

The complication of cyber manhunt: How cyber manhunt further complicated the ethical conflict between breaching the confidentiality and endangering the society in face of the COVID-19 pandemic

Yen-Chang Chen, Yen-Yuan Chen

Submitted to: Journal of Medical Internet Research
on: March 27, 2021

Disclaimer: © The authors. All rights reserved. This is a privileged document currently under peer-review/community review. Authors have provided JMIR Publications with an exclusive license to publish this preprint on its website for review purposes only. While the final peer-reviewed paper may be licensed under a CC BY license on publication, at this stage authors and publisher expressly prohibit redistribution of this draft paper other than for review purposes.

Table of Contents

Original Manuscript.....	4
---------------------------------	----------

Preprint
JMIR Publications

The complication of cyber manhunt: How cyber manhunt further complicated the ethical conflict between breaching the confidentiality and endangering the society in face of the COVID-19 pandemic

Yen-Chang Chen¹ MD, MA; Yen-Yuan Chen² MD, MPH, PhD

¹Department of Internal Medicine, Lotung Poh-Ai Hospital Taipei TW

²Department of Medical Education, National Taiwan University Hospital Taipei TW

Corresponding Author:

Yen-Yuan Chen MD, MPH, PhD

Department of Medical Education, National Taiwan University Hospital

#7, Rd. Chong-Shan S.,

Chong-Cheng District

Taipei

TW

Abstract

While health care and public health workers are working on measures to mitigate the COVID-19 pandemic, there is an unprecedentedly large number of people spending much more time indoors, and relying heavily on the Internet as their lifeline. What has been overlooked is the influence of the increasing online activities on public health issues. In this article, we pointed out how a large-scale online activity called cyber manhunt may threaten to offset the efficacy of contact tracing investigation, a public health intervention considered highly effective in limiting further transmission in the early stage of a highly contagious disease outbreak such as the COVID-19 pandemic. In the first section, we presented a case to show how personal information obtained from contact investigation and disclosed in part on the media provoked a vehement cyber manhunt. We then discussed the possible reasons why netizens collaborate to reveal anonymized personal information about contact investigation, and specify, from the perspective of public health and public health ethics, four problems of cyber manhunt, including the lack of legitimate public health goals, the concerns about privacy breach, the impact of misinformation, and social inequality. Based on our analysis, we concluded that more moral weight may be given to protecting one's confidentiality, especially in an era with the rapid advance of digital and information technologies.

(JMIR Preprints 27/03/2021:29135)

DOI: <https://doi.org/10.2196/preprints.29135>

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

☒ **Please make my preprint PDF available to anyone at any time (recommended).**

Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.

Only make the preprint title and abstract visible.

No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

☒ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**

Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain visible to all users.

Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <http://preprints.jmir.org/preprint/29135>

Original Manuscript

MAIN ARTICLE BODY**Introduction**

As of February 5, 2021, the Corona Virus Disease-2019 (COVID-19) global cases totaled 105,387,133. Among them, 2,299,083 individuals have died. As reported by Johns Hopkins Coronavirus Resource Center, the top five countries with confirmed COVID-19 cases are the U.S. (26,808,328), India (10,814,304), Brazil (9,447,165), the U.K. (3,922,910), and Russia (3,891,274), and the top five countries with total deaths from COVID-19 are the U.S. (459,403), Brazil (230,034), Mexico (164,290), India (154,918), and the U.K. (111,477) [1]. Originating from Wuhan, China, this illness seemed to seriously devastate European countries and the U.S., most of which undoubtedly had a lot of trade and transport links to China.

