems of political and social control.

6.1.2. User Perceptions versus Technical Realities. This study’s findings illuminate potential gaps between user perceptions and technical realities of government adversaries’ capacity and will. Crucially, vague perceived threats from the government shaped respondents’ behaviors alongside clearer, directly experienced threats from peers. Thus, the development and design of circumvention tools must address not only the technical censorship apparatus, but also the user perspectives that determine behavior within it. This disconnect between perceptions and realities also presents an opportunity for circumvention tools to serve an educational purpose, helping users accurately assess censored content and more make informed decisions about how to engage with it.

6.1.3. No “One-Size-Fits-All” Solutions. We find that respondents’ attitudes cannot be characterized as wholly pro- or anti-censorship, which suggests that there can be no one-size-fits-all solution in either censorship or resistance to it. Respondents who otherwise opposed censorship expressed desire for other information controls, exhibiting varying assessments of what is or is not acceptable to restrict. This finding provides thorough, country-level confirmation of Shen and Tsui’s [50] recent survey finding that popular support for freedom of expression coexisted with pro-censorship attitudes among Internet users in several Asian countries.

Respondents also employed distinct repertoires of censorship circumvention, anonymity, and self-censorship strategies, with respondents selecting different tools at different times for different content. Below, we recommend future technical and research directions that account for this variety.

6.2. Technical Directions and Future Research

Survey and interview findings motivate technical directions and future research grounded in respondents' practices and threats. Our goal with these recommendations is not to pinpoint any single "right" approach, but to start a dialogue about the strengths and weaknesses of different strategies to give users more freedom to access and engage with censored content.

6.2.1. Content Assessment. Respondents expressed confusion between government censorship and geoblocking, paywalling, and other restrictions on Internet content. Thus, when encountering a blocked site, some respondents did not know who or what had caused the block. We therefore propose the development of methods to help users understand the reason(s) a given website may be blocked. Moreover, we propose investigating ways to do this not only (1) after the user has loaded the site, but also (2) before they attempt to access it.

The former goal (1) could be accomplished within the browser alone. Building on Jones et al.'s work automatically fingerprinting block pages [24] and leveraging other information available within the browser, a browser extension could infer why a site is inaccessible and report that inference to the user.

In addition to information available to the browser, communication between the browser and external servers could facilitate more thorough content assessment. Both (1) after and (2) before visiting a blocked site, the user could query an external server for more information about it. For example, our respondents were especially interested in where websites were hosted and whether they appeared on any known government block lists. Given the trend of respondents encountering blocked content through links from Facebook or other websites as well as through direct navigation, the browser extension could also pre-fetch information about content linked from the user's current site.

However, particularly for the purposes of goal (2), queries to an external server could be more susceptible to government or adversary eavesdropping than any attempt to access blocked content directly. We propose studying novel approaches to safely achieve goal (2). For example, we propose studying private information retrieval (PIR) as a novel solution for this context. With PIR, the browser could query external servers without revealing the index of the queried item. Where previous work has shown that PIR is necessary for censorship resistance in systems [45], we argue it also has this application for user education toward smarter censorship circumvention. PIR still poses significant privacy challenges, however, as the number and timing of a user's queries over time could reveal information about their browsing behavior. To address these privacy challenges, such a system would need to use steganographic mechanisms and/or achieve widespread use. A related open question is whether it is possible to achieve sufficient security with lighter-weight solutions.

Overall, a tool to identify censors could help users both (1) better understand what signals indicate what kind of censorship and (2) make more informed decisions about whether or not to visit websites that may be sensitive.

6.2.2. Flexible, Readily Available Tools. Our findings suggest that respondents searched for new circumvention tools every time they encountered blocked content, and tended to install and/or use the first tools they found. Such search practices may make users vulnerable to malware and surveillance from the government or other adversaries. Therefore, we argue it is essential to deliver trustworthy tools to users *before* they need them.

While respondents' trust in Google search results for tool selection may have been misplaced, that trust in browser and service providers could drive use of official, browser-associated tools—for example, bundling uProxy with Chrome downloads or Tor with Firefox downloads.

