Towards Understanding Privacy Trade-off In An Epidemic*

Sajedul Talukder
Department of Mathematics and Computer Science
Edinboro University
Edinboro, PA 16444
stalukder@edinboro.edu

Abstract

Although the COVID-19 is still as complicated as ever, it is an significant job for private networks across the globe to gather and share data in the light of the battle against coronavirus. The scale and severity of the disease are not rare, but they seem to be near it. Consequently, drastic steps to remedy the situation seem to be the rule in a very short period of time. These acts in particular impact the privacy of individuals. In certain cases, the whole population has been intensively monitored and diagnostic records from those who are infected with the virus are usually distributed around organizations and nations. While in many countries innovative approaches have been introduced to counter this, privacy advocates are concerned that technology would eventually erode privacy, while regulators and supporters are concerned about the type of effect that this may have. The content of this problem shows that the best way is to strike the right balance. The cases related to the ability of public authorities to intervene with the fundamental right to privacy in the interests of national security or public safety have consistently shown the prospect of achieving a fair balance.

1 Introduction

The spike in coronavirus cases in the USA and around the world has contributed to countries being practically halted as policymakers are urging people to stay indoors, even using coercion. [3]. The spread of viruses has influenced daily life, from social networks [13, 1, 12, 5, 18] to e-governance [7, 9], from digital automation [6, 15] and cyber security [2, 16] to cellular networks [4]. Many high-tech strategies to help humans fight the virus are brought together during the global coronavirus outbreak. Unless we had no access to advanced technologies, it would not have been possible to isolate us from society. Content for hundreds of millions of users has been generated by digital media outlets, vast numbers have begun telecommuting schools and jobs and the usage of surveillance tools has expanded significantly, as millions more people are treated with telehealth apps, the last thing policymakers worldwide anticipated to see citizens with very contagious symptoms.

The use of these systems does, however, often raise some concerns about privacy. As the coronavirus pandemic spread across the world, countries developed massively controlled networks to track virus transmission and forced governments all over the world to take into account trade in health and protection for millions of people. South Korean government agencies are using camera tracking, smartphone location data and credit card payment records to track recent patient movements of coronavirus and establish transmission chains. App promising for COVID-19 recovery, Iran released. Most of what it is doing today is gathering information from million people and essentially supplying the government with real-time monitoring. U.S. federal health officials plan to track viral dissemination-a practice known as "syndronic surveillance" -using encrypted, consolidated customer data from Internet providers to avoid further outbreoks. Many reports, however, have warned that the government access to confidential location information may now lead to the reduction of the degree of privacy, especially if government start demanding unanonymized information.

Asia is seeing more and more the data security implications of attempts to control the spread of coronavirus. When this economic crisis is completely under control, China can be commended for its technological achievement in avoiding an outbreak that could have infected billions. However, it definitely comes at a cost. Definitions of "epidemic maps" indicate the precise location of confirmed and suspected cases in real time so that people can stop and visit the same place. There is also an app that helps people to interact, whether on trains or flights, with someone who contracted the virus. These interventions are also successful, but involve a large amount of medical data processing and distribution. Similarly, Korea and Singapore have adopted innovative solutions to tackle the problem, which seem to have been successful, in response to the

wide-ranging and obvious intrusions to privacy.

The right to privacy is not an absolute right anywhere in the world. Privacy and data protection regulations can not and should not threaten a common-sense life-saving solution. All these systems therefore allow data to be used and shared for that purpose, if applicable. At the same time, the conditions laid down in the law can not be overlooked, except in times of crisis. Disproportionate decisions and actions are always the result of knee-jerk reactions and when it occurs internationally everyone is at risk, no matter how often they have washed their hands.

