

*UNDERSTANDING
INTERNET
FREEDOM:
VIETNAM'S
DIGITAL
ACTIVISTS*

SECONDMUSE



OPEN TECHNOLOGY FUND



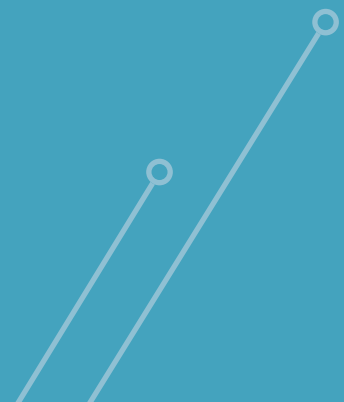
Radio Free Asia

TABLE OF CONTENTS

2	Executive Summary
4	Meet the Bloggers
8	Key Insights and Recommendations

APPENDIX: A DEEPER UNDERSTANDING

13	Our Human-Centered Design Process
15	Building an Understanding



EXECUTIVE SUMMARY

To effectively serve community or an individual, one must first meet them where they are. Meeting them where they are means understanding their goals, the motivations behind them, the barriers in front of them, and the perceptions surrounding them. It is with this understanding that one can most effectively serve the community in moving forward. In Internet freedom, this deep understanding of the communities and individuals is often lacking. Designing tools and programming to effectively serve them can be especially challenging as a result.

This report helps combat that challenge. It provides a concise understanding about the motivations, behaviors, threats, and needs of Vietnam's digital activists through the lens of a diverse group of six high profile bloggers. In May 2014 these activists visited Washington DC with a coalition of NGOs, consisting of Access, Electronic Frontier Foundation, Reporters Without Borders, Radio Free Asia and Viet Tan. SecondMuse and Viet Tan, the Vietnamese pro-democracy organization, collaborated on a Needfinding process to coincide with this visit in order to establish an understanding that can be shared with the wider community of organizations and individuals fighting for Internet freedom around the world.

These bloggers face significant risks. Vietnam currently imprisons more than 30 online activists, and the government penalizes a range of activities from political commentary to sharing info on social media. All of the bloggers we met have at some point fallen victim to arrest, harassment and other varieties of persecution as a result of their online activities.

SecondMuse employed a Needfinding process for this work based on the human-centered design approach to research: an empathy-based approach that puts the motivation and mission of a community at the center. We focused our research around a series of key research questions, such as “What does it

mean to a blogger to be safe and secure?” and “What are the security-related behaviors that the bloggers employ in their daily communication activities?” We then designed a series of interviews, activities, and collaborative exercises to draw out a deep understanding of these bloggers. We then took this understanding and determined a series of key insights for the greater Internet freedom community of software developers, intermediaries, funders, and trainers to understand in order to even better serve this community.

We developed a broad understanding of how these bloggers understand security, and interact with communication technology in service of their goals. Most bloggers did not understand or utilize encryption, but they did employ a range of self-guided security mechanisms such as regularly changing passwords and holding different email accounts for different personal and professional purposes. While the bloggers may not widely use tools such as the Tor Project, they do have their own established means for identifying government backed agitators who invade their online discourse.

This broad understanding is also synthesized into a number of key points for different audiences seeking to serve this community. This includes key recommendations for developers and organizations seeking to serve the activists. For developers, we discuss how the risks of shared devices and physical device confiscation must be paramount considerations when developing new tools. For intermediaries and trainers, we discuss the value of family-based metaphors for privacy and security concepts. We discuss the power of “feeling” secure and the role personal trust plays in the dissemination of information and adoption of communication tools. These points and more can be found in the final section.



MEET THE BLOGGERS

In marking 2014 World Press Freedom Day, a coalition of free expression organizations sponsored six Vietnam-based bloggers and digital activists to come to the U.S. for a series of educational and human rights activities in Washington, D.C. and New York. During their three week stay in the US, they participated in a range of activities including meeting at Congressional offices, UN human rights office, and various human rights organizations to share first hand accounts of their day-to-day hardships, as well as relay concrete suggestions for furthering freedoms in Vietnam. They also testified at a congressional briefing on “Media Freedom in Vietnam” and held a public seminar at Radio Free Asia to mark World Press Freedom Day. In addition to these events, the trainers participated in extensive digital security and citizen journalism training events.