Adaptive, flexible tools could also address tool selection challenges. Upon inferring the cause(s) of an instance of blocked content, the browser extension described above in "Content Assessment" could suggest a menu of appropriate tools to the user depending on the content they are trying to access—for example, a VPN for media-heavy content, anonymity tools for known government-censored content, or alternative searches for website shutdown.

6.2.3. Plausible Deniability on Social Media. Survey and interview responses emphasize the value of safe options for social media engagement in Thailand, particularly the need for plausible deniability in the face of dynamic threats from peers, the government, and constantly changing legal regulations. Respondents were concerned about Facebook in particular, but the actions they described (i.e., liking, sharing, commenting) are common to other social media platforms. The power of network effects suggests that alternative censorship-resistant platforms [4, 8] may not be a widely applicable solution.

Instead, there is evidence that popular social media platforms are willing to make technical changes in response to users' censorship circumvention needs and concerns. For example, Facebook's technical support for Tor access suggests that internal changes in existing social media platforms are feasible if they encourage freer use in repressive contexts [12]. In Thailand in particular, recent statements [3] demonstrate that Facebook is responsive to Thai users' security concerns about the government.

With this in mind, we make the below recommendations for alterations to existing social media platforms.

Anonymity. Instead of making likers' identities public, social media platforms could display only counts of likes, or display identities only to the original poster.

Control Over Content. To deter public shaming or other manipulation of one's content, users could designate posts that cannot be shared, liked, or commented on.

Impermanence. As an additional mitigating measure, likes, comments, and other interactions could be set to self-destruct after they have served their social purpose, e.g. after particular users have seen them. Corresponding activity history could also be set to self-destruct at regular intervals.

These user-side modifications to social media platforms cannot alone solve the larger problems of censorship and self-censorship, but can raise the bar. Further, such modifications could help move the conversation in the direction of giving users more control over their online identities and related content.

Currently, respondents' most immediate option to achieve the plausible deniability they needed on social media was strict self-censorship. Thus, our findings suggest that the above recommendations for building selective impermanence, anonymity, and control into existing social media platforms may, somewhat counter-intuitively, result in more user activity.

6.2.4. Longitudinal and Comparative Study. This study's survey instrument is designed to generalize to other settings, presenting an opportunity for rigorous longitudinal and comparative study to build on this initial sample. In Thailand, the trajectory of information controls throughout successive political crises offers a natural experiment in the making and re-making of a nation's Internet. Beyond Thailand, surveying users in other countries via this neutral, non-political survey instrument can help build more precise metrics for understanding how users in different countries and settings experience Internet censorship.

7. Conclusion

We conducted 229 online surveys and 13 in-depth interviews with users of the Internet in Thailand to learn more about how they assessed and interacted with Internet censorship. Analysis of this quantitative and qualitative data provides an in-depth examination of respondents' practices, threats, and problems related to censorship. While respondents were able to access blocked information, they faced unresolved needs in content assessment, tool section, and action on social media. Our results highlight simple but powerful steps the security community can take in response. This study provides a foundation for future research toward implementing those steps. The broader lesson of this study is the value of area-focused engagement with real users, and the empirical grounding it can give to the development and delivery of more user-focused anti-censorship tools.

Acknowledgements

We are especially grateful to: our anonymous second author, for their commitment to this project despite its sensitive and controversial nature; several native Thai-speaking teachers and colleagues, for assisting with translation, verification, and transcription of survey and interview responses and materials; Art Suriyawongkul, Aim Sinpeng, and C.J. Hinke, for their generous consultation and guidance; to the UW Security and Privacy Research Lab, for several rounds of valuable feedback and discussion; and the survey and interview respondents, for lending us their time and experience. This work was supported in part by the University of Washington Tech Policy Lab and the Short-Dooley Professorship.

References

[1] Aceto, G. and Pescape, A. 2015. Internet censorship detection: A survey. *Computer Networks: The Int. J. of Computer and Telecomm. Networking.* 83, C, 381-421. DOI: 10.1016/j.comnet.2015.03.008.