Due to Taiwan's proximity to and hundreds of daily direct flights between China, Taiwan was anticipated to have the second largest number of COVID-19 confirmed cases outside of China based on predictions of the Johns Hopkins Center for Systems Science and Engineering [2], and approximately six thousand imported cases and four thousand local cases were expected. Surprisingly, only 923 cases were confirmed to have been infected by COVID-19 in Taiwan, with only nine of them dying of COVID-19 [1]. In addition, only a few of them were locally transmitted cases, and no evidence has supported that local spread is ongoing in Taiwan. Without any lockdown, Taiwan so far has successfully flattened the increasing number of COVID-19 confirmed cases and total deaths, and prevented local spread of COVID-19.

According to Wang et al.'s report, Taiwan implemented many actions in response to the suspicion of the unknown pneumonia in Wuhan, China as early as the end of 2019 December [3].

Some of these actions included contact investigation for all COVID-19 confirmed cases, mandatory home quarantine and self-monitoring for a total of 14 days from the last exposure to the confirmed case employed by the government, and fining those who did not comply. For transparency purposes, medical officials from the Central Epidemic Command Center (CECC) have been holding daily debriefings outlining each COVID-19 confirmed case, and addressing the COVID-19 pandemic's presence in Taiwan. To this end, there has been widespread use of big data—the National Health Insurance Dataset for border control, case identification, case containment, etc, to inform the ongoing response [3].

Among those actions taken by the government in response to the COVID-19 pandemic, epidemiological investigation for contact history is a very important strategy employed by the CECC investigation officers to identify those who have directly contacted with a COVID-19 confirmed case, and then strict home quarantine is carried out for those with direct contact with the case for preventing the possibility of local transmission in Taiwan. If the travel and contact history of a COVID-19 confirmed case, for any reason, is not clear, surveillance footage will be accessed by making use of the big data from mobile phone GPS monitoring, surrounding security cameras, and so on. During the daily debrief, the CECC's leading members anonymously reflect upon each newly confirmed COVID-19 case, as well as all persons the newly confirmed case has directly contacted. The following case was a COVID-19 confirmed case, No. 379, implying the ethical issue associated with the potential conflict between protecting an individual's confidentiality which is highly likely ruined by cyber manhunt and protecting the public health.

The Story

“Minister of Health and Welfare Chen Shih-Chung, who heads the center, said that the domestic case, No. 379, is a woman in her 30s who sought treatment at a hospital for a fever and a runny nose on Saturday last week, and tested positive yesterday.

While the woman leads a relatively simple life and mainly remains at home, her husband in January traveled to Guangzhou, China, for work and she visited Southeast Asia in early February, Chen said, adding that 21 people who had direct contact with her have been identified and a further contact investigation is under way.

Centers for Disease Control Deputy Director-General Chuang Jen-Hsiang said that the woman claimed that she usually stays at home and only walks to nearby shopping centers every day.

However, due to some difficulties in conducting the contact investigation, the local health department would need to access surveillance footage and other data sources to trace her activities and the possible source of infection, he said.” [4]

“TAIPEI (Taiwan News) — It has been confirmed a KTV bar hostess in Taipei City had Wuhan coronavirus (COVID-19) and continued to serve customers despite the fact she was experiencing symptoms.

On Wednesday (April 8), the Central Epidemic Command Center (CECC) announced that day’s sole confirmed local case, No. 379, was a woman in her 30s who had started developing a fever and had a runny nose during the Qingming holiday. On April 4, she sought medical treatment and on Wednesday tested positive for the disease.

Early on Thursday morning (April 9), Liberty Times reported the woman was a hostess at a well-known KTV bar frequented by wealthy businessmen near Taipei City's red-light district of Linsen North Road. When Department of Health personnel inspected the woman's place of employment on Wednesday night, they found it packed with hostesses and customers, reported ET today.