The bloggers made up a diverse group--five men and one woman, ranging in ages from 26 to 71, and from various parts of the country, primarily urban but with some rural representation as well. Their activism ranges from independent journalism to shining light on corruption and human rights abuses on Facebook to expounding facts and setting historical records straight to lending support and visibility to pro-democracy activities. Many of the bloggers are part of the rising middle class in Vietnam and through their activism they address day to day grievances with the Vietnamese government. In spite of the great diversity of characteristics and activities represented within the group, their motivations illustrated a similar theme--that of ordinary people called to extraordinary action.



LE THANH TUNG (Anthony Le), born 1977, is a freelance journalist and digital activist based in

Saigon. He is a contributor to the Vietnamese Redemptorists' News (www.chuacuuthe.com), a popular citizen journalist platform. He writes on issues of religious freedom, corruption, and political persecution. As a result of his blogging, security police raided his place of work and pressured the management to end his employment in 2013.



Anthony was motivated to become a blogger and independent journalist in 2008 upon reading in the news that the Vietnamese authorities had attacked a Catholic parish in Hanoi. Touched by the information, he went to the site to learn more and shared the information he learned online.

That turned into his first article and later he and a few colleagues went on to join the Vietnam Redemptorists media network to train independent journalists and shed light on social issues in Vietnam.

NGO NHAT DANG, born 1958, is a writer and freelance journalist based in Hanoi. He

is a contributor to the BBC Vietnamese section. As a university student, he was drafted into the People's Army of Vietnam (PAVN) and served in the 1979 border war with China. He is publishing a history of the Army of the Republic of Vietnam (ARVN) in which he explores efforts by the Hanoi communist government to reconcile with China but not with Vietnamese compatriots who fought on the other side of the civil war.

Dang saw a group of young people protesting Chinese aggression against the Vietnamese islands many years ago and so admired their passion that he sought to learn more and felt responsibility to begin speaking out himself.



NGUYEN DINH HA, born 1988, is a blogger and digital activist from Hanoi. He utilizes various online

platforms to post news and commentaries on life in Vietnam. He is a graduate of Hanoi Law University. He has participated in advocacy meetings with Hanoi-based foreign embassies and international NGOs.

He is a member of the Network of Vietnamese Bloggers and the Democratic Party of Vietnam. Since 2011, he has been harassed by police for his online critiques and offline participation in public demonstrations.



Ha was in college doing reading on the internet when he came to realize the many inaccuracies in way Vietnamese state media treated topics from the Vietnam/China border dispute to facts of Vietnam's history. Ha says "I have an itchy mouth," --a desire to expose fraud or falsity where he sees it. That feeling of responsibility led him to start using social media and blogging platforms to share his concerns on social and legal issues.

NGUYEN THI KIM CHI, born 1943, is an actress, director and playwright living in Hanoi.

A member of the Vietnamese Communist Party for over four decades, she starred in communist propaganda films during the war. In recent years, she became disillusioned with the corruption and repression of the regime.

Kim Chi was thrust into pro-democracy activity when her conscience prompted her to decline an award for her work from the Vietnamese Prime Minister in protest against government oppression. She stated that she did not want “the signature of someone who caused misery to this country and its people” in her home. She does not call herself an activist, yet her sharing of news on government corruption through Facebook has gained a following of thousands both in Vietnam and internationally.



NGUYEN TUONG THUY, born 1952, is a military veteran, poet and writer. He blogs

on social injustices in Vietnam, often speaking up for those who are voiceless. His blog is among the most read in Vietnam and, as result, he has been repeatedly harassed and interrogated by security police. His blog is also the target of constant hacker attacks. He participates in a number of unsanctioned civic groups including: Bau Bi Tuong Than Association, Brotherhood for Democracy, Civil Society Forum, and Network of Vietnamese Bloggers.


Thuy was a freelance journalist for many years and witnessed firsthand what he felt was cronyism and lack of journalistic integrity within Vietnam’s state media. Those frustrations led him to become an independent blogger to expose what he saw as the true facts.



TO OANH, born 1948, is a blogger and former contributor for state-owned newspapers in his home province of Bac Giang, northern Vietnam. After retiring as a high school geography and computer science teacher, he began covering government corruption under various pen names for citizen journalism sites. A Buddhist, he has written extensively about the injustices and faced by Vietnam’s Catholic community, especially the problem of Church properties confiscated by the government.

As a computer science teacher, Oanh was often the first in his rural area to have access to new technology, including the Internet. As a result he received requests to verify information and events, and that access and research led him to begin contributing to blogs and websites.