Our Contributions: The following contributions are presented in this article:

- **Study privacy issues**. This paper presents the first systematic study on different data security problems at different fronts during the pandemic. It is the first systematic study to tackle privacy issues from all fields, from surveillance to medical data, to our best knowledge.
- **Recommend privacy principles**. This paper offers multiple privacy strategies, including privacy protection measures, aggregated anonymized data and collaborative data for software and device designers.

The rest of the paper is organized as follows. Section II describes the privacy issues. Section III describes the recommended privacy principles. Finally, Section IV concludes the paper with a highlight on the scope of future work.

2 Privacy Issues

2.1 Privacy of Surveillance Data

When South Korea fights a snowball number of incidents involving COVID-19, the government let people know whether they are in the patient area. But the volume of data has led to certain distressing moments and fears about social stigma are as high as the fear of disease. The German Robert Koch Institute (Covid-19) was giving 5 GB of consumer data to combat coronaviral transmission by Deutsche Telekom, Europe's biggest telco firm. The Institute will use the anonymized data to track the general public 's behaviors to forecast the spread of the virus and to raise concerns about the efficacy of social distance. Likewise, Vodafone published a five-point plan to support the transfer to Lombardy, Italy of private customer data. Also contributions were made by the Austrian largest telco, A1. There are concerns that in many countries mobile technology is used more authoritarianly already. These data are used in China, Israel and South Korea for monitoring and enforcement of quarantine contacts

between infected locals. Critics also challenge the legitimacy of the donations and the protection of customers' privacy-and whether it would be beneficial to donate data. Whilst the GPS data can be very reliable, the tracking data of mobile telephones can be used to track clients [14].

Much of the information relates to the mobility data that could be compounded by the lack of openness in telecommunications companies which have long collected and sold their clients' geolocation data [11, 10]. In the USA, the government has talks currently about how their consumer data can be used to discourage COVID-19 distribution through internet companies such as Google, Apple and Facebook. A medical school in Hanover, Germany is developing an app that allows individualized monitoring of infections with local mapping companies Ubilabs. A COVID-19 positive test individual willingly supply GPS data [8] on his phone with the GeoHealth software, which is supposed to be available within a few weeks. The Spanish Government has recently released its own app, called STOP COVID19 CAT. Anonymous data can also be easily re-identified, which, they say, increases fear in these situations. This was a major obstacle to use of data, as occurred during Ebola, in the past and the absence of a program.

However, the good news is that global data protection organizations provide their guidance and recommendations on data management activities and on coronavirus regulation. A reasonable middle ground would be the best solution, so as not to neglect the implementation of fundamental privacy standards.

2.2 Privacy of Medical Data

The outbreak of coronavirus pushes the US Government to amend one of its few data privacy rules. The Act on the Portability of Health Insurance and Accountability is one of the safeguards against abuse of medical data, but the Administration for Health and Human Services has clarified that the penalties for alleged HIPAA violations are suspended. Protected health care providers covered by the HIPAA Regulations will attempt to link to patients through remote communication systems and provide telehealth services. Nearly all video messaging services meet the criteria of HIPAA and advanced applications like Zoom for Healthcare and Skype for Business [17]. But with COVID-19 threats to spread exponentially, HHS decided to open more common video chat applications for physicians, with governments suggesting that people stay at home for control of the epidemic. This includes well-known FaceTime, Google Hangouts, Skype applications, and Facebook Messenger. The HHS Civil Rights Office has clarified that it will not place limits on healthcare providers with these incompatible video messaging systems. Another issue is that HIPAA-covered staff would be able to share knowledge about their workplace in an outbreak of infectious disease such as COVID-19.