[2] Al-Saqaf, W. 2016. Internet censorship circumvention tools: Escaping the control of the Syrian regime. *Media and Comm.* 4, 1, 39-50. DOI: 10.17645/mac.v4i1.357.

[3] Asian Correspondent Staff. 2016. Thailand: Facebook denies sharing user information with military. *Asian Correspondent*. Available at: https://asiancorrespondent.com/2016/05/thailand-facebook-sharing-info-military/.

[4] Bacharach, D., Nunu, C., Wallach, D. S., & Wright, M. 2011. #h00t: Censorship resistant microblogging. Available at: http://arxiv.org/pdf/1109.6874v1.pdf.

[5] Baumer, E. P. S., Ames, M. G., Burrell, J., Brubaker, J. R., and Dourish, P. 2015. Why study technology non-use? *First Monday.* 20, 11 (Nov. 2015). DOI: http://dx.doi.org/10.5210/fm.v20i11.6310.

[6] Biernacki, P. and Waldorf, D. 1981. Snowball sampling: Prolems and techniques of chain referencing. *Sociol. Methods Res.* 10, 2, 131-163. DOI: 10.1177/004912418101000205.

[7] Bunyavejchewin, P. 2010. Internet politics: Internet as a political tool in Thailand. *Canadian Soc. Sci.* 6, 3, 67-72.

[8] Burnett, S., Feamster, N., & Vempala, S. Chipping away at censorship firewalls with user-generated content. In *Proceedings of the 19th USENIX Security Symposium*.

[9] Chen, L., Zhang, C., and Wilson, C. 2013. Tweeting under pressure: Analyzing trending topics and evolving word choice on Sina Weibo. In *Proceedings of the 1st ACM Conference on Online Social Networks*. 89-100. DOI: 10.1145/2512938.2512940.

[10] Connolly, C., Lincoln, P., Mason, I., and Yegneswaran, V. 2014. TRIST: Circumventing censorship with transcoding-resistant image steganography. USENIX Workshop on Free and Open Communications (FOCI).

[11] Deibert, R. and Rohozinski, R. 2010. Control and subversion in Russian cyberspace. In *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Eds. R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain. Cambridge: The MIT Press.

[12] Dingledine, R. 2014. Facebook, hidden services, and https certs. Tor Project blog. https://blog.torproject.org/blog/ facebook-hidden-services-and-https-certs.

[13] Erbar, P. 2014. Facebook: Top 10 cities with most users. *Tech Insider.* Available at: http://www.techinsider.net/ facebook-inc-fb-top-10-cities-with-most-users/1111266.html.

[14] Filasto, A. and Appelbaum, J. 2012. OONI: Open Observatory of

Network Interference. Presented at the 2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI).

[15] Gebhart, G. and O'Brien, D. 2016. The amended Computer Crime Act and the state of Internet freedoms in Thailand. Available at: https://www.eff.org/deeplinks/2016/12/amended-computer-crime-act-and-state-internet-freedoms-thailand.

[16] Gill, P., Crete-Nishihata, M., Dalek, J., Goldberg, S., Senft, A., and Wiseman, G. 2015. Characterizing web censorship worldwide: Anotehr look at the OpenNet Initiative data. *ACM Trans. on the Web*. 9, 1, 4:1-4:29. DOI: 10.1145/270339.

[17] Guo, S. and Feng, G. 2012. Understanding support for Interent censorship in China: An elaboration of the theory of reasoned action. *J. Chinese Political Sci.* 17, 1, 33-52. DOI: 10.1007/s11366-011-9177-8

[18] Hardy, S., Crete-Nishihata, M., Kleemola, K., Senft, A., Sonne, B., and Wiseman, G. 2014. Targeted threat index: Characterizing and quantifying politically-motivated targeted malware. In *Proceedings of the 23rd USENIX Security Symposium*.