It is hard for the reality of the threat that these bloggers face to be understated. The bloggers engage in activism and endeavor to make their voices heard in an environment where pro-democracy activity and online political debate is actively suppressed. Bloggers who question or challenge government policy and action are routinely persecuted, facing harassment, interrogation, arrest and potentially imprisonment.

According to Freedom House, there are more than 30 online activists currently imprisoned in Vietnam and the lengths of sentences handed down have been increasing. Government decrees passed in recent years have further constrained bloggers' freedoms by penalizing social or political commentary, the dissemination of press or literature. Government powers of surveillance and censorship have increased by compelling Internet service providers (ISPs) to comply with government censorship, including intermittent blocking of Facebook. Not only that, the three primary ISPs in Vietnam which accounting for 95% of online traffic in the country are owned by the government or military. The mobile marketplace is similarly dominated by 3 government-owned providers, further undermining the presumption of confidentiality of any client information or data. Meanwhile cyber attacks on websites and individual bloggers using malware are becoming commonplace and the government freely admits employing numerous "opinion-shapers" whose specific job is to antagonize and undermine activists through argumentation and comments to discredit them.

All of the bloggers we met with were known activists of a relatively high profile with a following or community whom they have the potential to influence and educate, however not so high profile that the Vietnamese government would actively prevent them from leaving the country. Each blogger has at some point fallen victim to arrest, harassment and other varieties of persecution, including lost employment and economic opportunity, as a result of their online activities. All of the bloggers were aware that their actions were routinely monitored by the government, from surveillance of phone lines to being targeted by malware attacks and government opinion-shapers. This awareness actively informs whether and how they choose to protect information and activity on the Internet.

In spite of the constant threat of arrest and interrogation, the bloggers remained staunch in their commitment to digital activism. They all use the internet on personal computers at their homes and they universally expressed that the internet was the primary medium for much of their communication, as well as for surfing the web and reading news on both foreign and domestic sites, and for posting on their blogs and Facebook.

KEY INSIGHTS AND RECOMMENDATIONS

The following is a synthesis of learnings that result from our process of understanding. We have organized them as they relate to a general audience seeking to better understand and engage with the user community that these bloggers represent, developers seeking to build and deploy tools, and supporting organizations seeking to better design supporting programming such as training and outreach.

Reading the appendix is strongly encouraged to fully understand the context of this section. These insights and recommendations are best understood within the context in which they were drawn.

KEY INSIGHTS ON ENGAGEMENT WITH INTERNET FREEDOM AND SECURITY TECHNOLOGY

When faced with questions over their ability to communicate securely, bloggers will generally choose to communicate anyway.

There are a number of reasons for this behavior, but the overall point is consistent. The bloggers regularly face great danger in order to achieve their work - work which is conducted through communication, whether it be blogs, social media, in-person gatherings, or phone calls. This willingness to face risk means that they will not necessarily hold back when their communication security is in question.

The “feeling” of security has a significant impact on the bloggers’ desire to embrace a communication tool. We learned repeatedly that some of the most profound experiences related to communication security are those that instill a strong feeling of security in the user. The only blogger who regularly utilized the Tor Project explained a sense of joy when he checks his IP address after connecting to the network and seeing that his IP address is visibly associated with the country in which the exit node is stationed. Another very common behavior is the deletion of chat history, and that receiving visual feedback that a chat message has been “removed” on their local machine and the recipient made them feel secure. The feeling of security can be different from the reality of security - but it is the feeling that is a major factor in evoking continued use of a communication tool. For example, one blogger also indicated feeling that she was more at risk with Yahoo! as an email provider as she saw lots of spam in her inbox. Switching to Google, where she does not see the spam in her primary inbox, and therefore is unaware of it, has made her feel safer.

Trust in the provider of a communication tool has a profound impact on usage of the tool, and trust as a concept runs deep culturally. Gmail is the most widely used email platform among the bloggers. Many used to use Yahoo! Mail but two key events changed that. First, news broke of Yahoo!’s role in the jailing of a Chinese journalist. Second, was Google’s refusal to hand over information requested by the Vietnamese government. This prompted bloggers to leave one platform for the other, and all of the bloggers expressed a great amount of trust in Google and cite it as the primary reason they utilize the service. But trust as a concept

goes deeper than whether a provider has done something right or wrong. Some bloggers expressed the need to trust a tool or service provider. They believe it is their ethical responsibility to hand over the information a provider asks for, such as name and birthday. One blogger told us, “Many people provide fake information for their address and name [to Facebook]. I give my real information. Because In my opinion we need to provide our information and we have to believe them.”

