Life vs. Livelihood – User Privacy During COVID-19 Virus Communication

Full Paper

Paras Bhatt
The University of Texas at San Antonio
paras.bhatt@utsa.edu

Naga Vemprala
The University of Texas at San Antonio
naga.vemprala@gmail.com

Rohit Valecha
The University of Texas at San Antonio
rohit.valecha@utsa.edu

H. Raghav Rao
The University of Texas at San Antonio
hr.rao@utsa.edu

Abstract

Twitter has been one of the commonly used means of communication for connecting people. Twitterers actively share tweets which include details about their activities and the location of the users. However, in the case of COVID-19, , questions are raised about communication monitoring of virus spreading hotspot locations and the transmission of alarming messages about virtual assistants powered by artificial intelligence, violating privacy resulting in a spiraling financial loss over social media. Considering the prevalence of debates on Health vs. Economy issues, the discussion of privacy concerns around these topics require a closer study. Using tweets collected during the outbreak, we conduct exploratory research and find a herd activity about privacy messages.

Keywords

coronavirus, covid-19, exploratory analysis, privacy, text mining, text analytics, data mining, LDA.

Introduction

There have been numerous incidents of breaches of user privacy (The National Law Review, 2020, March 12) following the onset of the Covid-19 pandemic. Protecting user privacy during times of crisis is crucial because if personal information is revealed to the public without adequate privacy protection, it can have a negative impact on both their lives and their livelihoods (Hiller & Russell, 2017). Pandemics are traumatic times, and the last thing a person needs to worry about during that time is that someone has knowledge about them. On the contrary, even reclusive people wish to be connected to society more during times of disaster so that they have a better chance at survival. Covid-19 is no different as there has been an influx of patients that are now on Medicaid and Medicare programs (Modern Healthcare, 2020, April 29). A steep increase in healthcare services to such an affected population is accompanied by a tremendous amount of health data being generated and recorded. It is only but natural that some of this data falls through the cracks during times of this global medical emergency that has overwhelmed healthcare institutions all over the world. However, cases of negligence are on the rise (Mercer, 2020, April 06), and they can certainly have long-term effects on the lives of the affected people.

There have been significant efforts to be as robust as possible while collecting information during this pandemic. However, as is the case during times of disaster, user privacy has yet again taken a backseat in the times of the novel coronavirus outbreak worldwide (Palen et al., 2010). Besides the rapid advances in telehealth/telemedicine, remote work, and unique supply chains, the conversation regarding protecting users' privacy becomes even more important. Mental health issues lead users to pursue counseling online, people with Covid-19 seek medical advice through web portals, patients who self-quarantine at home are monitored using remote health devices, and government and medical agencies are increasingly calling for personal information to limit the spread of the virus. Contact tracing dominates the conversation about privacy and poses a potential risk that the sincere efforts of the government will be derailed merely because

of the malicious intent of some adversaries to compromise user's privacy. Negligence is another factor to consider when using the methodology of contact tracing identifying cases while protecting the privacy of those tracked and monitored.

User privacy has always been a contentious issue even when everything is normal, but it becomes even more critical during times of emergencies when the probability of a lack of oversight is particularly high. Users online are fearful of their privacy being compromised, and their personal health information being misused, which can have a detrimental effect on their personal lives. In the same light, users are afraid of the ramifications that privacy breaches might have on their ability to participate in the economy. Users are fearful of the impact that a disclosure of private information, related to Covid-19, can have on their livelihoods – whether they would be able to rent an apartment or not, or be retaliated against at work or even fired because of fear of spreading the virus to the rest of the workforce (Vemprala, Akello, Valecha & Rao, 2020). This privacy discussion around Lives vs. Livelihood is central to our methodology in this paper. We outline how users online are expressing their privacy concerns related to how they live their lives and how they earn their livelihoods during these testing times, where a pandemic still rages on in the community. However, some studies argue that the social media act as a platform for individuals to share controlled information at their own will and is beneficial for saving lives (Househ, 2012).

Therefore, we follow a topic modeling approach to the social media messages to determine what privacy means for people in society during a pandemic. We study Twitterati tweets to outline the general feelings in these times about user privacy. We also take a look at the public's emotional response to privacy in discussions related to both health and the economy. We find that people are more concerned about protecting their health-related information and ensuring privacy. Our analysis clearly aligns with the context of answering the questions below in this exploratory study.

1) What are the privacy concerns of Twitterati during COVID-19 pandemic?

2) What is the trend of privacy in relation to Health (life) versus Economy (livelihood) during the COVID-19 pandemic?

Literature Review

People crave information during times of crisis, especially in online environments, such as Twitter. In such times, there is a desire to gather as much information as possible. However, not much effort is being made to protect the privacy of the data collected (Adam, Shafiq, & Staffin, 2012) as is the case with the Covid-19 crisis where there were instances of releasing sensitive information without properly masking people's identity. Such deliberate or unintentional disclosure of information could have far-reaching implications for people's privacy. They can have an impact on both personal and professional lives.