[19] Hamnevik, A. and Persson, M. 2015. Upholding the code of ethics during censorship: A qualitative study of strategies used by journalists under the pressure of the military government. (Thesis). http://lnu.diva-portal.org/smash/record.jsf?pid=diva2%3A822002&dswid=-4325

[20] Hassid, J. 2012. Safety valve or pressure cooker? Blogs in Chinese political life. *J. of Comm.* 62, 2, 212-230.

[21] Head, J. 2015. Thai courts give record jail terms for insulting king. *BBC News*. Available at: http://www.bbc.com/news/world-asia-33819814.

[22] Hinke, CJ. Private communication. April 2016.

[23] International Federation for Human Rights. 2016. 36 and counting: Lèse majesté imprisonment under Thailand's military junta. Report No. 671a. Available at: https://www.fidh.org/IMG/pdf/fidh_thailand_report_lese_majeste.pdf.

[24] Jones, B., Lee, T. W., Feamster, N. and Gill, P. 2014. Automated detection and fingerprinting of censorship block pages. In *Proceedings of the 2014 Conference on Internet Measurement*. DOI: 10.1145/2663716.2663722.

[25] Khattak, S., Javed, M., Anderson, P. D., and Paxson, V. 2013. Towards illuminating a censorship monitor's model to facilitate evasion. Presented at the 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI).

[26] Khattak, S., Javed, M., Khayam, S. A., Uzmi, Z. A., and Paxon, V. 2014. A look at the consequences of Internet censorship through an ISP lens. In *Proceedings of the 2014 Conference on Internet Measurement*. 271-284. DOI: 10.1145/2663716.2663750.

[27] Khattak, S., Elahi, T., Simon, L., Swanson, C. M., Murdoch, S., and Goldberg, I. (2016). SOK: Making sense of censorship resistance systems. In *Proceedings on Privacy Enhancing Technologies (PoPETS),* (4):37-61. Available at: https://cypherpunks.ca/~iang/pubs/crsok-popets16.pdf

[28] King, G., Pan, J., and Roberts, M. E. 2013. How censorship in China allows government criticism but silences collective expression. *American Pol. Sci. Rev.* 107, 2, 326-343. DOI: 10.1017/S0003055413000014.

[29] Kopsell, S. and Hillig, U. 2004. How to achieve blocking resistance for existing systems enabling anonymous web surfing. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society*.

[30] Laungaramsri, P. 2016. Mass surveillance and the militarization of cyberspace in post-coup Thailand. *Austrian Journal of Southeast Asian Studies*. 9, 2, 195-214.

[31] LeBlond, S., Uritesc, A., Gilbert, C., Chua, Z. L., Saxena, P., and Kirda, E. 2014. A look at targeted attacks through the lens of an NGO. In *Proceedings of the 23rd USENIX Seecurity Symposium*.

[32] Leberknight, C. S., Chiang, M., and Wong, F. 2012. A taxonomy of censors and anti-censors, Part II: Anti-censorship technologies. *International Journal of e-Politics*. 3, 4, 20-35. DOI: 10.4018/jep.2012100102.

[33] Lincoln, Y. S. and Guba, E. G. 1985. *Naturalistic Inquiry*. Newbury Park, CA: SAGE Publications.

[34] MacKinnon, R. 2008. Flatter world and thicker walls? Blogs, censorship, and civic discourse in China. *Public Choice*. 134, 2, 31-46.

[35] MacKinnon, R. 2010. Networked authoritarianism in China and beyond: Implications for global Internet freedom. Presented at *Liberation Technology in Authoritarian Regimes*.

[36] Marczak, W. R., Scott-Railton, J., Marquis-Boire, M., and Paxson, V., 2014. When governments hack opponents: A look at actors and technology. In *Proceedings of the 23rd USENIX Seecurity Symposium*.

[37] McGregor, S. E., Charters, P., Roesner, F. 2015. Investigating the computer security practices and needs of journalists. In *Proceedings of the 24th USENIX Security Symposium.*

[38] Nisar, A., Kashaf, A., Uzmi, Z. A., and Qazi, I. A. 2015. A case for marrying censorship measurements with circumvention. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*. DOI: 10.1145/2834050.2834110.

