1. BACKGROUND

1.1 About TibCERT

The Tibetan Computer Emergency Readiness Team (TibCERT) is a formal, coalition-based structure for reducing and mitigating online threats in the Tibetan community, expanding Tibetans' technical research capacity on threats in the diaspora, surveillance, and censorship inside Tibet, and ultimately ensuring greater online freedom and security for Tibetan society as a whole.

1.2 Purpose

The purpose of this TibCERT quarterly bulletin is to share updates about TibCERT and offer advice on digital threats observed in the community. We also aim to help Tibetans in the diaspora stay safe physically, emotionally, and digitally during the COVID-19 pandemic, as well as provide resources and awareness on issues surrounding the global pandemic.

1.3 TibCERT Updates

The coronavirus pandemic has affected everyone. Since India is under national lockdown, to maintain social distancing, we are all currently working remotely from home and are continuing to provide support and create digital security resources for our stakeholders and the community. The status of the lockdown is still uncertain at the time of writing and we will continue to provide remote support and have been exploring ways to do virtual training and policy implementation.

1.4 Summary

The fourth edition of the Bulletin features:

1.4.1 Disinformation/Misinformation

Disinformation (shared deliberately) and misinformation (shared accidentally) are fake/unverified pieces of information that can mislead people and cause harm (e.g., through blog posts, texts, WeChat comments, infographics, etc.). In order to help keep the Tibetan community safe during the coronavirus pandemic, TibCERT's Knowledge Base now has a section where information circulating on COVID-19 can be either verified as true, identified as disinformation/misinformation, or some of both. Please visit https://learn.tibcert.org/category/disinfo-misinfo/ for more information. If you want to verify something that is not yet on the website, please write to support@tibcert.org.

1.4.2 COVID-19 Updates

There are Tibetans all over the world working to help each other combat and cope with this pandemic. In order to provide a space for Tibetans to find resources ranging from health tips, online training, helplines, tech tips, advice for elders, and more, we created a website to connect the community at https://covid19.tibcert.org/.

Meanwhile in China, authorities and tech companies have launched an effort to stop the spread of the virus through several apps that track people and their level of exposure to COVID-19. However, without their knowledge or consent, each time a person runs the app, their personal data is shared with law enforcement and stored on a server. This raises major privacy concerns, posing a threat that the data is being used for social control which can continue even after this pandemic.

1.4.3 Kaspersky Report

Online privacy group Kaspersky recently published a report on a watering hole attack targeting several Tibetan websites. This kind of online attack compromises the sites and shows a fake pop-up asking the user to install the latest Adobe Flash player. If downloaded, the visitor's operating system is then infected with malware. Since learning of the attacks through Kaspersky's report, the TibCERT team has conducted incident response to as-

sist the stakeholders who were compromised.

1.4.4 Digital Security Update

- During the COVID-19 pandemic, the Citizen Lab of the University of Toronto conducted research of censorship taking place on WeChat. Using sample testing, researchers discovered keywords that were censored in order to stop the posting of coronavirus-related content. The Citizen Lab also recently published a report on Chinese government surveillance of WeChat through accounts registered outside of China, which authorities are using to improve the censorship algorithm for China-registered accounts. This report contains critical information to help understand WeChat censorship and is an important milestone in surveillance research given that it is the first report to discuss WeChat surveillance outside of China and Tibet.
- TikTok, owned by ByteDance, has several security risks and vulnerabilities that allow attackers to use malicious links that seem to be from TikTok in order to gain access to user accounts. Attackers can then manipulate the account's content, upload and delete videos, and access personal information such as private email addresses. It has also been discovered that TikTok has been censoring issues such as the Tiananmen Square massacre, Tibetan independence, the religious group Falun Gong, widely publicized pro-democracy protests in Hong Kong, Chinese government oppression of the Uyghur Muslim population, and other issues that criticize the social structure of the Chinese Communist Party (CCP). In addition, TikTok has sent emails to the company's India content moderation team to remove any content related to His Holiness the Dalai Lama and Tibet. This shows how TikTok has been trying to control content being posted outside of China as well.
- In order to maintain social distancing during this pandemic, many people started working from home, leading to the rise of the use of video conferencing tools. Through its usability, Zoom became the tool that most people adopted and, in some ways, "Let's Zoom" has become similar to "Let's Skype," which used to be synonymous with video calls a few years ago. However, researchers recently found some security issues with Zoom. One of them directly relates to Tibetans as the research showed Zoom data travelling through China. The question on everyone's mind is, "Is Zoom safe to use and if not, what should we use?" We will explore questions such as these below in more detail, along with the underlying concept of how much we can trust proprietary software.

2. DISINFORMATION/MISINFORMATION

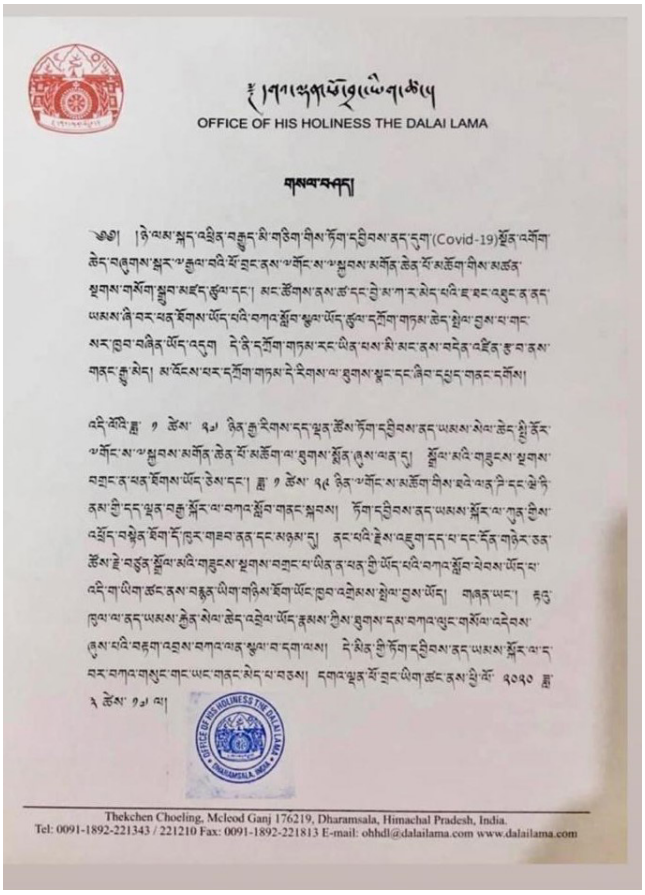
False news is a major problem these days. Individuals and governments are using social media and other communication platforms to dispatch both misinformation and disinformation. Misinformation refers to the unintentional spread of false information whereas Disinformation refers to false information that is deliberately created to harm a person, social group, organization, or country. The spreading of disinformation can blur the lines between reality and fiction and is meant to confuse people.