Upon being confirmed with the disease, the hostess claimed she had not traveled during the holiday and mostly stayed at home, other than visiting a nearby shopping center. However, people questioned at the KTV bar said she had continued to work during the period she had been experiencing symptoms." [5]

Given that the insufficient personal information and vague contact history provided by No. 379 to the investigation officer might result in local transmission of COVID-19, and that several reporters in the CECC daily debrief were so interested in and focused on No. 379's contact history, the leading members in the CECC daily debrief disclosed some of No. 379's personal information. Many online users were very interested in this case and actively tried their best to cyber-manhunt more personal information about No. 379. Since then, No. 379's personal information has gone viral. She was a high-profile hostess working part-time in several bars and KTVs in Taipei's most famous red-light district. A lot of personal information such as her marital status, her family members, the daily increasing number of persons being home quarantined due to having a direct contact with the hostess, and so on, can be easily googled and identified on several traditional Chinese webpages [6-9].

Contact Investigation and Cyber Manhunt

To contain a highly transmissible infectious disease, it is a crucial, early strategy to conduct complete epidemiological investigations on confirmed cases for every essential bit of personal contact history. In Taiwan, once a person is confirmed infected with COVID-19, limiting further transmissions by contact investigation would require investigation into where the person had travelled and visited, to whom the person had a close contact, what activities they had engaged in together, how long their interactions had lasted, and so forth. After that, those who have been in close contact to the confirmed case are required to undergo a 14-day mandatory self-quarantine starting from their last close contact. On one hand, if the information required for contact investigation is clearly and honestly disclosed by the confirmed case, and all persons to whom the confirmed case had a close contact are self-quarantined, then a COVID-19 local transmission is highly likely minimized or ceased. On the other, if a COVID-19 patient fails to disclose important information to the investigators, the CECC is likely to waste more time, efforts, and resources on contact investigation by using more intrusive methods, such as implementing facial recognition technology, assessing citizens' mobile location data, or even disclosing a part of the individual's sensitive personal information and travel history to the public in the CECC's daily briefings, broadcasted through the news media and disseminated on major social media. Contact-tracing investigations here act like a double-edged sword, in that while Taiwan's relatively low COVID-19 infection and death counts are attributable to its highly effective contact-tracing investigations [10], these public health interventions also generate significant concerns about privacy leaks and confidentiality breaches.

The intrinsic and derivative value of privacy and confidentiality matters from both the perspectives of morality and public health. While protecting one's confidential information from unauthorized access and misuse is considered of crucial value in medical and public health practice [11], it is arguable that confidentiality as a moral value is not absolute. In other words, confidentiality

breaches may be ethically acceptable as long as other more valuable interests are at stake [12]. However, as most people have their private realms that they do not want to be delved into, breach of confidentiality, caught easily by the public by access to the daily briefing, would undermine the trust between the public health authorities and the public, making further contact investigation more arduous and, as a possible result, increasing the chance for disease transmission. As the trust between the two groups is breaking down, the least intrusive contract tracing methods would become less effective, forcing the public health authorities to implement more intrusive interventions to maintain the effectiveness of their disease control task. Therefore, given that the accuracy of contact investigations is critical in containing a deadly infectious disease, the public health authorities are also responsible for maintaining the trust between the two groups. One possible way of maintaining the trust is to limit the degree of infringement of individual privacy by disclosing only part of the information (i.e., anonymization of personal information) that is not only just sufficient to protect the public's health, but also just insufficient to identify the patient.

Personal information and a contact history that is purposefully made incomplete to protect individual privacy, however, can trigger interested people's curiosity [13], foment their fear of infection [14, 15], and cause public panic [15, 16]. Curiosity has been put forward by previous researchers as a major factor in general that prompts netizens to commence a cyber manhunt [17]. Although there was no previous research conducted to understand the cyber manhunts associated with issues about infectious disease control, incomplete information may evoke netizens' subconscious fear of being infected, provoking a sense of insecurity (e.g., everyone including myself might have been in contact with the patient) and prompting initiation of a cyber manhunt to find out the anonymized individual's information. What remains unclear, however, is to what degree this fear impels netizens to call for a cyber manhunt. Moreover, social justice or online vigilantism is also an important factor for netizens to start a cyber manhunt. Disclosure of incomplete contact-tracing