To promote adoption and trust of secure tools, establishing the capacity of trusted community members to train and advocate for secure tools is key. The bloggers are interested in more secure ways of communicating, but have not made significant efforts on their own to find other, safer tools - even when they learn that a tool they use may not be as safe as they originally believed. In virtually every instance a blogger discussed adopting a new method of communicating it was because a trusted friend, colleague, or trainer recommended to them they do so. It is clear that increased usage of Internet Freedom Tools within Vietnam is strongly intertwined with deep community outreach to cultivate trusted champions within them. Many of these bloggers are already in positions of trust and leadership in their local communities and take on these responsibilities to the best of their ability. Increasing those abilities, as Viet Tan has worked to do on this trip, is a valuable starting point. A blogger shared this view when he said, “I saw my friend believe and trust in Facebook so I trust in them.”

Bloggers are more focused on mitigating risk around the storage of data rather than the transmission of that data. All of the bloggers have experienced harassment or arrest by police and security officials, and many of them have had their devices taken away as a result. They view the confiscation of devices as the highest point of risk associated with their work. As a result, the bloggers take a number of steps towards securing stored data such as 2-step verification for their email accounts. The risk of data being intercepted is understood as a general concept, but is not given as much consideration due to a broad lack of awareness about what that transmission means - “It’s Invisible!,” one blogger told us.

Circumvention is often the motivating use case in situations where privacy or security may be just as important, if not more so. Methods used to protect or encrypt the transmission of data, such as HTTPS, as well as tools with strong privacy and security properties, such as Tor, were viewed by the bloggers as circumvention tools to access banned websites. They were not explicitly utilized as security tools to protect the information being transmitted. The reasons for this appear to vary but include the bloggers a lack of knowledge about the security benefits to not having a full picture of the threat model they may face.

RECOMMENDATIONS FOR TOOL DEVELOPERS

Tool security design must assume the likelihood of a device being confiscated by authorities as an essential part of the threat model. Physical devices are commonly confiscated by authorities, and bloggers have widely cited the risks posed by confiscation due to the information they keep on their devices. Carefully consider this aspect of the threat model when designing security features for a tool.

Devices are often shared with friends or family, particularly home desktop and laptop computers. Multiple bloggers discussed how they must share devices with their friends and family due to the fact that authorities have confiscated their personal device. In many cases, families do not have the financial means to replace such devices. This reality presents obstacles to creating secure, usable software but the reality of device sharing must be accepted. When security cannot be guaranteed due to this constraint, a harm reduction approach to design should be embraced.



Examine your tool through the lens of existing popular tools used by the community. This does not mean one should simply copy other tools, but one should be familiar with these tools and use them as examples of “where users are” - and design to meet them there. Facebook, Gmail, Wordpress, Blogspot, and Skype are the most widely used communication tools.

Language localization is important in order to reach a wide audience of users in Vietnam. While the bloggers we spoke with claimed they did not necessarily need language localization because they knew the basics of how a user interface is generally laid out, they demonstrated that this was often not enough through their limited knowledge of some more advanced security concepts. Language localization will continue to remain an essential component for serving the needs of many communities, including digital activists in Vietnam.

Software designed for this audience should require minimal set-up. This audience is capable of using a range of tools effectively, but exhibited little understanding or interest in configurations beyond the “default” that is presented to them. For example, the group did not configure privacy settings on Facebook to reflect the threats they face, though they are aware of such threats. The reasons behind this are partly due to technical education, and partly due to cultural norms of trust and perceptions of privacy. But the result is the same.

Embrace design elements that signify secure behavior. The bloggers widely cited instances of tool usage that signified secure behavior - even if in some cases the perception of security was greater than the reality. Examples of this include deleting written messages on Skype which replaces the original text with “This message has been removed,” the use of IP lookup sites when using Tor and visually seeing what country the exit node is present in, and receiving text messages when using 2-step verification for Gmail. These signifiers suggest to users that they are doing things that are actively supporting their security, and that motivates continued secure behavior.

RECOMMENDATIONS FOR TRAINERS, SUPPORTERS AND INTERMEDIARIES

Invest in establishing the capacity of trusted community members to train and advocate for secure tools. Trust is essential in the propagation of secure behavior within this community in a variety of ways. Most secure behavior changes stemmed from trusted friends and colleagues sharing advice.


Frame abstract privacy and security concepts in a familial context. The abstract concept of privacy can be challenging for this community embrace and understand, but framing it in the context of family can be helpful. Concepts such as planning a surprise birthday party for a spouse can have resonance where abstract concepts of privacy do not.