Recently, we've seen a lot of fake information related to COVID-19 being shared on social media. It can be difficult to tell sometimes what is fake and what is real, but when people forward false content, it amplifies the problem, spreading misinformation and disinformation that can harm the Tibetan community. In order to help the problem, TibCERT began researching these false news items and sharing the correct information on our Knowledge Base website at https://learn.tibcert.org/category/disinfo-misinfo/.

Three important examples of misinformation/disinformation are as follow:

On March 16th, 2020, fake news spread that His Holiness the Dalai Lama had advised Tibetans to drink black tea for the prevention of COVID-19. Many people believed this to be true and the information went viral on social media. Soon after, the Office of His Holiness the Dalai Lama had to

respond to the rumor, making an announcement to clarify that His Holiness was not recommending black tea as a prevention for COVID-19.


OFFICE OF HIS HOLINESS THE DALAI LAMA

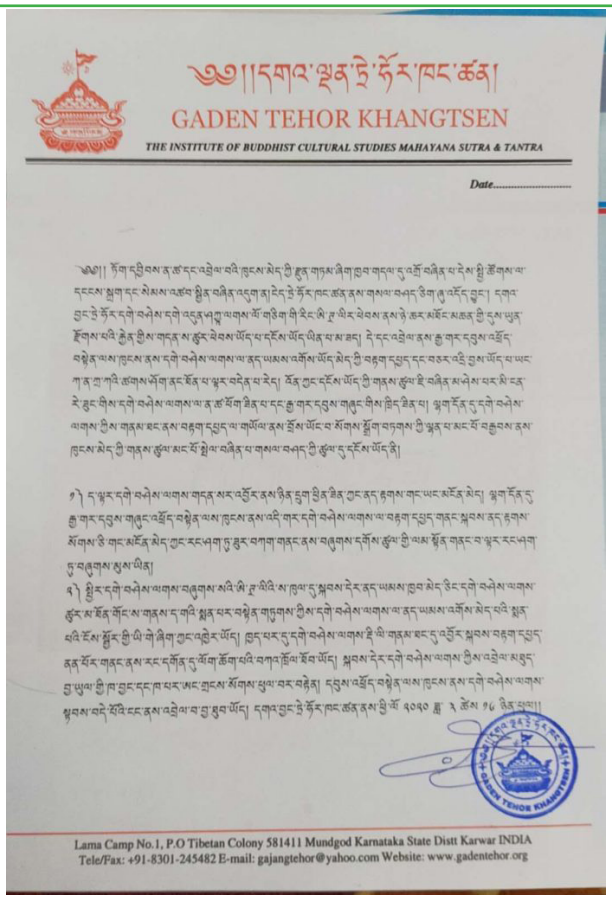
Thekchen Choeling, Mcleod Ganj 176219, Dharamsala, Himachal Pradesh, India.
Tel: 0091-1892-221343 / 221210 Fax: 0091-1892-221813 E-mail: ohhdl@dalailama.com www.dalailama.com

Figure 1: Clarification Letter by the Private Office of HHDL

Likewise, there was also false news circulating that said a monk from Gaden Jangtse had been infected with COVID-19. This was completely untrue and the Gaden monastery sent out a correction stating that the monk had tested negative.

Finally, another example of false news circulating in the Tibetan community was about protection from the coronavirus by keeping a picture of a certain spiritual amulet, as done by Sakya Trizin. This was not true and to correct this notion, the Office of Sakya Dolma Phodrang released a statement clarifying that while the amulet can help someone in general, it should not be relied on to help with COVID-19.

Just as it can be said that, "War isn't new," it's also true that misinformation and disinformation aren't new. What's different now is that we are living in a digital age where forwarding information is as quick as lightning. People tend to forward messages and stories if they see a catchy headline, without necessarily reading the content or determining if the in-

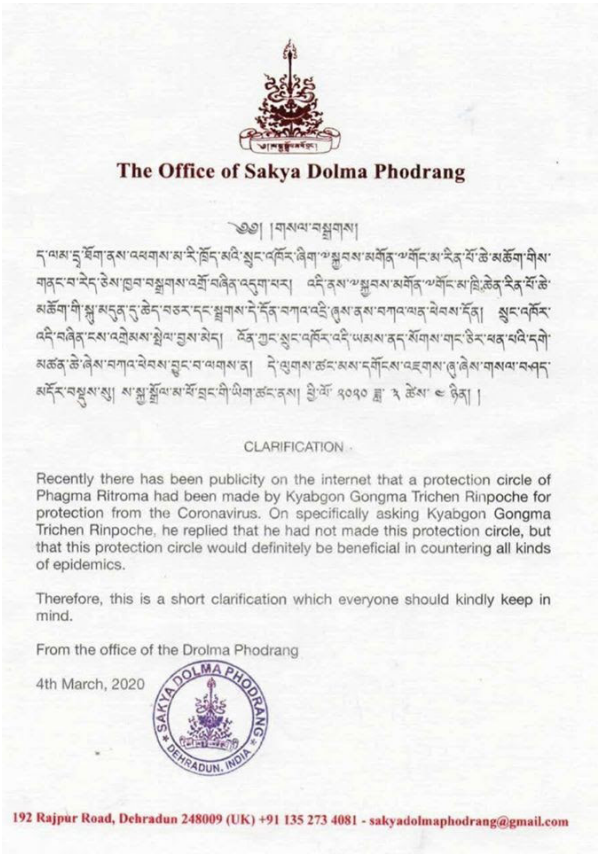

GADEN TEHOR KHANGTSEN

THE INSTITUTE OF BUDDHIST CULTURAL STUDIES MAHAYANA SUTRA & TANTRA

Date.....