Covid-19 has devastated lives with the loss of loved ones, compromised citizens' health, and bankrupt economies with the increasing infection spread across much of the industrialized world. Many strategies have been put in place to combat the pandemic, including large scale testing of patient samples. Advances have been made in the field of testing from routine testing, which is an uncomfortable experience attached to a drawn-out wait to get the results to rapid and pooled testing that delivers results within hours and can be used to test samples from multiple people at once. Nevertheless, these testing advances are not all smooth and privacy conserving. Concerns about privacy breaches have been raised where the testing information could be compromised or mismanaged (HHS.gov, 2020, April 9).

Another strategy was to practice social distancing and either self-imposed or mandatory quarantines. Even after these quarantines, people still managed to use collaborative online video conferencing solutions to work and study remotely, make appointments and visits to doctors using telehealth facilities, and apply for online economic stimulus payments. Like testing, remote work and telehealth also have a fair share of infringements of privacy that can be counterproductive to the whole point of shifting such online operations. However, with the only option to work off-site during the pandemic, there are numerous concerns about such privacy violations, as past studies show that off-site employees are more likely to infringe data (TechRepublic, 2018, June 20).

Yet another concern is the contact tracing efforts of the Government or other related agencies that are tasked with monitoring the spread of the virus. Contact tracing methodology used in the past has not been devoid of privacy concerns (Levine, 1988). There have been numerous pleas by the scientific community to

maintain patient privacy, and a violation while using such methodology can have grave impacts for those whose data gets compromised. It is for this reason that so many people are concerned about the extent to which the agencies can trace individuals and what information exactly do they need.

Conversely, privacy is also being used as a shield to protect organizations from looking bad in the eyes of the public by not releasing actual Covid-19 numbers and relevant information. While withholding information about the virus and the situation in the community affected by it, officials and agencies are using privacy as a shield to prevent themselves from being accountable (kcrg.org, 2020, March 3). This duplicitous use of privacy is increasingly being used by community officials in Covid-19 hotspots to hide their administration's lax efforts to control the virus spread.

All of these issues related to Covid-19 are in the public domain, and there are multiple health agencies, governments, and medical institutions that are handling the pandemic as they deem fit. They carry out press briefings, publish newsletters and advisories that outline the official response to the pandemic. However, there have been few public forums and institutions that study or lend support to the voice of the public. In such a condition, the emotional response to the pandemic has been heavily shared on social media platforms and none more so than Twitter.

The public is divided between supporting the Government and its contact tracing efforts or protecting their fourth amendment rights. The Right to Privacy is fundamental in the American Constitution, and people are wary of being traced because of past misgivings regarding surveillance (Aivazpour and Rao, 2019; Chen, 2017). In the discussions regarding health, there are ethical questions regarding whether in times of pandemic, the health of people is more important or to honor their desire for privacy. In the discussions about the economy, it is imperative to protect the privacy of people in the workforce as getting a positive diagnosis of Covid-19 can affect their current work status, insurance, and also their ability to find work in the future. Further, people are not aware of what are the implications of being tested positive and in such situations who knows, how much, and why are important questions raised by people. Twitter serves as an outlet for these people to voice these concerns about users' privacy during Covid-19.

Methodology

Given the tremendous use of Twitter during crisis communication management, researchers have adopted various techniques to extract meaningful information from tweets using text mining techniques like content analysis (Oh, Agrawal, & Rao, 2011), Social Network Analysis (Chatfield & Brajawidagda, 2012), and Clustering (Ashktorab, Brown, Nandi, & Culotta, 2014) so as to deal with the highly dynamic, uncertain and extreme nature crisis events. During such emergencies, Twitter can help learn about the situation and educate communities on preparedness measures, lessen the intensity of negative messages, and promote positive messages (Rao, Vemprala, Akello, & Valecha, 2020; Vemprala et al., 2020). In order to establish such a crisis response management system, we need to explore the data based on both temporal characteristics as well as semantic text. Therefore, in this study, we focus on examining privacy concerns during the COVID-19 pandemic, outlining various topics discussed in the tweets using LDA topic modeling, a text-mining algorithm.

This study presents an analysis of tweets produced from January 20, the day China officially confirmed the existence of the infection outside Hubei province. We used twitter streaming API to collect the tweets based on the keyword coronavirus and added COVID-19 to our list, when the WHO officially named the disease. This streaming API looks for these keywords anywhere in the tweet and extracts the tweet text and the tweet characteristics, including retweets count, screen name of the tweet user, time when the tweet is posted, and hashtags. As of June 6, we collected around 142 million tweets for 139 days. Figure 1 shows the records count by days.