2.3 Privacy of Tech Company Data

Tech companies offered their services, support and face mask shackles following the outbreak of the coronavirus pandemic. Many companies which work with the data now develop their data collection tools to attempt to monitor or avoid the spread of the virus. A data company called the Social Distance Scoreboard [19], Unacast, which collects and provides data on the cell phone location and analysis for retail, real estate, marketing and tourism industries. The scoreboard is an interactive map, which gives each state and country in America letter scores based on how much the citizens separate themselves from others. Facebook's Data for Good platform uses de-identified statistical data from its users to endorse Disease Prevention Charts, which can help health officials track and predict disease transmission or where to go next. It provides details on where people live and where they move. Kinsa Health utilizes data from its smart thermometers to attempt with its U.S. Health Climate Monitor to identify extremely high influenza rates, which it claims had correctly forecast the spread of flu in the past and could also map outbreaks of coronavirus. The stumbling block is that users are able to access the location data without realizing these applications. There is no easy way for the average user to see what SDKs an app may use as the App's privacy rules typically suggest the specifics are given by third parties without disclosing who those parties are. Unacast says that its SDK is its "preferred" website database, but that the Company would not identify applications or partners with which it works if it was asked for clarification. Typically speaking it is not possible to use the privacy safeguards that the consumers have as the majority of them do not even know that data collection systems, such as Unacast, do not have federal laws that prevent such processing.

2.4 Privacy of Student Data

FERPA is a federal statute that preserves the privacy of student education data. FERPA forbids the removal of PI I from the academic record of kids without prior notice, without exception to the general agreement clause, to government (e.g. school districts) and organizations (e.g. schools). (20 U.S.C. (2232 g; 34 C.F.R. Section 99) For instance, under a "health or safety emergency" exception, educational institutions and universities can, without prior written authorization, submit PIIs from student training records to an emergency department, if the public health authority discloses such details in full. Unless the deletion of the entire PII is permitted by the organization or institutions, FERPA requires that schools and organizations disclose information on educational documents without permission, provided that a fair decision was reached that the name of the student could not be identified in

public, whether in single or multiple releases. It would also be troublesome for students to complain that a specific class or category is absent as a result because, for example, the names of each student in that class or grade are included in the list. There have been several documented attacks and individual data from anonymous data collection can be de-anonymized. This is also possible to inform through the school on the need for COVID 19 for parents of other school children within the community to a particular pupil, teacher, or other school official.

3 Privacy Principles Recommendation

During the spread of an outbreak, the conflict between the security of human rights and the acquisition of information that is essential to the general interest differ. Core specifics should be sorted by device designer supervision: how to evaluate telephone closeness and user security, where the information is processed, who uses it and in what format. Currently, digital contact tracing services work in a range of countries, but there are scant specifics and privacy questions.

Several new projects aim to establish cooperative, data protection-conscious telephone control mechanisms. A prototype of a private kit app was developed by a team of the Massachusetts Institute of Technology. The application stores up to 28 days of user-supplied GPS location data logged every 5 minutes. If you perform positive coronavirus tests, you should share your current data with health authorities to identify and publicize places that might have been at risk for others. In countries where data security laws are strict, it is possible to share sensitive, aggregated information that they have already obtained by telephone and other software providers. Unfortunately, the data will reveal general trends of where and when people interact and avoid the spread of infection when individual users are unknown. The sharing of anonymized location information with the US Government is also debated between Google and Facebook.

One option is to use a coronavirus-specific application to start new applications, which will require users to freely share location and health information. A new application in Germany relies partly on location data for its account holders already held by Google. Anyone who does good can use the GeoHealth app to donate their place 's history. The data is then stored anonymously on a central server. Fortunately, the organization also employs advanced PET cryptographic methods. This has been rigorously investigated and tested by the global scientific community, and business leaders make a concerted effort to standardize PETs, such as ZKProof, to encourage broader adoption. If applied correctly, PET would be more encouraging than restricting businesses. This will help them reliably exploit and stay competitive with data from third

parties without violating consumer privacy or confidentiality.

4 Conclusion

It will be important to protect privacy in designing and implementing these techniques. To order to step forward together to this next process, monitoring and testing, and using similar techniques built to cope with the pandemic, it is more important than ever to understand the concept of privacy. The explanation why it collects data, what data is collected and how long they are kept must be accessed through transparency. This should also ensure that the user understands the purpose of data collection, the nature of the data to be collected, the time spent retaining data, and the benefits of collecting data.