Lama Camp No.1, P.O Tibetan Colony 581411 Mundgod Karnataka State Distt Karwar INDIA
Tele/Fax: +91-8301-245482 E-mail: gajangtehor@yahoo.com Website: www.gadentehor.org

Figure 2: Clarification Letter by Gaden Tehor Khangtsen


The Office of Sakya Dolma Phodrang

CLARIFICATION

Recently there has been publicity on the internet that a protection circle of Phagma Ritroma had been made by Kyabgon Gongma Trichen Rinpoche for protection from the Coronavirus. On specifically asking Kyabgon Gongma Trichen Rinpoche, he replied that he had not made this protection circle, but that this protection circle would definitely be beneficial in countering all kinds of epidemics.

Therefore, this is a short clarification which everyone should kindly keep in mind.

From the office of the Drolma Phodrang

4th March, 2020

192 Rajpur Road, Dehradun 248009 (UK) +91 135 273 4081 - sakyadolmaphodrang@gmail.com

Figure 3: Clarification Letter by the Office of Sakya Dolma Phodrang

formation is genuine or not. Since misinformation/disinformation can be so harmful, it's every individual's responsibility to check whether the content has been verified or not. In addition, it's very important to report fake content wherever you can, including to TibCERT at submit@tibcert.org. In this way, we can all help keep our community updated with correct and useful information.

Think Before You Share

Figure 4 "Think Before You Share"

These days, most people get their news from online sources, relying heavily on mobile devices for communication. It is therefore easy for false information to spread naively and quickly, leading to confusion about what is true and what is not true. Therefore, the best practice you can always take is to "Think Before You Share," making sure not to forward unverified information to your contacts. In this way, we can help save our community from the effects of receiving and acting on false information. Since we have elections coming up in a few months, it will be critical for us all to avoid disinformation campaigns. If you come across any suspicious information, feel free to share with us for verification at submit@tibcert.org.

3. COVID-19 UPDATES

3.1 TibCERT COVID-19 Website

Tibetans in the diaspora are creating and distributing great resources to combat and cope with the ongoing pandemic. In order to collate and share useful information related to COVID-19 for Tibetans all around the world, TibCERT has created a website https://covid19.tibcert.org available in both English and Tibetan.

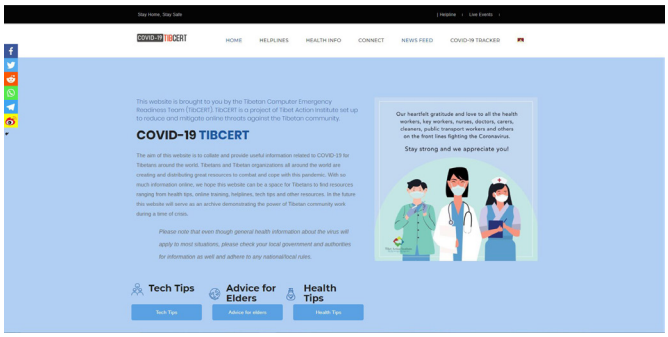


Figure 5: TibCERT's COVID-19 Resource Website

In particular, the website contains regional helplines for people who are in need of help, health tips to know more about the disease, tips specifically for elders, and basic protective measures to stay safe and help keep others safe as well. We have also included a video of advice from Dr. Tsetan Sadutshang la, Delek Hospital's Chief Medical Officer and personal physician to His Holiness the Dalai Lama. Since many organizations and individuals are now working from home in order to maintain social distancing, you will also find tech tips on how to keep yourself safer online from digital threats. Finally, to find organizations and individuals working on COVID-19, you can go to the "CONNECT" page on the site.

We are planning to make this website even more resourceful in the coming weeks, including new features like a discussion platform where Tibetans around the world can discuss and meet virtually. In addition, we will create a COVID-19 Volunteer Task Force of people who can physically go help those who are not able to buy groceries, for example, or elders who are alone and in need of connection. When we look back, this website will also serve as an archive demonstrating the power of Tibetan community work during a time of crisis.

3.2 China's COVID-19 Contact Tracing App and the Privacy Implications

COVID-19, also known as coronavirus disease, is an ongoing pandemic spreading across the globe. In an effort to mitigate the situation and the spread of the virus, many governments have been collaborating with technology companies to create apps that help track people and their contact with individuals who are infected.

According to the New York Times, when the government of China began encouraging people to return to work a couple of months ago, they rolled out an app for people to identify whether they have been exposed to the coronavirus[1]. Partnering with Ant Financial (a sister company of e-commerce giant Alibaba), China published an app called "Alipay Health Code." Through the app, individuals scan QR codes and are sorted into color-coded categories such as red, green, and yellow that theoretically indicate a person's health status (though it is not known through what criteria, forcing people to self-isolate at times with no idea why). Beyond this confusion, such a system also allows a person's movement to be tracked by authorities, an underlying major privacy concern. For example, when someone scans a code, a program labeled "ReportInfoAndLocationToPolice" sends the person's location, city name, and an identifying code to authorities. Not only is the connection to law enforcement not made clear to users, the app shares the data with a server every time someone scans the code. This accumulation of data on individuals and the template for tracking could create new forms of automated social control that could persist long even after the pandemic subsides[2].

This is also true for a new app developed by Tencent (the company that operates China's popular, multipurpose messaging app WeChat) with help from China's National Development and Reform Council. The "Tencent Healthcare Code" is also reported to operate through a similar QR code-based tracking system that can be used to track and obtain the health status of users[3].

Apart from these central health code apps, many local governments have also launched their own health code mini-programs using the same traffic light color code of red, yellow, or green. These color code results are said to be generated based on contact with known, suspected, or confirmed cases of COVID-19, as well as self-reported symptoms. The data has been integrated with travel, including from bus, train, and flight bookings[4].