information conveys to the public a false sense that the CECC has encountered difficulties in acquiring necessary information from the confirmed case, particularly when public health authorities also announced that the confirmed case has violated the COVID-19 control rules. While any confirmed cases who conceal or equivocate about information required for a comprehensive contact investigation can be legally punished in Taiwan, incomplete information disclosed in a daily briefing, even if the confirmed case did not violate any regulations, can be misunderstood as that the confirmed case must have disregarded the safety of the public. This can provoke netizens into calling for a cyber manhunt to complete the information that they thought the government had not been able to complete. Last but not least, to collaborate in finding information to protect others is probably done simply out of the nature of all social animals, like what meerkats do to warn others about approaching danger.

The Problems of Cyber Manhunt: a Public Health perspective

Public Health Is Not the Goal

Cyber manhunt can never be a legitimate public health intervention because the collective goal of all the participants is to uncover and expose the anonymized private information rather than to improve or protect the public's health. Although the outcome of some cyber manhunts may bring the targeted person(s) to justice and may benefit public health as a benign side effect, each individual participant in the same cyber manhunt activity may have a goal different from the goals of other participants. Thus, it is imprecise to say that these certain cyber manhunts are done out of a collective goal to improve or protect the public's health. We do not deny that a cyber manhunt can be advantageous in some cases (e.g. to find criminals) if conducted by netizens with care and conscience. Nonetheless, this is just not the case in acute outbreaks of sufficiently lethal, highly

contagious diseases because people share a subconscious fear of infection that increases their potential to behave irrationally [14]. Once a cyber manhunt is successfully launched in the cases of seemingly incomplete contact investigation, the massive scale of participation and involvement in that quest makes it difficult for public health authorities to control the cyber manhunt and avoid its adverse effects, such as stigmatization, infringement of privacy, involvement of the innocent, and so forth. Therefore, cyber manhunts conducted to dig up the details of a patient carrying a dreadful infection, as seen in the case we presented, is likely to cause more problems than advantages.

Breach of Digital Privacy

Privacy is a foundational value from the viewpoint of public health ethics [18]. To maintain public's trust and the effectiveness of infectious disease control measures, personal information gathered in the course of contact investigations can only be revealed to the public if its revelation is relevant to controlling a particular infectious disease and not traceable by the public to the person(s) at issue. On the contrary, participants of cyber manhunts, aiming at revelation of private information to the public, have no respect for privacy. In many countries, regulations protecting against infringement of privacy in general also restrain against cyber manhunts. For example, in Taiwan, online personal data is "information or data which can be used to identify a natural person" and is subject to the requirements of the Personal Data Protection Act (PDPA) [19]. Under Taiwan's PDPA, netizens who conduct a cyber manhunt can be held liable if they distribute personal data (such as one's phone number, home address, photos, and national identity number) without getting advance approval of the person(s) concerned. Given the extensive participation and unruliness of most cyber manhunts, the issues concerning infringement of privacy usually involves not only the person(s) targeted by interested netizens, but also the innocent people who are implicated in the cyber manhunts without justifiable reasons. In addition, online service providers who are responsible for

processing, collecting, and using their users' personal information confidentially may also be held liable.

The Impact of Misinformation Generated by Cyber Manhunt

During serious infectious disease outbreaks, the authenticity of the information about the disease is key to contain further transmission. However, most information reported in cyber manhunts is found to be nothing more than misinformation based on netizens' personal speculations [17]. Through the Internet, the impact of misinformation is unprecedented because it usually goes unchecked yet is spread quickly and reaches an enormous number of people, as during the COVID-19 pandemic [20]. Whereas speculations can become misinformation without being made up by people with bad intentions, it is not uncommon that some manipulative internet users tend to bend the truth and fabricate misinformation to draw the public's attention to serve individual interests [21]. Therefore, a cyber manhunt can be initiated based on mere misinformation and the trajectory of a large-scale cyber manhunt with millions of participants can be misled by just one interested, malicious internet user. Misinformation reproduced by the media can aggravate everyone's fear of infectious disease, prompting them to behave in the ways that run counter to the principles of infectious disease control. For example, people with an illness unrelated to COVID-19 may avoid seeking immediate medical attention because of fear of being infected by COVID-19. Misinformation about someone who were confirmed infected with COVID-19 at a hospital can scare off people who need medical attention provided by the hospital until the misinformation is debunked. Patients who are infected with COVID-19 and avoiding going to the hospital will not be diagnosed in time and are likely to pass the virus to other people.