Design programming elements that promote collaboration and co-creation between participants. Elements of the process employed here, such as the tool design exercise, can activate and motivate a group. Doing so contributes to an individual’s sense of agency in regards to their privacy and security. This can have a lasting impact in perpetuating positive security behavior changes and tool adoption.



APPENDIX: A DEEPER UNDERSTANDING

The following sections are intended to impart a deeper insight into how the insights and recommendations were determined, as well as for the reader to draw some of their own insights through a deeper understanding of where the bloggers are in their security knowledge and behaviors. It also outlines the human-centered design approach that SecondMuse employed in gathering this information.

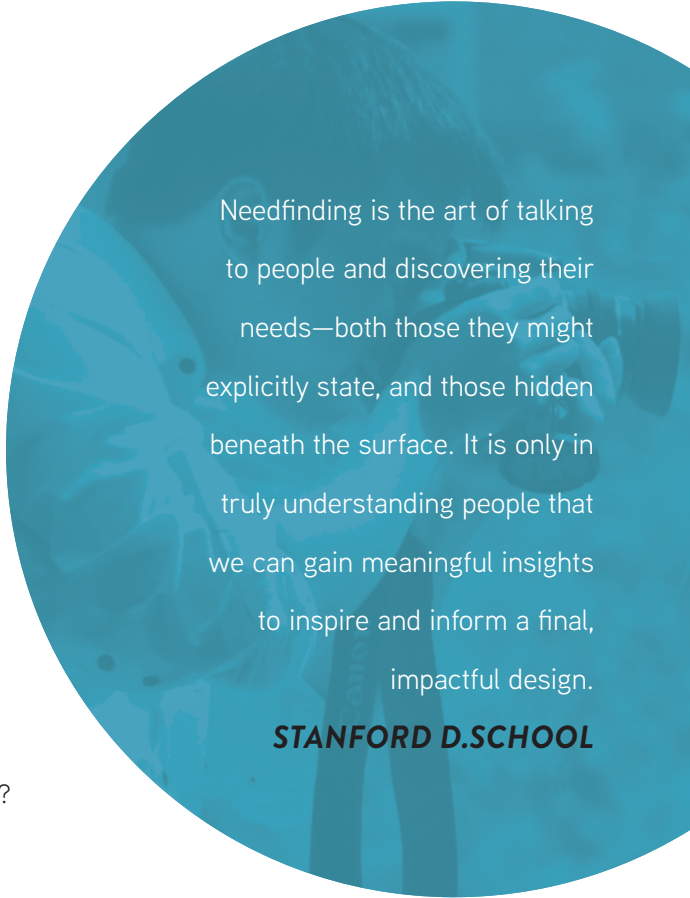


OUR HUMAN-CENTERED DESIGN PROCESS

SecondMuse embraces the art of human-centered design, and applies an empathy-based research approach that centers around the motivation and mission a community. We design exercises, interviews, and gatherings to uncover motivation, understand mission, and draw out needs of individuals that can be addressed by those who seek to serve the community.

The first step in our process is to establish the research questions we seek to understand. These questions are intended to serve as a guide to help the team focus on what we want to learn and how we want to learn it.

- What does it mean to a blogger to be **safe and secure**?
- What are the **priorities** for the bloggers when they are communicating?
- What are the **security-related behaviors** that the bloggers employ in their **daily communication activities**? Why?
- What kind of **communications tools** are the bloggers using, and why?
- What level of understanding to the bloggers have on **key security and privacy concepts**?
- How do the bloggers **perceive and understand the threats** that they face?
- How do the bloggers **learn** about communication security?



Needfinding is the art of talking to people and discovering their needs—both those they might explicitly state, and those hidden beneath the surface. It is only in truly understanding people that we can gain meaningful insights to inspire and inform a final, impactful design.

STANFORD D.SCHOOL

As human-centered design practitioners we must immerse ourselves in the context of the community of bloggers, as well as identify and fill in gaps in our understanding following our time with them. The central component of our was a two-day assessment with the six bloggers from Vietnam as well as members of the Viet Tan organization. Prior to and following this workshop we conducted interviews and background research as part of our Needfinding process.

During our time with the bloggers we employed a range of tools including group storytelling activities, one on one interviews, and a series of creative exercises focused on drawing out the perceptions of each blogger about how they view their own communication and security priorities. We also worked with them to security tools, asking them to design and pitch a tool that addresses their security and communication needs.