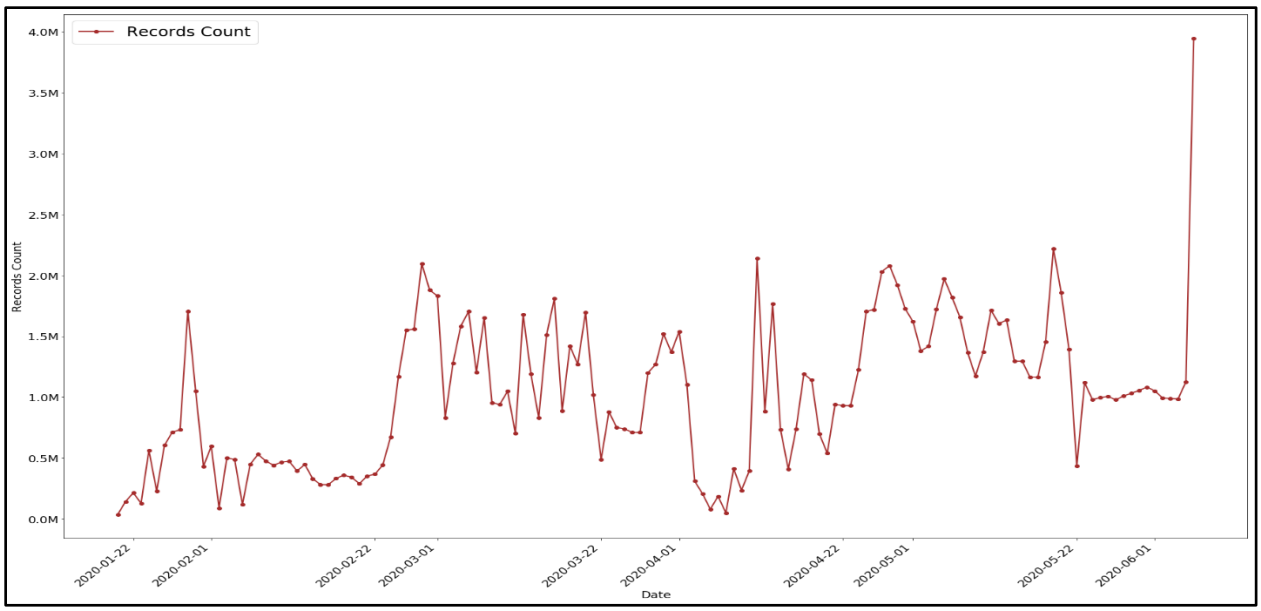

Figure 1. Timeline of Coronavirus Tweets

The spread of the virus during this period left many communities and health workers who were exposed to disease, under severe psychological stress, while exacerbating existing challenges in the healthcare domain. Over three-fourths of the world is under lockdown in an effort to stay safe, with many technology-based organizations providing work-from-home options to their employees while many other companies are laying off their employees, leaving millions of workers jobless. People around the world are under two types of stress due to COVID-19, Health, and Economy. In this study, we study the privacy concerns of users in the context of Health vs. Economy in privacy-related tweets. We used a keyword-based search to search for privacy-related tweets and included both privacy and confidentiality keywords in our search criteria. There were no privacy-related messages in our dataset during the initial 45-day period. As a result, we considered the tweets from March 1 to June 6 in our current study. We classified these tweets into Health privacy and Economy privacy categories. In order to objectively classify the tweets for Health and Economy, we need the keywords specific to COVID-19 for health and economy. Hence, we trained an LDA topic model using the most relevant web pages providing health and economy updates on COVID-19 (Blei, 2012). Topic model provides keywords that are closely related to each of the topic. We systematically analyzed the words under each topic, separated the health and economy keywords to represent unique keywords in each of the categories, and classified health and economy-related tweets if any of the respective keywords are present in the tweets. Figure 2 shows the distribution of privacy-related tweets by health and economy categories.