The Problems Stemmed from Social Inequality

Social inequality is an inherent problem with cyber manhunting given that it is hardly possible for everyone, connected literally by the COVID-19 pandemic despite living in different communities or countries, to have an equal opportunity to access the Internet. Nowadays, even in countries with high smartphone penetration rates, this social inequality, also known as the Digital Divide, remains an issue to be addressed [22, 23]. For example, while most of the world's cyber manhunts occur in China, only about 0.854 billion out of 1.439 billion people (about 59.3%) had used the Internet by 2020 [24]. In Taiwan, there was still about 17% of its population who had never used the Internet in the same year as when the cyber manhunt reported in this paper occurred [25]. In addition, Digital Divide is a very complex issue because, for those who have an access to the Internet, the actual time spent on the Internet each day also varies in different genders, age groups, broadband speeds, means of connection, and so on [26].

The power of cyber manhunts conducted in the context of contact investigation cannot reach every corner of the world since the Internet is not ubiquitous. While in many developed countries only a small proportion of people lack access to the Internet, it is worth noting that these people are also socially marginalized, vulnerable, and disadvantaged. They have been suffering from health inequality and are now suffering more during the COVID-19 pandemic [27]. Lack of the Internet access further prevented them from getting online public health information and services, rendering them under a greater risk in public health crises. If cyber manhunts could bring about any benefits to the community, e.g., a warning to those who might have a close contact to a confirmed case, netizens who have a higher internet usage would be more likely than those who seldom or never used the Internet to benefit from the information discovered and posted online.

Ironically, for those who are underprivileged in terms of the Digital Divide, the Digital

Divide serves as a barrier against cyber manhunts. Although one who has never used the Internet might also fall prey to a cyber manhunt [28], those who spent less time online arguably have a smaller chance of becoming victims of a cyber manhunt. In the context of contact tracing, interested netizens will find out nothing or only paucity of personal information about those who have never connected to the Internet. In this case, a cyber manhunt only begets few, if any, advantages but it does create more problems.

Considering those proposed above, more moral weight should have been given to protecting No. 379's confidentiality, rather than disclosing No. 379's sensitive personal information such as her occupation as a part-time hostess, contact history about who she had close contact with, and the bars, KTVs where she worked as a hostess, the information which absolutely would attract a lot of online users' interests in cyber-manhunting more details. Moreover, if No. 379 must continue to be reported to the public in the CECC's daily debrief, all the sensitive information that would be highly anticipated to attract a lot of the public's attention should not be disclosed to the public. Instead, only the information that seems to be general and helpful for press release, e.g. the viral load, the clinical presentation, and so on, is appropriate for disclosure to the public.

Conclusion

Particularly in the pandemic of COVID-19 which is highly transmissible, and easily wreaks havoc on the health care system, protecting one's confidential information is never easy, due to the conflict between protecting confidentiality and protecting public health. With the swift advance of digital and information technology, we are continually in awe of how much technology has been helpful to our daily lives, without fully realizing how much inconvenience and harm technological advance can have on another's daily life. Searching one's information online is so easy,

yet protecting one's confidential information is even more difficult now with more digital and informational technologies. Therefore, based on the above ethical analysis, breaching one's confidentiality for protecting public health in face of a public health crisis should be carefully deliberated. More moral weight may be given to protecting one's confidentiality, especially in an era with the rapid advance of digital and information technologies.