When speaking about QR code-based tracking apps, Alain Labrique (Associate Professor at Johns Hopkins Bloomberg School of Public Health) said such apps raise disturbing questions about privacy. "Sharing information about an individual's health without their explicit consent is quite problematic, especially when that information is unlikely to have much utility in preventing disease," Labrique said.[5]

There are some other speculations from surveillance experts. "Unfortunately, as you might expect, there's not much transparency about why an individual might get a yellow or red score," Albert Fox Cahn, Executive Director of the Surveillance Technology Oversight Project, told ABC News, "and this leads to a lot of possible abuses, where political dissidents and other historically marginalized groups can be targeted for punitive quarantine measures just as a way to cut them off from public life."[6] Mr. Fox Cahn also suggested that it is not hard to imagine the Chinese government using its massive surveillance structure to target human rights defenders and political protesters, deflecting criticism by saying it was all for public health purposes.[7]

According to a report from TechNode, several users have said they received different color codes than their family members, even though they have been in isolation together for weeks. This poses a seri-

1 https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
2 https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
3 https://www.voanews.com/student-union/phone-apps-china-track-coronavirus
4 https://www.wired.co.uk/article/lockdown-in-wuhan-coronavirus
5 https://technode.com/2020/02/26/virus-tracking-apps-arent-helping-fight-panic/
6 https://abcnews.go.com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story?id=70131355
7 https://abcnews.go.com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story?id=70131355

ous question about how the system analyzes health and travel data and makes it hard to rely on the app completely.[8]

To stop the growth of the on-going pandemic, some other governments are also choosing to use contact-tracing apps, while South Korea tackled its COVID-19 response with other surveillance methods as well. However, surveillance and tracking methods raise a concern about the privacy of the users or an attacker misusing the data collected through contact tracing. In any case, it is important to be aware of what data is being shared with authorities and how they may use it.

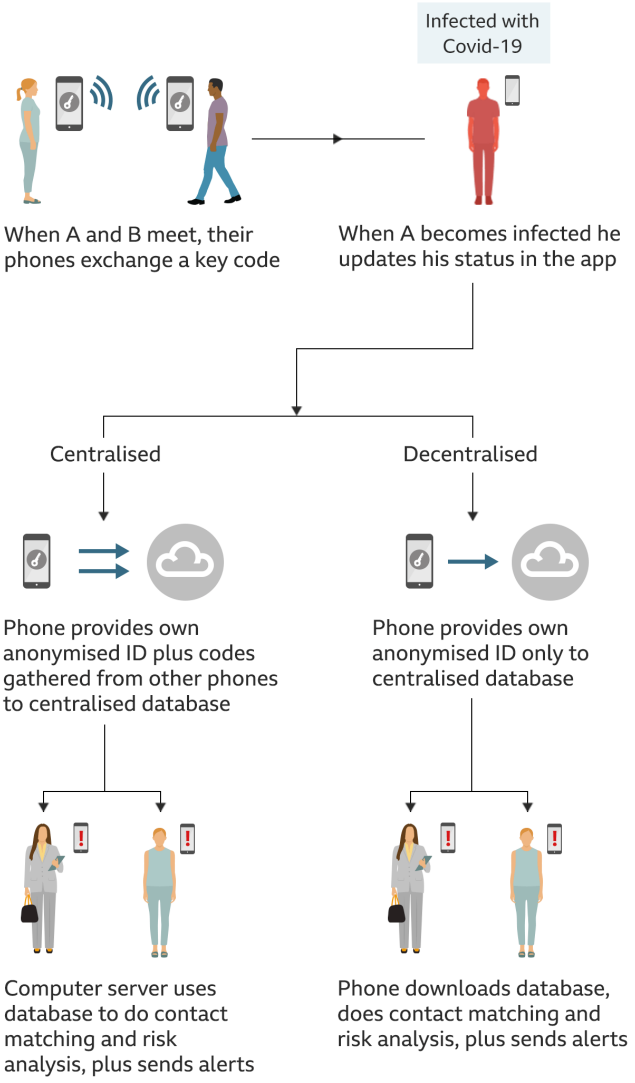


Figure 6: Centralised vs Decentralised Apps

Currently, there are two different models being promoted for how contact-tracing apps could work: 1) a "centralized" structure, and 2) a "decentralized" structure, both illustrated below by the BBC.[9] The debate between the two methods centers on how these apps protect a user's privacy versus how much and in what way data is gathered and stored in an effort to stop the spread of the virus.. [10]

4. KASPERSKY REPORT

4.1 Report

A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users (e.g., the Tibetan community) by infecting websites that members of the group are known to visit. On December 4, 2019, Kaspersky (a global cybersecurity company) published an Advanced Persistent Threat (APT) Report titled "Holy Water: Ongoing Targeted Water-holing Attack in Asia."[11] In this report, Kaspersky revealed that they had discovered waterholing attacks on multiple websites that selectively triggered a drive-by download attack. This happened through fake Adobe Flash update warnings that, when downloaded, would infect the user's device. It works like this: a previously hacked but legitimately embedded resource will load a malicious JavaScript onto the affected website. When someone visits one of the compromised sites, the visitor is checked by an external server to see if that person is a target (likely based on IP range). If yes, then the server gathers information on the visitor which is hosted by the compromised website. When the visitor is verified as a target, the first JavaScript stage will load a second script which will trigger the drive-by download attack, showing a fake update pop-up (see Figure 7 below). The visitor is then supposed to fall into the trap and attempt to update the flash player on their device, thereby downloading a harmful installer package. This in turn will set up a backdoor that allows the attacker remote access to the device.

8 https://technode.com/2020/02/25/how-china-is-using-qr-code-apps-to-contain-covid-19/

9 https://www.bbc.com/news/technology-52355028
10 https://qz.com/1857556/western-nations-havent-reached-consensus-on-contact-tracing-apps/
11 https://securelist.com/holy-water-ongoing-targeted-water-holing-attack-in-asia/96311/

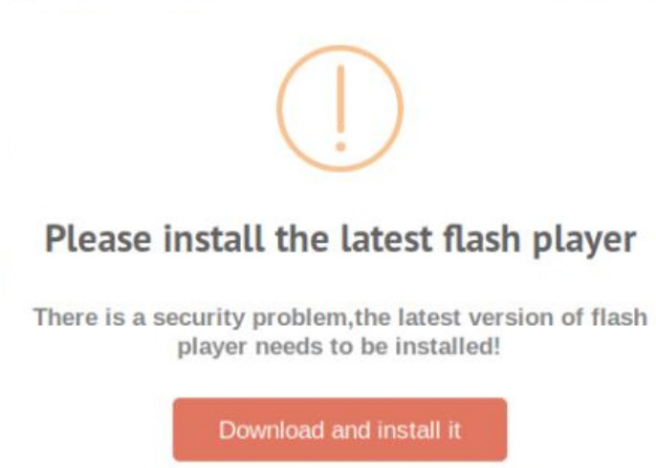


Figure 7: Warning generated by the second payload

Since May 2019, the attack campaign has been active, targeting various Asian religious and ethnic groups. This includes some Tibetan websites that have been compromised by this attack. Kaspersky's report indicates that compromised websites belong to personalities, public bodies, charities, and organizations of the targeted group. When the report was released, some of these websites were still compromised, continuing to direct selected visitors to harmful downloads like the Adobe Flash malicious update. All of them were hosted on the same server. A few examples are below with some of the information redacted for privacy:

Domain	Description
*****corps.org	Voluntary service program
*****ct.org	Religious personality's charity
*****policy.net	Policy institute
*****che.com	Religious personality
*****parliament.org	Public body
*****ialwork.org	Charity
*****nature.net	Environmental conservation network
*****airtrade.com	Fair trade organization

Kaspersky stated the attackers have set up a large yet very selective watering hole attack with lots of compromised websites and implanted hosts. The attacker exhibits characteristics of a small but agile team whose toolset is not advanced or fully developed, yet they have been able to modify their methods several times in a few months. Kaspersky also stated that they believe some tracks indicate the Godlike12 backdoor set up by the attackers is most likely used to conduct reconnaissance and data-exfiltration operations but have been unable to link the attack to any known APT groups.

4.2 An Update on Incident Response

After Kaspersky's report came out, TibCERT became aware of the organizations that fell victim to this attack. As a result, TibCERT contacted the organization whose website was compromised and our team is working collaboratively with the group to locate the malware and remove it. We also are engaging the TibCERT member organization whose office systems and server were compromised through contact with a compromised website. Since India is still under national lockdown, we are providing incident response remotely at this time. Due to confidentiality and privacy of the affected organizations, we can not disclose any more information.

It is important to underscore that the only way to be impacted by this attack is to have attempted to download the fake Adobe Flash player update on an affected website, not just visiting the site. If you believe you may have been infected, please reach out to support@tibcert.org. And remember, the practice of "Think Before You Click" (https://tibetaction.net/digitalsecurity/onlinesecurity/) is the best way to stay safe from attacks.

3.3 Disinformation Campaigns

An unusually active social media campaign was observed during the Tibetan elections of 2011 and 2016. In the midst of the political campaigning on social media platforms such as Facebook and WeChat, there was a concern that the Chinese government and Chinese trolls were using fake accounts to spread disinformation via fake news, sharing disturbing content and doctored images.
t: https://learn.tibcert.org/knowledge-base/how-to-report-content-or-fake-profile-in-facebook/

5. DIGITAL SECURITY UPDATE:

5.1 WeChat COVID-19 Research by the Citizen Lab

COVID-19 is a pandemic that originated in Wuhan, China in early December, 2019. Since then, the pandemic has triggered the government of China to increase its scope of censorship on social media platforms in order to cut out any coronavirus-related content.

Given the high level of censorship on the popular messaging platform WeChat, the Citizen Lab of the University of Toronto set out to discover censored keyword combinations. When a message is sent from one WeChat user to another, it passes through a server managed by Tencent (WeChat's parent company) which detects if the message includes any blacklisted keywords. To determine what is being censored, the Citizen Lab used scripted group chat conversations to test certain words, publishing their findings in a report[12] detailing censorship of WeChat messages during this pandemic.

For their research, the Citizen Lab used Chinese

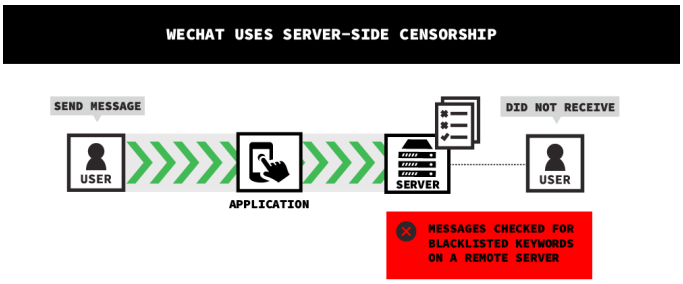


Figure 8: An Illustration of Client-side vs. Server-side Censorship

WeChat accounts to monitor whether the messages they posted in group chats were being filtered. They used three test accounts: one registered to a mainland Chinese phone number and two registered outside of China. None of these accounts were tied to actual users. If the Chinese account did not receive the message sent from the other users, then the message was flagged as containing one or more keyword combinations that had triggered text censorship. For the safety of other WeChat users, the Citizen Lab limited their test accounts to interacting with each other in the group chat and never interacted with real users on the platform.

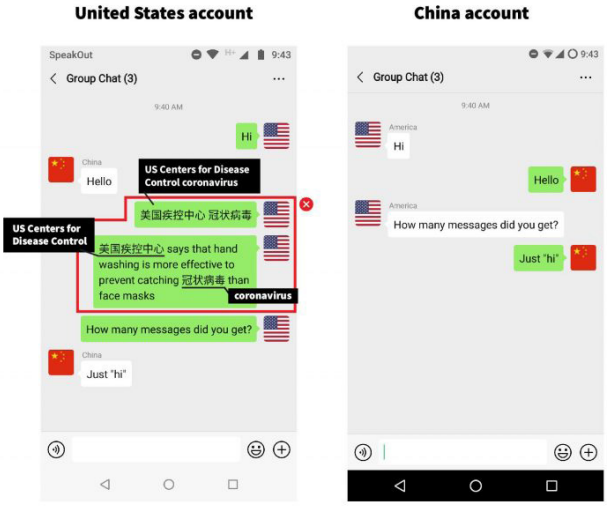


Figure 9: Example of Keyword Censorship for User in China

Between January 1, 2020 and February 15, 2020, the Citizen Lab found 516 COVID-19-related keyword combinations that were censored in the scripted WeChat group chat. This included 132 keywords found from January 1st–31st, 2020 and 384 new keywords found in just two weeks of February 2020. The government of China's internet censorship has been known to censor any information that authorities decide could harm the country, though a major goal of state censorship is to maintain control over people under the Chinese government's rule, including in Tibet. Also, we have seen that the government's censorship changes with situations like this pandemic. In late December, for example, authorities began censoring COVID-19-related content with 45 keywords, with the word count greatly increasing as the coronavirus pandemic took hold. This censorship may include companies over-censoring in order to avoid official reprimands for failing to prevent the distribution of "harmful information" including "inappropriate comments and descriptions of natural disasters and large-scale incidents," as required by the Chinese government.[13]

5.2 WeChat Research on Surveillance

Until now, we have only known about WeChat surveillance and censorship of China-registered

12 https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/

13 https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/

accounts. Thanks to another recent report[14] by the Citizen Lab, we now know that WeChat surveils accounts registered outside of China for any politically sensitive content, collecting the account's MD5 hash (a kind of digital fingerprint).

