Pandemic Surveillance

Nearly half of American adults have had at least one COVID-19 vaccination. But how many people are aware of the fact that data collected by contact-tracing apps is still floating around? Now, the United States is faced with a potential privacy crisis: Who has the power to decide which entities have access to the sensitive data collected by contact-tracing apps, and how will that data be stored, used, or possibly abused?

Many people may not believe contact-tracing app data privacy laws are warranted; After all, less than 10% of Americans in most states even report using contact-tracing apps. Although low adoption of these apps may suggest that few people will be harmed by the potential misuse of data, what may seem like microscopic impacts actually have implications on a macroscopic scale for data privacy.

Current U.S. privacy laws do not apply to contact-tracing app data. HIPAA only protects medical information that health care providers, like doctors or hospitals, collect. Even if HIPAA did apply, the U.S. Department of Health and Human Services suspended most penalties during the pandemic to facilitate contact-tracing efforts.

The Federal Trade Commission Act of 1914 (FTC Act) does not adequately protect contact-tracing app user data either, despite its broad premise. Companies can still decide which privacy protections they choose to enforce as long as they avoid deception and injury. With so much room for interpretation, corporations who have collected contact-tracing data essentially have private ownership of the data, provided that the company informed their users about the privacy protections – or the lack thereof – that they are offered.

Evidently, our privacy laws are not up to date; No system is in place to properly protect the sensitive information gathered by contact-tracing applications. Clearly articulated privacy laws concerning contact-tracing app data must be enacted because current U.S. privacy laws do not sufficiently protect the privacy and data of contact-tracing app users.

Abuse of contact-tracing app data is already a tangible reality in other countries. The malicious use of personal data collected by contact-tracing apps is particularly worrying in the United Kingdom, for example. Rights groups have pointed out users' inability to delete personal data or determine how sensitive information may be used from the contact-tracing app developed by NHS X.

In addition, the British "government plans to retain the data it collects for up to 20 years," said experts Kristine Eck and Sophia Hatz. "The government has failed to conduct a legally mandated data protection impact assessment."

Like the NHS X project in the United Kingdom, Singapore also adopted its own contact-tracing app called TraceTogether that boasted an FAQ internet page to address questions users may have about the way the app collects information.

Despite the openness of the TraceTogether app, "the notions of privacy and openness enacted in the app remained very limited," revealed professors Hallam Stevens and Monamie Haines. "In the context of the app, privacy, for example, meant only locational privacy." Once activated, the government can force users to give the government the data collected by TraceTogether.

The United States needs to adopt clear privacy policies for contact-tracing application data to prevent the potential abuse of the personal data about location and health status that has already been seen in other countries.

The consequences of a nation without contact-tracing app data privacy laws extend far beyond the near future: Failure to enact privacy laws surrounding contact-tracing apps now prevents the success of contact-tracing apps in the future. Without a clear structure of privacy protection, many Americans were unwilling to use contact-tracing applications during the COVID-19 pandemic – and without enough contact-tracing app users, contact-tracing applications fail to slow the spread of disease.

The root of the public's refusal to widely adopt such applications lies in the lack of contact-tracing app data privacy laws. In a 2020 study, researchers concluded that privacy-preserving technology with public education is necessary for digital contact-tracing apps to become effective in the United States. Additionally, privacy laws concerning contact-tracing app data must be addressed now – research has found that Americans are less willing to download and use a contact-tracing app when disease concerns are high, meaning the United States must take proactive measures now instead of reactionary measures later. The absence of a precedent concerning data privacy laws for contact-tracing apps will ultimately lead to their failure in the next public health crisis.

Without proper protection, U.S. citizens face the potential abuse or exploitation of the data they have already given up in an effort to protect public health safety during the COVID-19 pandemic and the loss of an extremely valuable tool in the next public health crisis.

With such little legal protection in the U.S. for data privacy to begin with, how can we start creating policies to protect contact-tracing app data? To answer that question, Senator Gillibrand has recently introduced the Data Protection Act of 2020 bill that would give the United States its own Data Protection Agency, protecting the privacy of Americans with the authority to administer data practices. As citizens, we have the responsibility to fight for the data privacy

rights we want – and we can do it by calling our representatives and urging them to vote in favor of Senator Gillibrand's proposed bill.

Bibliography

CDC. (2020, March 28). *COVID Data Tracker*. Centers for Disease Control and Prevention. https://covid.cdc.gov/covid-data-tracker

Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior*, *119*, 106718. https://doi.org/10.1016/j.chb.2021.106718

Eck, K., & Hatz, S. (2020). State surveillance and the COVID-19 crisis. *Journal of Human Rights*, *19*(5), 603–612. https://doi.org/10.1080/14754835.2020.1816163

Gillibrand, K. E. (2020, February 13). *Text - S.3300 - 116th Congress (2019-2020): Data Protection Act of 2020* (2019/2020) [Legislation]. https://www.congress.gov/bill/116th-congress/senate-bill/3300/text

Why Aren't Contact Tracing Apps Working? (n.d.). Time. Retrieved May 14, 2021, from https://time.com/5905772/covid-19-contact-tracing-apps/

Zhang, B., Kreps, S., McMurry, N., & McCain, R. M. (2020). Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. *PLoS ONE*, *15*(12), 1–16. https://doi.org/10.1371/journal.pone.0242652