The Aftermath

The CECC's disclosure of some personal information and footage of COVID-19 case No. 379 to the public in a daily debrief resulted in widespread cyber manhunts. The hostess' photo, whether it was fake or not fake, then could be identified easily online. Most of the reporters, online users, and those who were very interested in No. 379 now knew where the hostess worked, her and her husband's occupations, details about her kids, and some of the most intimate detail of her life. The hostess not only had to experience the loneliness of the 14-day quarantine, but also she needs to make more efforts on how to let her husband and kids accept the fact that she was a hostess, and how to protect her home from being ruined by the cyber-manhunts, a serious complication induced by the governmental action to disclose only limited confidential information of the hostess to the public for the purpose of protecting the society.

ACKNOWLEDGEMENTS

This study was supported by the research grants from Taiwan Ministry of Science and Technology (MOST 108-2634-F-002-024). The funder did not have any involvement in ethical analysis, proposing suggestions, writing of this manuscript, and decision to submit this manuscript for publication.

CONFLICTS OF INTEREST

To the best of our knowledge, no conflict of interests exists.

REFERENCES

1. Johns Hopkins University Coronavirus Resource Center. COVID-19 Dashboard. 2020 [cited 2021 February 5]; Available from: <https://coronavirus.jhu.edu/map.html>.
2. Gardner L. Modeling the Spread of 2019-nCoV. 2020 [cited 2021 February 5]; Available from: <https://systems.jhu.edu/research/public-health/ncov-model/>.

3. Wang CJ, Ng CY, Brook RH. Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing. *JAMA*. 2020 Apr 14;323(14):1341-2. PMID: 32125371. doi: 10.1001/jama.2020.3151.
4. Lee IC. Virus Outbreak: Three new COVID-19 cases confirmed. *Taipei Times*; 2020 [cited 2021 February 5]; Available from: <https://www.taipeitimes.com/News/front/archives/2020/04/09/2003734266>.
5. Everington K. Coronavirus-infected Taipei KTV hostess kept serving customers. *Taiwan News*; 2020 [cited 2021 February 5]; Available from: <https://www.taiwannews.com.tw/en/news/3912974>.
6. Ministry of Health and Welfare. 3 2 1 . Ministry of Health and Welfare; 2020 [cited 2021 February 5]; Available from: <https://www.mohw.gov.tw/cp-4633-52651-1.html>.
7. Ministry of Health and Welfare. 9 . Ministry of Health and Welfare; 2020 [cited 2021 February 5]; Available from: <https://www.mohw.gov.tw/cp-4633-52664-1.html>.
8. SETN. 379 . SETN; 2020 [cited 2020 May 3]; Available from: <https://www.setn.com/news.aspx?NewsID=722969>.
9. Liberty Times net. 379 . Liberty Times net; 2020 [cited 2021 February 5]; Available from: <https://news.ltn.com.tw/news/life/breakingnews/3129020>.
10. Chang IJ. Taiwan's Model for Combating COVID-19: A Small Island with Big Data. 2020 [cited 2021 February 5]; Available from: <https://www.mei.edu/publications/taiwans-model-combating-covid-19-small-island-big-data>.
11. Beltran-Aroca CM, Girela-Lopez E, Collazo-Chao E, Montero-Perez-Barquero M, Munoz-Villanueva MC. Confidentiality breaches in clinical practice: what happens in hospitals? *BMC Med Ethics*. 2016 Sep 2;17(1):52. PMID: 27590300. doi: 10.1186/s12910-016-0136-y.
12. Sulmasy DP, Veatch RM. Should Institutions Disclose the Names of Employees with Covid-19? *Hastings Cent Rep*. 2020 Apr 12. PMID: 32279318. doi: 10.1002/hast.1107.