We employ a range of techniques and through observing each of them we are able to synthesize key themes and reveal important needs. Getting an answer from an individual about what their security threat is, or what key features they want in a piece of software is not in and of itself Needfinding. Individuals communicating their perspectives on an issue is important, but we cannot trust those perspectives alone to tell us what a need or motivation is.

For example, one group of bloggers designed a tool that is actually a physical button one keeps on their person. If they are under threat of arrest, a single press of the button would emit a radio signal that signals to their devices to delete all of information on them. This seems to be a completely reasonable request - but one must decode the expressed desire in order to extract the underlying need. By looking at this tool design in a broader context of knowing the threat, knowing the tools that are available, and listening to what the bloggers have been speaking about during our time with them, one may determine the underlying need is an easy way to protect local data. In this case, perhaps disk encryption would suffice to mitigate the risk that the blogger faces.



BUILDING AN UNDERSTANDING

Effectively serving a community requires one to first develop a deep understanding of their particular circumstances, challenges, interests and paths to greater security in order to enable to meet them where they are and create tools and mechanisms that will be most relevant to their current reality. The understanding we came to is that while the bloggers may not have deep understanding of all of the threats they face or the ways in which to combat them, they have a keen sense of how to take the knowledge they do have and use it to serve their security needs as they understand them. This is a key take-away as it **demonstrates the potential for significant improvements in the capabilities of activists** on the ground in Vietnam to combat the threats they face.

KNOWLEDGE OF PRIVACY AND SECURITY

In order to create successful programming and software for this diverse group, it is essential to clarify their understanding of privacy and security. In addition to shedding light on where the bloggers fell within the spectrum of use of internet freedom tools, the Needfinding process made clear that the topic of online privacy had been given minimal consideration. When asked what privacy and security meant to them, responses across the group were very similar. **“Security means that information that is supposed to be kept private, should stay private,”** said Nguyen Dinh Ha, a statement that was echoed by many, **but the bloggers had some difficulty in defining what kind of information should be considered private.** Ultimately they cited data on their hard disks, draft essays or articles, communications with fellow activists about upcoming activities, and occasionally their names and identification numbers or SMS messages with their personal contacts.

Cultural elements are acutely relevant here. In Vietnamese culture the conception of privacy is vastly different from in many parts of the Western world. In a country where family and community are paramount and extended family living is still the norm, there is a much lower expectation of keeping information to oneself. The comparatively narrow conception of privacy exhibited by the bloggers naturally impacts the information they feel they need to protect and the methods they use to do so.

Yet another area where culture elements come into play is how and where bloggers choose to place their trust. Whereas in many parts of the world mistrust of corporate use of personal data is a significant concern, an inclination was observed among the Vietnamese bloggers interviewed to trust that information being requested of them is needed by the requesting, often foreign, company. For example, **one blogger indicated that he felt responsible to provide accurate personal information to Facebook**--from name to birth date to address--**because he felt they would not ask for it if they did not need it.** This trust, moreover, requires users to rely on the “honor” of the companies that collect their personal data and on numerous occasions the bloggers indicated choosing one service over another because of trust in the company’s honor. In some circumstances that reputation honor, or lack thereof, was a result of the company’s actions as was the case in the highly trusted Google and generally distrusted Yahoo! In other cases, it was simply a tentative trust in big name brands or tools popular among peers, as is the case with Skype and Facebook.

SECURITY CONCEPTS AND INTERNET FREEDOM TOOLS

In spite of their common use of technological platforms as a voice for their activism, the level of understanding of internet freedom tools, as well as technology and internet use in general, varied widely within the group: from To Oanh, a former computer science teacher with some areas of complex computer expertise to Nguyen Thi Kim Chi, an entry-level computer user, to Nguyen Dinh Ha, a typical millennial youth whose smartphone and favorite apps are a part of everyday life. Despite this variety, **the bloggers do not possess strong knowledge of common security concepts and the most powerful privacy and security tools**. This is notable given the potential for certain technologies, such as disk encryption, would have in mitigating risks associated some of the most concerning risks they face such as the confiscation of devices with sensitive information. Here are summaries of the bloggers understanding and use of a few common concepts and tools.