This database of MD5 hashes eventually helps in censoring content sent in China-registered accounts. For example, when a document or image is sent in a conversation between two non-China registered accounts, it is scanned for sensitive text and the overall image is visually compared to a blacklist of known sensitive images (this happens in real time). If the file is determined to be politically sensitive, then the MD5 hash of that file is flagged, meaning that the hash is retained by WeChat and used to more efficiently censor these files in the future.

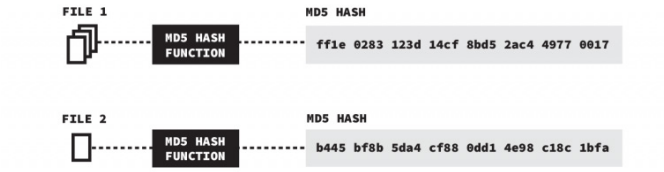


Figure 10: An Illustration of a Mapping File

As seen in Figure 10, a hash is a unique hexadecimal number. In theory, it should be difficult to find or create files that will produce the same hash. It is possible to study how WeChat's surveillance system works by creating two different images with the same hash—one politically sensitive and one benign.

According to the research done by the Citizen Lab, it was found that when sending politically sensitive images between accounts registered outside of China, politically benign images with that same hash ended up also being censored when sent between Chinese accounts. Since the images used would generally be considered benign, they would not normally have been flagged as sensitive, proving that the hashes themselves are being monitored and resulting in real-time censorship in China-registered accounts. Therefore, the Citizen Lab's research shows that not only are the files and images shared by people outside China under political surveillance, but their content is being used to train and build up the censorship system for China-registered WeChat accounts. Thus, it is evident that communication between WeChat's international users contributes to a censorship system that is used to censor China-registered users. While it is not yet known whether Tencent is sharing international WeChat users' communications with the Chinese government, the Citizen Lab's research is groundbreaking in its revelation that WeChat's surveillance system monitors content sent by one set of users to enhance the surveillance and censorship of another set.

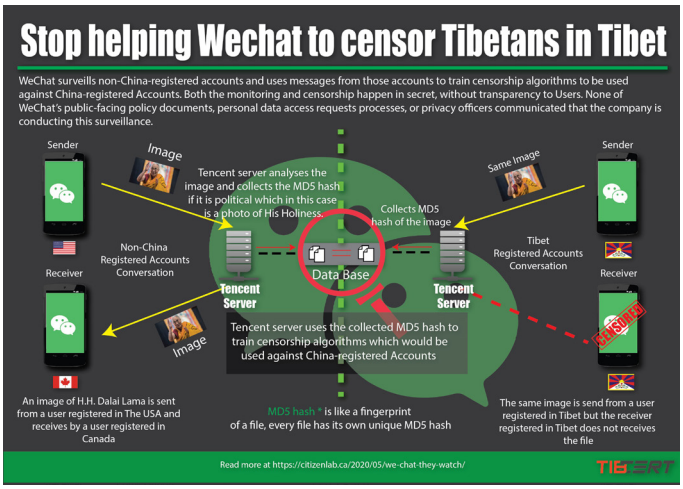


Figure 11: Illustration of an image of HHDL sent between non-Chinese registered accounts which Tencent identifies as politically sensitive after analysis and stores its MD5 hash. This stored MD5 hash is used to censor the same image sent between Tibet-registered accounts in real time.

5.3 TikTok Security Issues

In 2017, the Chinese internet company ByteDance bought the Musical.ly app (based in Shanghai but with most users living in the United States). After the acquisition, ByteDance (now the largest startup company in the world) relaunched the app as TikTok, migrating all Musical.ly accounts over by August 2018.[15]

According to documents reviewed by The Guardian, ByteDance has been using TikTok to help further Chinese foreign policy efforts.[16] TikTok's moderation policy, for example, showed TikTok censoring content that was embarrassing or sensitive to the Chinese regime, at times quietly changing videos to be visible only to the poster or labeling them as "not recommended" or "not for feed," thereby making

14 https://citizenlab.ca/2020/05/we-chat-they-watch/

15 https://www.vox.com/open-sourced/2019/12/16/21013048/tiktok-china-national-security-investigation

16 https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing

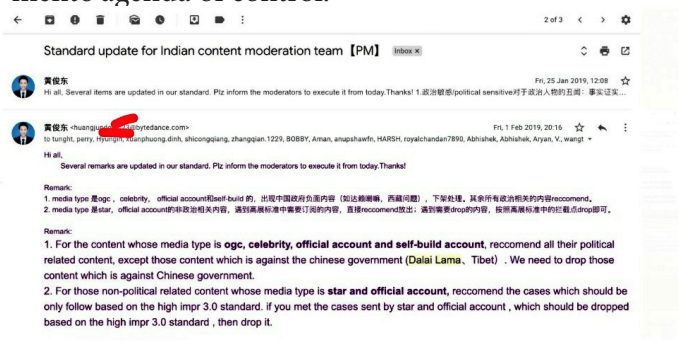
them difficult to access.[17] Such censored information has included highly controversial issues such as the Tiananmen Square massacre, Tibetan independence, the religious group Falun Gong, widely publicized pro-democracy protests in Hong Kong, Chinese government oppression of the Uyghur Muslim population, and other issues that criticize the social structure of the CCP.[18]

A specific incident of TikTok surveillance and censorship happened to Feroza Aziz when she was locked out of her account after the New Jersey teenager discussed the internment of Uyghur Muslims in Xinjiang in videos masquerading as makeup tutorials.[19] Even though TikTok is only available outside of China, the app is censoring such content that may be banned in Tibet and China but is legal in the jurisdictions where its users are based. This raises some serious implications of Chinese censorship reaching far beyond its borders into free societies.