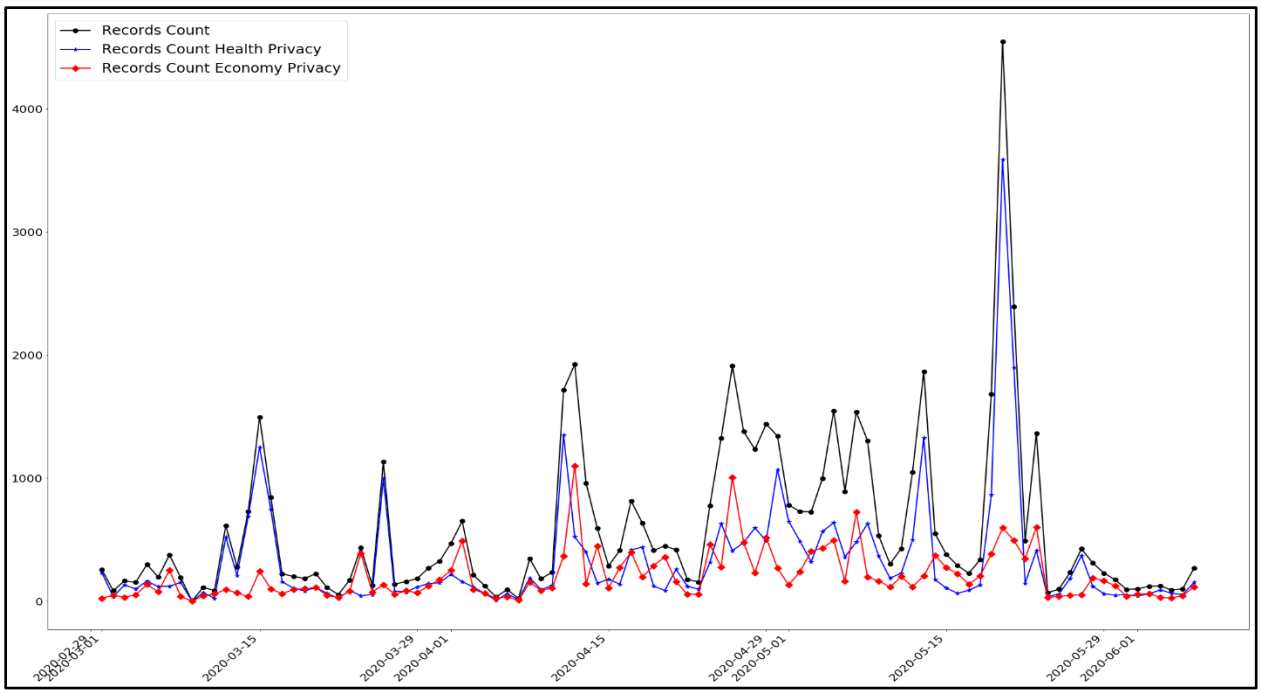

Figure 2. Diffusion of Privacy Tweets within Health vs. Economy Categories

The distribution of tweets count shows that the privacy concerns about health are greater in number than the economy-related concerns. To understand the underlying topics within the health and economy, we ran the LDA topic model using the privacy-related tweets. We measured the coherence score of the LDA model, assuming there is only one topic and continued this process until we reached ten topics. The coherence score was low for the LDA model with one topic, highest for a model with four topics, and then started declining. We selected the LDA model with four topics based on the best coherence score of 0.71. Based on the keywords generated for the four topics, we can see that the discussions are mainly about the patient health records, discussions about Chinese Government tracking patients through mobile apps, issues with some of the Chinese mobile apps, privacy could lead to domestic violence on vulnerable communities, and economic impacts due to the key user identifications landing into the wrong hands. We systematically analyzed the words under each topic and labeled them as "Patient Health Records," 'Chinese Digital Technology,' 'Address Confidentiality - Domestic Violence,' and 'Taxpayer Income - Hospital Patient Records.'

Figure 3 shows the line graph of tweets trends for each of these topics.

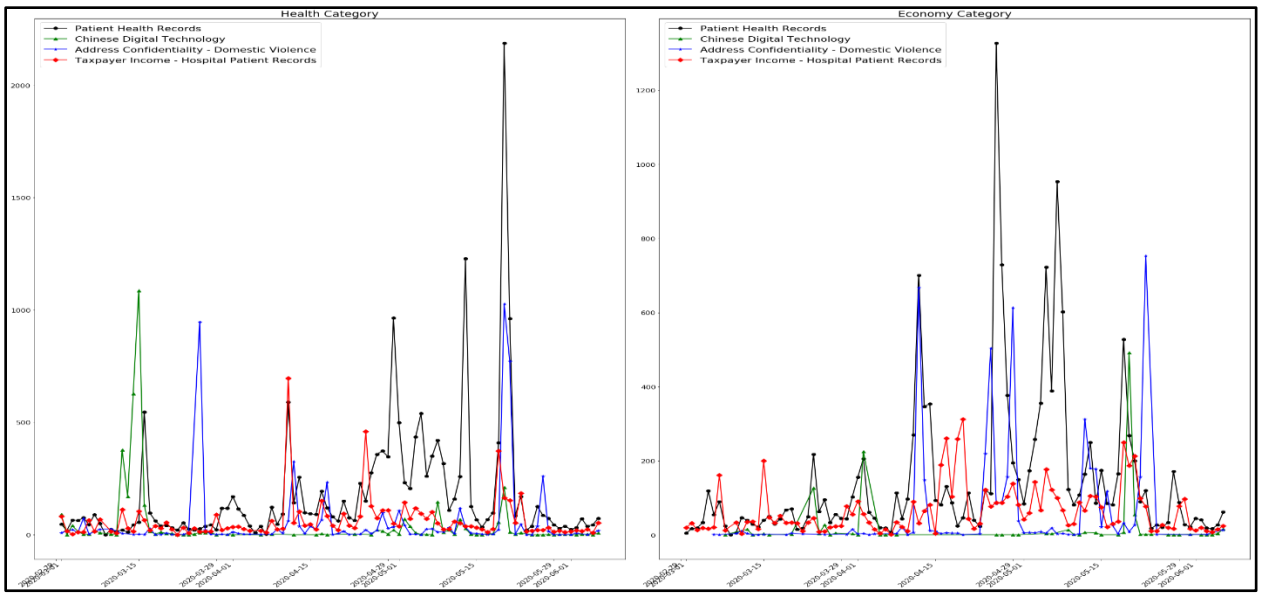

Figure 3. Diffusion of Privacy Tweets by Topics within Health and Economy categories

Most of the discussions are about "patient health records" topic, followed by "address confidentiality leading to domestic violence" topic. To gain further insights into key concerns across timelines, we ran a hierarchical clustering algorithm that clusters the tweets based on bi-grams (combination of two words). Bi-grams naturally cluster the co-occurring words together and provide an efficient cluster of sentences than the unigrams algorithm (Aiello et al., 2013). Specifically, we used DF-IDF (document frequency - inverse document frequency) approach rather than the regular TF-IDF technique (term frequency - inverse document frequency) which considers time dimension while extracting focal discussion (Aiello et al., 2013). A regular clustering algorithm based on the TF-IDF technique considers all these messages as a single large cluster and may ignore the emerging topics from new incoming messages (because the old, repetitive topics still carry a large weight), making it difficult to identify the development of new topics. Using the DF-IDF technique, lower priority is given to old tweets, and higher priority is given to newer tweets. We consider the last six weeks tweets as a six time intervals and when a new week data is captured, the earliest week's bi-grams are ignored in the similarity measure DF-IDF calculation. The inverse document frequency penalizes the document containing more number of same tweets, which indirectly extracts new information from the recent six weeks interval. Using this technique, we can extract the focal discussion within the tweets at each period.