13. Tang X, Renninger KA, Hidi S, Murayama K, Lavonen J, Salmela-Aro K. The Differences and Similarities between Curiosity and Interest: Meta-analysis and Network Analyses. 2020 [cited 2021 February 5]; Available from: <https://doi.org/10.31234/osf.io/wfprn>.
14. Pappas G, Kiriaze IJ, Giannakis P, Falagas ME. Psychosocial consequences of infectious diseases. *Clin Microbiol Infect*. 2009 Aug;15(8):743-7. PMID: 19754730. doi: 10.1111/j.1469-0691.2009.02947.x.
15. Samuel J, Ali GGMN, Rahman MM, Esawi E, Samuel Y. COVID-19 Public Sentiment Insights and Machine Learning for Tweets Classification. *Information*. 2020 Jun;11(6). PMID: WOS:000551236800009. doi: ARTN 314 10.3390/info11060314.
16. Nicomedes CJC, Avila RMA. An analysis on the panic during COVID-19 pandemic through an online form. *J Affect Disord*. 2020 Nov 1;276:14-22. PMID: 32697692. doi: 10.1016/j.jad.2020.06.046.
17. Chen R, Sharma SK. Human Flesh Search - facts and issues. *Journal of Information Privacy and Security*. 2011;7(1):50-71.
18. Lee LM. Public health ethics theory: review and path to convergence. *J Law Med Ethics*. 2012 Spring;40(1):85-98. PMID: 22458465. doi: 10.1111/j.1748-720X.2012.00648.x.
19. Laws & Regulations Database of the Republic of China. Personal Data Protection Act. 2015 [cited 2021 February 5]; Available from: <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021>.
20. Lee JJ, Kang KA, Wang MP, Zhao SZ, Wong JYH, O'Connor S, et al. Associations Between COVID-19 Misinformation Exposure and Belief With COVID-19 Knowledge and Preventive Behaviors: Cross-Sectional Online Study. *J Med Internet Res*. 2020 Nov 13;22(11):e22205. PMID: 33048825. doi: 10.2196/22205.
21. Chandel S, Chen Y, Dai J, Huang J. Cyber Manhunt: Evaluation of Technologies and

Practices for Effective Community Development and Maintenance. *Advances in Information and Communication*. 2020:883-902.

22. Robotham D, Satkunanathan S, Doughty L, Wykes T. Do We Still Have a Digital Divide in Mental Health? A Five-Year Survey Follow-up. *J Med Internet Res*. 2016 Nov 22;18(11):e309. PMID: 27876684. doi: 10.2196/jmir.6511.

23. Campos-Castillo C, Laestadius LI. Racial and Ethnic Digital Divides in Posting COVID-19 Content on Social Media Among US Adults: Secondary Survey Analysis. *J Med Internet Res*. 2020 Jul 3;22(7):e20472. PMID: 32568726. doi: 10.2196/20472.

24. Internet World Stats: Usage and Population Statistics. [cited 2021 February 5]; Available from: <https://www.internetworldstats.com/stats3.htm#asia>.

25. Taiwan Network Information Center. 2020 Taiwan Internet Report. Taipei Civil Education Foundation; [cited 2021 February 5]; Available from: https://report.twnic.tw/2020/en/TrendAnalysis_internetUsage.html.

26. Roser M, Ritchie H, Ortiz-Ospina E. Internet. 2015 [cited 2021 February 5]; Available from: <https://ourworldindata.org/internet>.

27. American Medical Association. Impact of COVID-19 on minoritized and marginalized communities. 2020 [cited 2021 February 5]; Available from: <https://www.ama-assn.org/delivering-care/health-equity/impact-covid-19-minoritized-and-marginalized-communities>.

28. Coonan C. Handsome Chinese vagrant draws fans of 'homeless chic'. 2010 [cited 2021 February 5]; Available from: <http://www.independent.co.uk/news/world/asia/handsome-chinese-vagrant-draws-fans-of-homeless-chic-1915812.html>.