One of the main areas of concern is that, due to Chinese data privacy laws, Chinese companies that collect user data have to share that data with the Chinese government upon request. It's not that Chinese authorities actively monitor every user's data in real time. However, the reality is that if and when authorities in Beijing make a demand, companies based in China have very little recourse to say no. This raises a major concern that the Chinese company Bytedance now owns TikTok, given that TikTok collects so much user data, including usernames, preferences, location data, and what's recorded by microphone and camera.[20]

Due to concerns about the implications of Chinese government censorship of information in the United States, in the fall of 2019, U.S. officials launched a national security investigation of TikTok, led by the Committee on Foreign Investment in the United States (CFIUS) which reviews foreign investment and real estate transactions in the U.S with regard to national security. Given that TikTok did not seek clearance from CFIUS when it acquired Musical.ly, the U.S. security panel now has scope to investigate the deal.[21]

Furthermore, it has recently been revealed that TikTok sent an email to its employees in India to remove any content which is related to His Holiness the Dalai Lama, Tibet, or thought to be against the Chinese government. This act by TikTok not only shows that users now have much less control over their content as it might be removed, but it reveals the influence and power Chinese authorities wield over corporations in order to further the government's agenda of control.


Standard update for Indian content moderation team【PM】 Inbox ×

2 of 3

黄俊东 Fri, 25 Jan 2019, 12:08

Hi all, Several items are updated in our standard. Plz inform the moderators to execute it from today.Thanks! 1.政治敏感/political sensitive对于政治人物的五阅：事实证实...

黄俊东 <huangjundong@bytedance.com> Fri, 1 Feb 2019, 20:16

to tunght, perry, Hyunghi, Hamphuong.dinh, shicongqiang, zhangqian.1229, BOBBY, Aman, anupshawfn, HARSH, royalchandan7890, Abhishek, Abhishek, Aryan, V, wangt

Hi all,

Several remarks are updated in our standard. Plz inform the moderators to execute it from today.Thanks!

Remark:

1. media type 是ogc， celebrity， official account和self-build 的，出现中国政府负面内容（如达赖喇嘛，西藏问题），下架处理。其余所有政治相关的内容reccomend。

2. media type 是star，official account的非政治相关内容，遇到高展标准中需要订阅的内容，直接reccomend放出；遇到需要drop的内容，按照高展标准中的拦截点drop即可。

Remark:

1. For the content whose media type is **ogc, celebrity, official account and self-build account**, reccomend all their political related content, except those content which is against the chinese government (Dalai Lama、Tibet) . We need to drop those content which is against Chinese government.

2. For those non-political related content whose media type is **star and official account,** reccomend the cases which should be only follow based on the high impr 3.0 standard. if you met the cases sent by star and official account , which should be dropped based on the high impr 3.0 standard , then drop it.

Figure 12: Email from TikTok to Indian Employees

Finally, the cybersecurity firm "Check Point " found that TikTok has "multiple" security vulnerabilities. For example, attackers could create a fake text message that appeared to be from TikTok but actually contained a malicious link. Once users clicked on the link, hackers could take control of the account, manipulating the content by uploading and deleting videos and revealing personal information such as private email addresses.[22] When describing TikTok, Reddit CEO Steve Huffman said, "Because I look at that app as so fundamentally parasitic, that it's always listening, the fingerprinting technology they use is truly terrifying, and I could not bring myself to install an app like that on my phone." "I actively tell people, 'Don't install that spyware on your phone,' he later added."[23]

17 https://www.vox.com/open-sourced/2019/12/16/21013048/tiktok-china-national-security-investigation

18 https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing

19 https://www.theguardian.com/technology/2019/nov/27/tiktok-makeup-tutorial-conceals-call-to-action-on-chinas-treatment-of-uighurs

20 https://www.tiktok.com/legal/privacy-policy?lang=en

21 https://www.cnbc.com/2019/11/01/us-to-investigate-tiktok-over-national-security-concerns-sources-say.html

22 https://www.cnbc.com/2020/01/09/tiktok-security-flaw-found-that-allowed-hackers-to-access-accounts.html

23 https://techcrunch.com/2020/02/26/reddit-ceo-tiktok-is-fundamentally-parasitic/

5.4 Zoom

With the outbreak of COVID-19 pandemic, various nations imposed lockdowns and quarantine laws to contain the spread of the virus. With the increased social distancing, many people around the globe started using video-conferencing platforms for personal and professional purposes. One of the most used platforms is Zoom video-conferencing. Daily meeting participants for Zoom surged from 10 million in December to 300 million in April. The sudden popularity of Zoom, however, also uncovered multiple privacy risks when it expanded rapidly to massive numbers of people around the globe.

However, before we go into the security issues related to Zoom (part of a research report by the Citizen Lab), it is important to take a step back and consider certain questions, parameters, and best practices when deciding whether or not to use any proprietary software or service (not just Zoom). For example:

- TibCERT promotes open source tools, however we acknowledge the reality that many of us will probably be using proprietary software for usability or functionality (whether paid or free). So the ability to use open source tools is not present at all times.
- When choosing a software or service, look into the track record of the company as it is an important aspect in understanding how the company operates. Has the company had any privacy issues in the past or misled the public in any way?
- Has the service or software you are considering been independently analyzed and verified? Does the company share responsible disclosure and how has it reacted to past compromises or challenges to its product or operations?
- What are you using this service for? Is it for public consumption (e.g., online events or conversations that would not be harmful if listened to by people outside your intended audience) or for more privacy focused work (e.g., planning calls or sharing of sensitive information).
- What and who are any threats to you or your work and are they involved with this company in any type of way that could be harmful to you or your organization?

When asking yourself such questions, it is important to remember that no technology application is the solution for everything as there are always pros and cons. The important thing to remember is that when deciding which tech to use, the answer is more nuanced than just focusing on black and white criteria. Know what tech you are using for what purpose, and if you decide not to use one type of software, do not just jump to another without properly vetting it and thinking about the above framework.