We considered one week of tweets as a single corpus and incremented our corpus from the first week of March until June 6. In-total, we have 14 weeks of tweets. The hierarchical clustering algorithm ranks the tweets using the DF-IDF score and provides us the tweets in the reverse order of their scores as focal tweets. These focal tweets contain contextual information widely shared on Twitter during the interval we run the algorithm. Table 1 provides the top 3 focal privacy tweets discussed during each week of the outbreak.

Week	Tweets
Week1 (Mar 1st – 7th)	I strongly oppose any effort to slip controversial PATRIOT Act provisions into the coronavirus funding. This sort of backroom trick would jeopardize our public health response and stifle an important debate on Americans' constitutional right to privacy.
	CCHS is following state and federal medical privacy laws by not identifying facilities caring for patients with #coronavirus.
	FluffyPony on Encryption, Clearview and How Coronavirus Could Impact Privacy: The former lead maintainer of Monero and co-founder of Tari speaks about the state of global privacy

Week2 (Mar 8th – 14th)	Hey guys this is Froste. A few hours ago Classify was quarantined in a holding cell unable to contact anyone. To our dismay, it wasnt coronavirus that he was tested positive for but for the ability of being the baddest b*** on Twitter dot com. He asks you respect his privacy
	We continue to work w/ inter-agency partners to provide local ed leaders the resources needed to ensure health & safety of students/educators. @usedgov released new info today on K-12 flexibilities, student privacy, & educating students with disabilities: https://t.co/xNdRNscOrz https://t.co/w7HESwiZUi
	Coronavirus emails are the new "we've updated our privacy policy" emails.
Week3 (Mar 15th – 21st)	New: "We are at war." Governments are racing to track the coronavirus through phone location data, sparking privacy concerns. These are desperate times, but some fear the expanded surveillance will last long after the outbreak ends https://t.co/LxUIXcRVzs
	Coronavirus: They want to use your location data to fight pandemic. That's a big privacy issue https://t.co/fgw9p4qCtA
	Government efforts to track virus through phone location data complicated by privacy concerns https://t.co/n4b5pejmrM
Week4 (Mar 22nd – 28th)	Cellphone tracking could help stem the spread of coronavirus. Is privacy the price? https://t.co/LCjfv8MMPg
	And this is why I refuse to get one or anything like it: Coronavirus: Employees urged to turn off Alexa devices while working from home due to privacy fears https://t.co/UB40Yzak3I
	Kids' education data are far less protected than health data. As schools close over #COVID19, edtech adopted now may long outlast today's crisis. Here's why we need to protect kids and their privacy in online learning. https://t.co/KBucQGE0OY
Week5 (March 29 – April 4)	NASHVILLE, Tenn. – GRAMMY®-winning country music legend Joe Diffie passed away today, Sunday, March 29, from complications of coronavirus (COVID-19). His family respects their privacy at this time.
	We may now be in the midst of another seismic moment in the history of digital privacy: Mass surveillance methods could save lives around the world, but could it create a new civil liberties crisis? https://t.co/Olobs5lu9b https://t.co/tMLBkL3Nfb
	The founder of Zoom apologized for privacy feature flaws and so-called "Zoom-bombings" that have taken place as the video conferencing company's popularity has skyrocketed during the coronavirus crisis.
Week6 (Apr 5th – 11th)	Zoom, the video conferencing app that has exploded in popularity during the coronavirus crisis, has a large - but little discussed - research and development department in China. Some are raising questions over what this means for user privacy: https://t.co/E65cEnibir
	Reporters barred. Records delayed. How #coronavirus shrouded local Government in secrecy. #opengov #Journalism #StateFOI via @jessica_priest and @USATODAY https://t.co/fodJ2QFbgS
	Exclusive: First public map reveals military bases with coronavirus cases as Pentagon secrecy draws backlash https://t.co/aGEbr78aXV
	Apple & Google teaming up to trace everyone who could potentially have coronavirus is another science fiction plot made real. This is all "opt in" but how long does that last? What privacy looks like in post-pandemic world is unimaginable to me right now. https://t.co/cXCoKqorDW https://t.co/bz5iNKi3C8

