Disaster apps share personal data in violation of their privacy policies

17 November 2020, by Jodi Heckel

Credit: Pixabay/CC0 Public Domain

Those in the path of a hurricane or wildfire may use an app to get alerts, communicate with first responders or let loved ones know they are safe. But once the emergency has passed, those apps may still be tracking their location or making personal information available to third parties.

Madelyn Sanfilippo is a professor in the School of Information Sciences at the University of Illinois at Urbana-Champaign whose research explores the interactions between people and technology, and the governance, personalization, privacy and social justice issues related to technology. Sanfilippo and a team of experts tracked the personal data sent by popular disaster apps and examined whether those practices conformed to their own privacy policies and government regulations. She is a co-author of an article on their findings, "Disaster privacy/privacy disaster," in the *Journal of the Association for Information Science and Technology*.

The research team looked at 15 apps, selected based on their popularity or the fact that they were recommended in news articles or promoted by app markets. Researchers found that many of them ignore their own privacy policies, capture location data as the default setting as soon as the apps are launched and don't identify all third parties that might receive personal data.

"While we might think an emergency situation is the best time to share information about ourselves with emergency services, we don't expect this would be used for other purposes or collected for a long period of time and stored," Sanfilippo said.

The apps that she and the other researchers reviewed fell into five categories: government agency apps, such as the Federal Emergency Management Agency app; general weather apps; third-party apps that are operated by government partners, such as the American Red Cross; third-party apps that misrepresent themselves as government apps; and third-party apps specific to a particular type of emergency, such as hurricanes.

In order to be hosted on major app markets such as Google Play or Apple, app developers are required to have privacy policies. Organizations that partner with government agencies also must comply with federal law and agency policies.

A common problem with privacy policies is that they state that information might be shared with third parties, but they aren't specific about either the type of information that might be shared or the identity of the third parties, Sanfilippo said.

Among the concerns about the apps are tracking and location-based personalization that continue despite attempts to disable such features in settings, and real-time tracking features that persist indefinitely unless the apps are uninstalled, Sanfilippo said.

Her research found that 13 of the 15 apps collect location information, although only seven transmit that information to other recipients. A total of 42

third-party recipients received location information about the users of the apps she studied. Even when "location services" is disabled in the apps, five of them continue to use the last identified location for a user.

Personal data is often collected by default and consumers don't know to opt out, Sanfilippo said. In other cases, information is shared between apps, particularly those developed by the same companies.

Some apps developed by third parties are deceptive in that they use the style and name of government agencies. Several look like they are operated by the National Weather Service or the National Oceanic and Atmospheric Administration, but neither of those agencies have their own app, Sanfilippo said.

Overall, government apps are doing a good job, Sanfilippo said. For example, the FEMA app collects no personal information without an opt-in by the user.

"They've really minimized data collection, and the information quality from those agencies is going to be very high," she said.

Sanfilippo said the research has raised questions about what counts as an emergency, when it begins and ends, what information is appropriate to gather, who should have access to that information and under what conditions, and when that access ought to end. The goal of the research is to support policies that reconcile pressing public safety concerns with long-term consequences for privacy. There should be broader regulations concerning privacy issues with the apps, including those developed by third parties, she said.

In the meantime, consumers can protect themselves by opting out of data collection when given the choice to do so, and they should delete emergency apps when the crisis is over.

"You might need a hurricane app during a hurricane, but you certainly don't need it tracking you for the next three to five years," Sanfilippo said.

The issues she studied also are relevant to the health information collected during the pandemic.

"It is interesting to see what lessons we learned—how to better educate consumers and better provide privacy protections—that will apply in other contexts," Sanfilippo said.

More information: Madelyn R. Sanfilippo et al. Disaster privacy/privacy disaster, *Journal of the Association for Information Science and Technology* (2020). DOI: 10.1002/asi.24353

Provided by University of Illinois at Urbana-Champaign