[39] O'Brien, D. 2014. Thai junta used Facebook app to harvest email addresses. *Deep Links* by the Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2014/06/thai-junta-used-facebook-app-harvest-email-addresses.

[40] Open Net Initiative. 2007. Thailand country profile. Available at: https://opennet.net/sites/opennet.net/files/thailand.pdf.

[41] Open Net Initiative. 2012. Thailand country profile. Available at: https://opennet.net/research/profiles/thailand.

[42] Pachenko, A., Lanze, F., Zinnen, A., Henze, M., Pennekamp, J., Wehrle, K/, and Engel, T. (2016). *Network and Distributed System Security Symposium.*

[43] Patton, M. Q. 2001. *Qualitative research and evaluation methods.* SAGE Publications.

[44] Pearce, K. and Kendzior, S. 2012. Networked authoritarianism and social media in Azerbaijan. *J. of Comm.* 62, 283-298. DOI: 10.1111/j.1460-2466.2012.01633.x.

[45] Perng, G., Reiter, M. K., and Wang, C. 2005. Censorship resistance revisited. Presented at 7th International Workshop on Information Hiding (IH). Available at: http://freehaven.net/anonbib/cache/ih05-csispir.pdf.

[46] Ramasoota, P. Internet politics in Thailand after the 2006 coup: Regulation by code and a contested ideological terrain. 2012. In *Access Contested: Security, identity, and resistance in Asian cyberspace.* Eds. R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, p. 83-114. Cambridge: The MIT Press.

[47] Roberts, H., Larochelle, D., Faris, R., and Palfrey, J. 2011. Mapping local Internet control. Berkman Center for Internet & Society. Available at: https://cyber.law.harvard.edu/netmaps/mlic_20110513.pdf.

[48] Senft, A., Dalek, J., Poetranto, I., Crete-Nishihata, M., and Sinpeng, A. 2014. Information controls during Thailand's 2014 coup. (Research Brief). Available at: https://citizenlab.org/2014/07/information-controls-thailand-2014-coup/.

[49] Sinpeng, A. 2014. The Cyber Coup. In F. Aulino, E. Elinoff, C. Sopranzetti, & B. Tausig (Eds.), *The Wheel of Crisis in Thailand*. Available at: https://culanth.org/fieldsights/568-the-cyber-coup.

[50] Shen, F. and Tsui, L. 2016. Public opinion toward Internet freedom in Asia: A survey of Internet users from 11 jurisdictions. Berkman Center Research Publication No. 2016-8.

[51] Shklovski, I. and Kotamraju, N. P. Online contribution practices in countries that engage in Internet blocking and censorship. In

Proceedings of the SIGCHI Conference on Human Factors in Computer Systems. ACM, 2011, 1109-1118. DOI: 10.1145/1978942.1979108.

[52] Tschantz, M. C., Afroz, S., Anonymous, and Paxson, V. 2016. SoK: Towards grounding censorship circumvention in empiricism. In *Proceedings of the 27th IEEE Symposium on Security and Privacy.*

[53] Verkamp, J. and Gupta, M. 2012. Inferring mechanics of web censorship around the world. Presented at the 2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI).

[54] Ververis, V., Kargiotakis, G., Filasto, A., Fabian, B., and Alexandros, A. 2015. Understanding Internet censorship policy: The case of Greece. Presented at the 5th USENIX Workshop on Free and Open Communications on the Internet (FOCI).

[55] Wang, D. and Mark, G. 2015. Internet censorship in China: Examining user awareness and attitudes. *ACM Trans. On Computer-Human Interaction*. 22, 6 (Nov 2015), 31:1-31:22. DOI: 10.1145/2818997.

[56] Wikileaks Staff. (2007). Internet censorship in Thailand. Available at: https://wikileaks.org/wiki/Internet_Censorship_in_Thailand

[57] Zhen, K. 2015. Estimating self-censorship on social media in China: A survey experiment. (Thesis). Available at: http://www.politics.as.nyu.edu/docs/IO/5628/Thesis.Zhen.Kevin.pdf