Week7 (Apr 12th – 18th)	Palantir, the US big data firm founded by the rightwing billionaire Peter Thiel are processing large volumes of confidential UK patient information in a data-mining operation that is part of the Government's response to the #CoronavirusPandemic. #COVID19 https://t.co/PSvydwoHg2 https://t.co/VpeLdDibbA
	From my #Open list: UK government using confidential patient data in coronavirus response | World news | The Guardian https://t.co/8MClAkKPlD, see more https://t.co/YOW49pSN57
	The story of the supply-chain group, a power center within the larger task force run by VP Pence, is one of chaos, secrecy and ineptitude, some officials say.
Week8 (Apr 19th – 25th)	This is Iran where authorities raid your home, disturb your privacy, & give you 80 lashes for drinking alcohol. I received this video from a mother whose son was lashed. Meanwhile, officials like @JZarif still claim Government doesn't interfere in people's private lives.
	Ministers warned last year UK must have a robust plan to deal with pandemic virus and its potentially catastrophic social and economic consequences in a confidential Cabinet Office briefing leaked to the Guardian https://t.co/CPyqOOVXUi
	Not to be missed also tonight, big scoop from @nickhopkinsnews. Leaked confidential Cabinet Office briefing warned last year the UK must have a robust plan to deal with a pandemic virus and its potentially catastrophic social and economic consequences. https://t.co/7ZE4eqz2dK
Week9 (April 26 – May 2)	Despite privacy concerns, the COVIDSafe app -- designed to help health authorities trace people who may have come into contact with someone who has Covid-19 -- has been downloaded more than 2 million times https://t.co/WIreYoDPLE
	Covid safe: Australian Government launches coronavirus tracing app. The scramble for contact tracing apps is on despite privacy concerns and the lack of evidence they could be effective without mass testing and most of the population downloading them (when a single digit percentage seems likely to do so). https://t.co/LF58qi9t17
	I got a look at a version of the HSE's Covid-19 tracker app - which is in the final stages of testing. It will collect information about people's health and require them to share their location despite privacy concerns. https://t.co/9Z5zOh8IPq via @businessposthq
Week10 (May 3rd – 9th)	Israel #COVID19 surveillance programme was considered a severe violation of the right to privacy by the High Court. Here is why governments need to think twice before taking similar measures: https://t.co/cRituvEyBh https://t.co/BCBGpxIxkO
	@afuahirsch says the Government must give more assurances on privacy and data protection if they more people to use the NHS coronavirus app #bbcqt
	Breaking: The NHS contact tracing app must not be released in its current form without increased privacy and data protections, parliament's human rights committee has said. It is calling for a new law on data gathering and an independent regulator
Week11 (May 10th – 16th)	Asked about BBC Scotland Disclosure's programme, which revealed an outbreak of #coronavirus at a Nike conference in Edinburgh in February, the first minster said the public were not informed and one of the reasons was patient confidentiality.
	U.S. Employers Rush to Adopt Virus Screening. The Tools May Not Help Much. Symptom-checking apps and fever-screening cameras promise to keep sick workers at home and hinder the virus. But experts warn they can be inaccurate and violate privacy.
	Yet another Telegraph scoop as it gets its hands on a confidential Treasury assessment of how we can pay for the black coronavirus hole in our economic lungs. Grim reading, paywalled so here's a copy: https://t.co/Aknqhgq3pv

Week12 (May 17th – 23rd)	After installing iOS 13.5 update, head to Settings & Privacy & Health Turn on/off COVID-19 Exposure Logging as per your convenience. #ios135 #iOS https://t.co/aeTXrlmDQy
	Dr Tony Holohan said reports that employers had received their employees Covid-19 test results first was "a breach of confidentiality full stop." @rtenews
	Citing "patient confidentiality" in order to dodge scrutiny just won't wash @NicolaSturgeon @JeaneF1MSP @scotgov. Not a chance. EXCLUSIVE: Scottish Government has no record of how many people have been contact traced for … https://t.co/ebcaaPF29D via @pressjournal
Week13 (May 24th – 30th)	China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears https://t.co/FqI7VhyY8p… https://t.co/71qVm4FZkM
	Just listened to @MattHancock solemnly telling us all to perform our 'civic duty' re Test & Trace. And then telling us, again, that Dominic Cummings abided by the guidance when he broke at least three lockdown rules. The Health Secretary has lost all credibility. Privacy Matters
	The @MIT again downgrades #AarogyaSetuApp: for purposes of contact tracing, the app is collecting more data than it needs to. Serious #privacy concerns here.
Week14 (May 31 – June 6)	Pakistan's Government is employing invasive #surveillance technology that can seriously infringe people's right to privacy once the pandemic is over. Pay attention now.
	The right to know? Balancing health risks and privacy rights for landlords during COVID-19 https://t.co/jNahL5QrDP
	Republicans and Democrats Introduce Competing Privacy Bills to Protect Consumers' Health Information Related to the COVID-19 Pandemic https://t.co/zcQAmsHixK

Table 1. Focus Tweets about Privacy Concerns

Table 1 provides support for our interpretation of graphs and shows the hierarchy of privacy-related discussions that are rampant across both the health and economy categories. We lead into the debate around the privacy concerns of users in the following section.