- **Encryption:** Most bloggers claimed they did not know what encryption was. The few who did recognize the concept were able to describe it as the scrambling of information, but did not possess a strong grasp of it.
- **PGP / Encrypted Email:** Most bloggers had not heard of PGP, and the one that did could not define it. Some bloggers had heard of the idea of encrypted mail, but none have ever attempted to use it..
- **Password Security:** Almost all bloggers claim to regularly change their passwords. This ranged from every three weeks to a couple of times per year. Most said they changed their passwords once every three months. Some change their passwords based on context, such as adding a more complex mobile device password prior to participating in an organized event.
- **Two-Factor Authentication:** Almost all bloggers used 2-step verification for their email accounts, namely Gmail and Yahoo! The bloggers did not employ this for other services, such as Facebook. The bloggers also disabled 2-step verification prior to leaving Vietnam for this trip and not attempt to use other means of utilizing it without access to their mobile phone, such as lists of temporary authorization codes.
- **Tor:** A few of the bloggers have heard of Tor, but the majority have not. One blogger claimed to use it regularly, and expressed joy in doing so. Another claimed to use it on occasion, but not often because of the slow speed of the network.
- **HTTPS:** Most said they knew what it was, but saw it as a circumvention technology as utilizing it allowed access to some websites that were not accessible via a standard HTTP connection.
- **Antivirus / Anti-Malware:** Virtually all bloggers utilized some form of anti-malware and antivirus tool. The most popular tools cited were Avast and Kaspersky. Some also utilized PC performance enhancing tools such as CCleaner, but associated them with anti-malware and antivirus tools.

PERCEIVED THREATS AND SECURITY BEHAVIORS

In discussing their security behaviors and concerns, it was clear that the bloggers viewed the government as their primary adversary, with particular groups playing different roles: the police and security forces posed the risk of arrest and confiscation devices, government opinion-shapers and hackers acted as agitators on blogs and Facebook and were potential sources of malware, and additional threats came from government-owned ISPs who regularly handed information on client activities over to the security police.

These choices of what information requires protection and where trust should be placed are foundational to understanding the bloggers' security behaviors and the tools and resources they use in their activism and their personal lives. **These behaviors also indicate the bloggers perception of their own threat model** - the technology they choose to use and behaviors they decide to adopt indicate the way they believe they are mitigating threats. Below we discuss a variety of the security concerns and responding behaviors identified by the bloggers:

- **Minimal use of phones for sensitive communication:** The bloggers unanimously felt their privacy and security was being compromised was in the use of their mobile phones. They were confident that their voice and SMS communications were regularly surveilled and thus have developed behaviors to try to minimize their security risks including: never sharing sensitive information by SMS message, and immediately delete anything sensitive they receive; regularly using code terms to communicate to fellow activists by phone, such as saying "let's drink tea" or a similar phrase to indicate the planning of a pro-democracy meeting, and substituting Skype in place of phones for voice communication--which bloggers felt was a safer option.
- **Protection of devices and hardware:** The bloggers were unanimously concerned about the possibility that arrest might result in the confiscation of their computers or mobile devices, making any information saved on those devices vulnerable. Notwithstanding, only a few bloggers mentioned behaviors addressing this potential vulnerability, including regularly buying and discarding prepaid SIM cards for mobile phones, implementing automatic locking on home computer screens, regularly changing computer passwords and ensuring mobile device access required a pin number. Just one blogger discussed putting sensitive information on an encrypted hard disk that he stored in a safe place.
- **Relying on companies they see as trustworthy:** Multiple bloggers repeatedly referenced trusting certain companies over others, such as Google, for various reasons including a company's historical actions. A strong basis for trusting Google was the widely-held view that the company refused to hand over information to Vietnamese authorities and also refused to put their servers inside Vietnam. In contrast, Yahoo's release of information to Chinese authorities regarding the communications of a Chinese journalist in 2005 largely destroyed multiple bloggers' trust in Yahoo as a platform for their email communications.
- **Deleting messages in chat communication:** Many bloggers expressed feeling more secure using chat programs in place of email and SMS, with Skype, Google Chat and Facebook Inbox among the most common choices. Most of the bloggers have adopted the security behavior of deleting messages in chat software after they are sent. Although the bloggers utilizing these methods were not certain whether deleting the messages actually permanently removed them, it gave them a level of comfort to know that the message was not visible on their computer any longer.