References

[1] Ali Ahani and Mehrbakhsh Nilashi. Coronavirus outbreak and its impacts on global economy: the role of social network sites. *Journal of Soft Computing and Decision Support Systems*, 7(2):19–22, 2020.

[2] Tabrez Ahmad. Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *Available at SSRN 3568830*, 2020.

[3] Nuno Fernandes. Economic effects of coronavirus outbreak (covid-19) on the world economy. *Available at SSRN 3557504*, 2020.

[4] Martín Lajous, Leon Danon, Ruy López-Ridaura, Christina M Astley, Joel C Miller, Scott F Dowell, Justin J O'Hagan, Edward Goldstein, and Marc Lipsitch. Mobile messaging as surveillance tool during pandemic (h1n1) 2009, mexico. *Emerging infectious diseases*, 16(9):1488, 2010.

[5] Raina M Merchant and Nicole Lurie. Social media and emergency preparedness in response to novel coronavirus. *Jama*, 2020.

[6] Kenneth Okereafor and Olajide Adebola. Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. *Journal Homepage: http://ijmr. net. in*, 8(2), 2020.

[7] Syed Sharfuddin. The world after covid-19. *The Round Table*, 109(3):247–257, 2020.

[8] S. K. Talukder, M. I. Islam Sakib, and M. M. Rahman. Digital land management system: A new initiative for bangladesh. In *2014 International Conference on Electrical Engineering and Information Communication Technology*, pages 1–6, April 2014.

[9] S. K. Talukder, M. I. Islam Sakib, and M. M. Rahman. Model for e-government in bangladesh: A unique id based approach. In *2014 International Conference on Informatics, Electronics Vision (ICIEV)*, pages 1–6, May 2014.

[10] Sajedul Talukder. Abusniff: An automated social network abuse detection system. *J. Comput. Sci. Coll.*, 35(3):209–210, October 2019.

[11] Sajedul Talukder and Bogdan Carbunar. When friend becomes abuser: Evidence of friend abuse in facebook. In *Proceedings of the 9th ACM Conference on Web Science*, WebSci '17, New York, NY, USA, June 2017. ACM.

[12] Sajedul Talukder and Bogdan Carbunar. Abusniff: Automatic detection and defenses against abusive facebook friends. In *Twelfth International AAAI Conference on Web and Social Media*, 2018.

[13] Sajedul Talukder and Bogdan Carbunar. A study of friend abuse perception in facebook. *Transactions on Social Computing*, 1(1), 2020.

[14] Sajedul Talukder, Iftekharul Islam Sakib, Faruk Hossen, Zahidur Rahim Talukder, and Shohrab Hossain. Attacks and defenses in mobile ip: Modeling with stochastic game petri net. In *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, pages 18–23, 2017.

[15] Sajedul Talukder, Md Iftekharul Islam Sakib, Zahidur Rahim Talukder, Upoma Das, Arnob Saha, and Nur Sultan Nazar Bayev. Usensewer: Ultrasonic sensor and gsm-arduino based automated sewerage management. In *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, pages 12–17. IEEE, 2017.

[16] Sajedul Talukder and Zahidur Talukder. A survey on malware detection and analysis tools. *International Journal of Network Security & Its Applications*, 12(2), 2020.

[17] Sajedul Talukder, Shalisha Witherspoon, Kanishk Srivastava, and Ryan Thompson. Mobile technology in healthcare environment: Security vulnerabilities and countermeasures. *arXiv:1807.11086*, 2018.

[18] Sajedul Karim Talukder. Detection and prevention of abuse in online social networks. *FIU Electronic Theses and Dissertations. 4026*, 2019.

[19] Unacast. Social distancing scoreboard. Unacast, `shorturl.at/gs068`, 2020.