Discussion

Lives vs. Livelihood (Health vs. Economy)

From following our topic modeling and hierarchical clustering approach, we were able to analyze tweets that are representative of the users' privacy concerns related to the proper protection of their health-related information during this pandemic. Users on Twitter are majorly concerned about their ability to live their lives without compromising on their private information, while still getting the best care in the most secure manner and maintaining their right to privacy. Apart from health-related privacy concerns, users online also engaged in a spirited discussion regarding the protection of their privacy in economic settings. They vented out their privacy concerns regarding the implications of being tested positive and what the disclosure of such private information, collected by mobile apps for surveillance, could harm their ability to obtain and maintain gainful employment in the economy. Based on our analysis of the tweets, we found that a majority of the online populace is concerned more about health-related privacy concerns rather than the economy-related privacy concerns. Interestingly this insight validates and follows Maslow's hierarchy of needs theory (Maslow, 1958). People are inherently more concerned about their safety, security and well being. As is mentioned in the theory, a person first seeks to fulfill their lower order needs (safety/security – health) before moving on to fulfill their higher order needs (esteem/belongingness – economy). A clearer understanding of human needs also has critical implications for defining future COVID-19 response and recovery strategies (Ryan et al, 2020).

We also saw comparable levels of health-related and health-privacy related concerns with user sentiment in both these conversations mimicking each other to show that users are equally concerned about their health as well as the protection of their personal information that is uniquely attached to their health records.

The health vs. economy debate has primarily been a debate about saving human lives versus saving the jobs that those humans perform to earn their livelihoods – lives vs. livelihood. Even the media is divided in proclaiming a clear winner for this debate. Though there has been a clear consensus about which among the two comes first – lives. For any kind of long term economic recovery to take place, it is imperative that first, the virus is dealt with swiftly and surely (The Hill, 2020, May 13). At the same time, there have been efforts, particularly by the local governments, to do away with lockdown and reopen the economy at the earliest, even if that means putting people in immediate danger of contracting the virus (Columbia Business School, 2020, May 11). The most sensible reports suggest that a middle path is the best way forward in times of this pandemic. The hard choice of selecting an alternative between the lives vs. livelihood quandary is not necessary. We, as a society, along with our governments, agencies, and nations, can come together to 'timebox' this Covid-19 pandemic (McKinsey, 2020, March 23). We need to be decisive in our response to this lives vs. livelihood debate by thinking about ways to suppress the virus and, at the same time, shorten the duration of the economic shock associated with this virus. This is inherently true for other societal crises like hurricanes and other natural disasters. The process of disaster recovery and rehabilitation is laced with similar concerns regarding the lack of proper privacy protections for the affected persons (Herold, 2006). The insights from our work can be generalized to represent the genuine concerns of people who are unfortunate enough to be affected by such societal crises. Privacy should thus be treated as an inalienable right even in times of emergencies.

In our corpus of tweets, we found conversations that were strikingly similar to this debate on lives vs. livelihood that is currently trending all over the world. Users that shared health-related privacy concerns were fearful of their health information being collected by mobile apps even when they do not explicitly want to reveal it (Week 9). Another health privacy concern was raised by a user where the UK Government was using large amounts of confidential Covid-19 patient data inappropriately (Week 7). As for economy-related privacy concerns, a user tweeted about their concern of being evicted from their apartment if the landlord came to know that they tested positive (Week 14). Other similar concerns included users' fear about the implications of testing positive can have on their livelihood. General fears of users related to topics such as fear of getting laid off, or not finding jobs and being ostracized in economic pursuits, or sharing too much information with apps that may be used to monitor users well after the pandemic is over (Week 13).

Contributions

By addressing a central moral conflict in the midst of a pandemic, we highlight the importance of privacy in the lives of the people as well as in their livelihoods. We present a mapping of health and economy-related privacy concerns of the public and bring to light their apprehensions about official responses to the pandemic.

In terms of theoretical contributions, this paper stresses the need to consider user sentiment and its sustained importance whence forming guidelines, designing protective measures, and establishing a response mechanism to fight pandemics. In times of crisis, privacy might not be a central focus for the authorities, but from our analysis of Twitter users, it most certainly is an emotional issue for the community. The right to privacy is even enshrined in the constitution, and users do not want to compromise it for a sure pandemic or not. Therefore privacy during times of crises such as pandemics is an essential avenue for future research in the domain of user privacy.

In terms of practical implications from this paper, official agencies can use the insights outlined here to focus on alleviating the privacy concerns of individuals in society. For ensuring the success of any response measures against battling the novel coronavirus, the participation of the people is paramount. It is then sensible to install measures that satisfy the basic tenets of confidentiality set forth in the right to privacy so as to ensure users' privacy is protected, and people are assured of the sanctity of their health information in both the health and economy-related contexts. This research can also help to drive official campaigns that target the need for community participation in handling crisis situations.

Future Work

This paper has been an exploration of Twitter data about users' sentiment and their privacy concerns in a crisis situation. We plan to extend this work into a drawn-out investigation of the privacy needs of users during pandemics. With respect to these user needs, we plan to investigate other similar issues around the domain of privacy and security of user data that is collected to map out the spread of pathogenic viruses. In our future efforts, we will also study the impact of privacy breaches on the population when their confidential data is used to drive a global response but without explicit user consent on data sharing. For other researchers in this domain, we present them with a few challenges regarding how to ensure privacy is maintained during times of a global emergency and how to sustain this privacy even when everything goes back to normal.

REFERENCES

Adam, N. R., Shafiq, B., & Staffin, R. (2012). Spatial computing and social media in the context of disaster management. *IEEE Intelligent Systems, 27*(6), 90-96.