- **Considering Facebook to be a largely public forum:** There was consensus among the bloggers that they considered Facebook to be public. Most had an active presence on Facebook with numerous followers, only a small percentage of whom they knew personally. Facebook friends constituted a broad readership, similar to a blog. As one blogger said, “for public, I post on Facebook; privately I use SMS and email.” If they sought privacy on Facebook, some bloggers used private Facebook groups or the inbox chat feature. There was limited knowledge of the option to increase privacy across Facebook settings overall and limited understanding of the information about a person that can be gathered by tracking Facebook activity.
- **Using certain characteristics to determine if commenters are government-employed “opinion shapers”:** Those bloggers who were active on Facebook all reported experience being targeted by government-employed opinion-shapers. They explained these individuals could be identified by their posturing and actions online, from their patterns of speech and writing, to their arguments, to their rude comments, vulgar language and accusatory tone. Some bloggers also reported malware being sent through Facebook by the opinion-shapers. The bloggers blocked people they believed were government opinion-shapers in order to protect themselves.
- **Trying to guard against malware infections:** Malware was a significant concern among the bloggers. As a result the bloggers do not click on links or attachments coming from strangers, exercise caution in determining reliable sites for downloading software, such as CNET. Some also used antivirus software such as Kaspersky and Avast as well as periodic cleanings of their hard drives with programs like CCleaner. Nonetheless, they expressed concern that regardless of how cautious they may be, if the people they communicate with are not equally cautious, the threat of malware is always present.
- **Arranging face-to-face meetings for high-risk communication:** As mentioned, the bloggers unanimously felt face-to-face meetings were the most secure behavior for sensitive communications. As one blogger stated, “of course you have the tradeoff of time and inconvenience, but it is more secure.” Use of code words to denote meeting times, places and purposes when scheduling meetings by phone was also a common practice.
- **Taking steps to protect email:** Protecting email was a primary concern of many bloggers. Although none used tools for encrypted email, they did employ other security behaviors. The use of 2-step verification for Gmail accounts was common and bloggers felt empowered by the fact that they would be notified when someone attempted to log in without the verification code. As one blogger mentioned, “The hacker knocked on the door, but did not get in.” Many bloggers also use multiple email accounts for different purposes, change email passwords regularly, and had alternate or backup email accounts set up. Just one blogger avoided typing passwords while online, instead typing while offline and then pasting the password into the online field.
- **Exchanging security information with friends and fellow activists:** Many of the bloggers also exchange information with fellow activists about security. Some indicated learning of tools like 2-step verification, Tor and security software Kaspersky from other activists. Hearing tools recommended by fellow activists whom they trusted made the bloggers more inclined to test out those tools themselves. A few bloggers also mentioned having participated in security trainings where they learned of new tools.

- **Circumvention Methods:** While almost all the bloggers were familiar with some methods of circumvention to enable them to access blocked sites, only a few bloggers indicated using circumvention tools for their own security. One occasional user of Tor liked the security of seeing that his IP address was located in different countries while using the software. Another blogger regularly used circumvention tools to continuously change his local port and IP address, and also rotated which operating system he used.

While the bloggers shared many security behaviors they have developed in response to their concerns, they also expressed concerns that they were uncertain how to address. These concerns are sometimes closely tied to a misunderstanding of the security threat that they face.

- **Web-based attacks and hacked accounts:** Multiple bloggers mentioned having been victims of malicious website attacks, included a DDoS attack originating from a government IP address that took down his website, and hackers targeting blogging and email platform accounts. In some cases, however, it was clear that a perceived hacking attack was simply a matter of a forgotten or mis-remembered password.
- **Security of information in transmission:** Many bloggers expressed uneasiness about whether information being transmitted online (email, chat) could somehow be accessed during the transmission even if the information was deleted by both the sender and the receiver. One blogger stated “it is invisible,” highlighting the confusion around the visibility and accessibility of information. Another blogger said “information flows from the sender to the receiver, and I’m not sure what the ISP is doing with the information.” Yet another blogger was adamant that “after 5 p.m. experts from the security police come to the ISP to pick up the data.”
- **Conflicting information on the security of tools in use:** Bloggers indicated that on occasion they received conflicting information on the security level of certain tools (Skype, for example) that left them feeling helpless and without options. As one blogger stated, “if there are other options I would use them, but if not, what can you do?” This sentiment was expressed on a number of occasions, but there was little indication that any of the bloggers interviewed actively sought alternatives to the tools called into question.

This report was written by SecondMuse with support from Viet Tan.

This work was made possible by the Open Technology Fund and Radio Free Asia.

Special thanks to Eva Galperin of the Electronic Frontier Foundation for contributions to this work.

Report layout and design by the Phuse.

SECONDMUSE / secondmuse.com

VIET TAN / viettan.org

OPEN TECHNOLOGY FUND / opentechfund.org

RADIO FREE ASIA / rfa.org

The activists featured in this report requested that their true name and photographs appear in order to raise their international profile and contribute to their safety.

This report was published in June 2014.