So the question that is on everyone's mind is should you use Zoom? In reality, this is for each individual to decide based on their own threats and how they are using Zoom (which again is true for any service or software). At TibCERT, based on the above criteria, we don't recommend using Zoom for any Tibet movement internal calls. However, based on its usability and reach, we feel that there is less risk of using Zoom, for example, for public and online briefings, given that the information is meant to be consumed by anyone. In this way, it does not pose a threat if, for example, the Chinese government were to access the information.

On April 3, 2020, the Citizen Lab at the University of Toronto released a research report[24] on Zoom which highlights the issues mentioned above. The key takeaways from the report are as follow:

Zoom was found to route its data traffic through China, even when none of the users were in China. The data being transferred through Chinese servers raised a number of questions regarding security, surveillance, and how Zoom might be forced to comply with the Chinese government if authorities demanded the release of data.

Zoom had claimed to use "AES-256" encryption for meetings. However, the Citizen Lab's research showed that for each Zoom meeting, a single AES-128 key was used in ECB mode which has an inherent weakness due to the fact that this mode preserves patterns in the input.

Zoom had earlier misled users by saying it was using "end to end encryption" when in reality, Zoom meetings only implement transport encryption. This means data is only encrypted

24 https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

between the user and the server and not from one user to another user, as in the case of true end to end encryption.

It must be noted that after the report came out, Zoom worked on these issues and provided updates with assurances that they have fixed the above and other security issues. However, it is also important to note that the only reason any of us are aware of these issues is the fact that the Citizen Lab decided to conduct this research for public knowledge. Given Zoom's past questionable disclosures and inaccurate statements about its product security, it is again recommended not to conduct any Tibet sensitive conversations or planning over Zoom.

To the question of what does TibCERT use instead of Zoom: we use Jitsi[25] which is an open source video conference system and we have deployed our own instance. As for live streaming, we use OBS[26] which is an open source live streaming software.

In conclusion, it is important to understand the nuances on how to select a software/service based on your own threat and what you are using it for. And again, know what tech you are using for what purpose, and if you decide not to use one type of software, do not just jump to another without properly vetting it and thinking about the above framework.

24 https://jitsi.org/jitsi-meet/
25 https://obsproject.com/

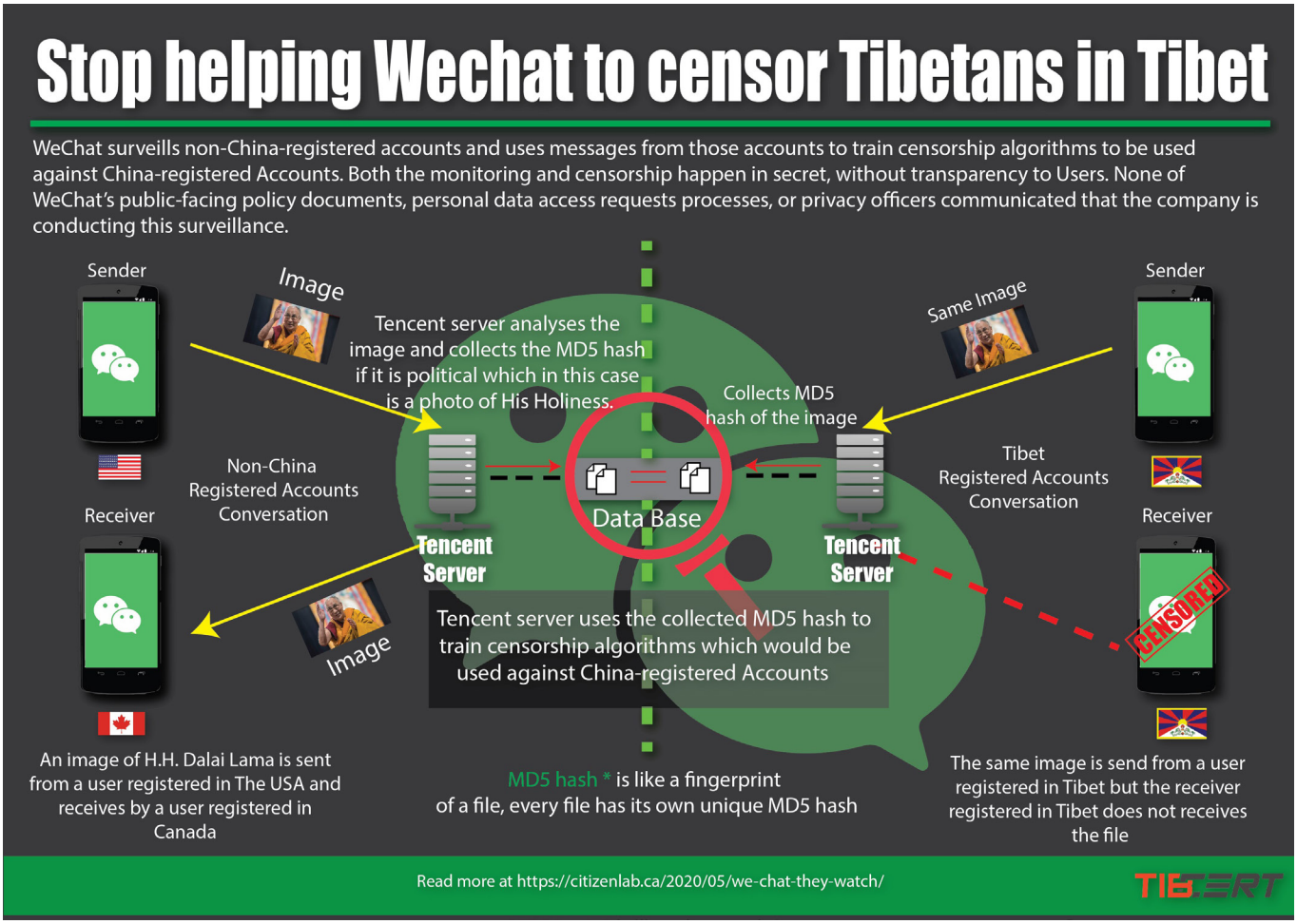


Figure 11: Illustration of an image of HHDL sent between non-Chinese registered accounts which Tencent identifies as politically sensitive after analysis and stores its MD5 hash. This stored MD5 hash is used to censor the same image sent between Tibet-registered accounts in real time.