Aiello, L. M., Petkos, G., Martin, C., Corney, D., Papadopoulos, S., Skraba, R., Göker, A., Kompatsiaris, I. & Jaimes, A. 2013. Sensing trending topics in Twitter. IEEE Transactions on Multimedia, 15, 1268-1282.

Aivazpour, Z., & Rao, V. S. (2019, January). Impulsivity and Information Disclosure: Implications for Privacy Paradox. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

Ashktorab, Z., Brown, C., Nandi, M., & Culotta, A. (2014). *Tweedr: Mining twitter to inform disaster response*. Paper presented at the ISCRAM.

Blei, D. M. (2012). Probabilistic topic models. *Communications of the ACM, 55*(4), 77-84.

Chatfield, A., & Brajawidagda, U. (2012). *Twitter tsunami early warning network: a social network analysis of Twitter information flows*. Paper presented at the 23rd Australasian conference on information systems, Geelong, Australia.

Chen, K. (2017). No place to hide: Edward Snowden, the NSA, and the US surveillance state: Taylor & Francis.

Columbia Business School. (2020, May 11). Saving Lives versus Saving Livelihoods: Can Big Data Solve the Pandemic Dilemma? Retrieved from https://www8.gsb.columbia.edu/newsroom/newsn/9005/saving-lives-versus-saving-livelihoods-can-big-data-solve-the-pandemic-dilemma Accessed on 2020, June 30

Herold, R. (2006). Addressing privacy issues during disaster recovery. Information Security Journal, 14(6), 16.

HHS.gov. (2020, April 9). OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency. Retrieved from https://www.hhs.gov/about/news/2020/04/09/ocr-announces-notification-enforcement-discretion-community-based-testing-sites-during-covid-19.html Accessed on 2020, June 30

Hiller, J. S., & Russell, R. S. (2017). Privacy in crises: The NIST privacy framework. *Journal of Contingencies and Crisis Management, 25*(1), 31-38.

Househ, M. (2012, February). Re-examining Perceptions on Healthcare Privacy-Moving from a Punitive Model to an Awareness Model. In International Conference on Health Informatics (Vol. 2, pp. 287-291). SciTePress.

kcrg.org. (2020, March 3). HIPAA overused to hide key COVID-19 data, Iowa journalism group claims. Retrieved from https://www.kcrg.com/content/news/HIPPA-overused-to-hide-key-COVID-19-data-Iowa-journalism-group-claims-569450781.html Accessed on 2020, June 30

Levine, M. L. (1988). Contact tracing for HIV infection: a plea for privacy. *Colum. Hum. Rts. L. Rev., 20*, 157.

Maslow, A. H. 1943. "A Theory of Human Motivation." Psychological Review 50 (4): 370–96.

McKinsey (2020, March 23). Safeguarding our lives and our livelihoods: The imperative of our time. Retrieved from https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/safeguarding-our-lives-and-our-livelihoods-the-imperative-of-our-time# Accessed on 2020, June 30

Mercer. (2020, April 06). COVID-19 raises HIPAA privacy, security issues. Retrieved from https://www.mercer.com/our-thinking/law-and-policy-group/covid-19-raises-hipaa-privacy-security-issues.html Accessed on 2020, June 30

Modern Healthcare. (2020, April 29). Medicare applications raise anxiety for seniors in pandemic. Retrieved from https://www.modernhealthcare.com/medicare/medicare-applications-raise-anxiety-seniors-pandemic Accessed on 2020, June 30

Oh, O., Agrawal, M., & Rao, H. R. (2011). Information control and terrorism: Tracking the Mumbai terrorist attack through twitter. *Information Systems Frontiers, 13*(1), 33-43.

Palen, L., Anderson, K. M., Mark, G., Martin, J., Sicker, D., Palmer, M., & Grunwald, D. (2010). A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters. *ACM-BCS Visions of Computer Science 2010*, 1-12.

Rao, H. R., Vemprala, N., Akello, P., & Valecha, R. (2020). Retweets of officials' alarming vs reassuring messages during the COVID-19 pandemic: Implications for crisis management. *International Journal of Information Management*, 102187.

Ryan, B. J., Coppola, D., Canyon, D. V., Brickhouse, M., & Swienton, R. (2020). COVID-19 Community Stabilization and Sustainability Framework: An Integration of the Maslow Hierarchy of Needs and Social Determinants of Health. Disaster medicine and public health preparedness, 1-7.

TechRepublic. (2018, June 20). Do remote workers increase your chance of a data breach? 86% of CXOs say yes. Retrieved from https://www.techrepublic.com/article/do-remote-workers-increase-your-chance-of-a-data-breach-86-of-cxos-say-yes/ Accessed on 2020, June 30

The Hill. (2020, May 13). 'Lives or livelihoods' misses the point of pandemic recovery. Retrieved from https://thehill.com/opinion/finance/497481-lives-or-livelihoods-misses-the-point-of-pandemic-recovery Accessed on 2020, June 30

The National Law Review. (2020, March 12). Privacy, HIPAA, Security and GDPR– COVID-19 Considerations. Retrieved from https://www.natlawreview.com/article/privacy-hipaa-security-and-gdpr-covid-19-considerations Accessed on 2020, June 30