Insight

Could Your Smart Phone Help in the Fight Against the COVID-19 Pandemic?

JENNIFER HUDDLESTON | APRIL 15, 2020

- Personal information, such as location and health data, can provide important insights that can improve public health responses to the COVID-19 pandemic.
- Companies working to provide data are taking steps to use privacy-sensitive technology and allowing individuals to opt-in to the services.
- Government data usage related to the COVID-19 pandemic should have limitations that protect civil liberties and prevent abusive government surveillance.

During the pandemic, policymakers and experts have debated how governments should be able to use location data and other personal information to track the contacts of those diagnosed with COVID-19, identify potential hot spots, or enforce social distancing or quarantine requirements. South Korea and Israel have used location data for individual contact tracing and pushing notifications to self-quarantine. But left unchecked, such monitoring could devolve into intrusive government surveillance that could curtail civil liberties and lead to future abuse. Innovative solutions harnessing aggregate data or new uses of existing technologies like Bluetooth can enable a data-informed response to the pandemic, but will require legal safeguards around the use and collection of this data by the government to limit the risk to civil liberties.

Using Data to Tailor Policies

Data regarding contacts of infected individuals or aggregated information about community trends can be used to map the spread of the virus, identify potential hotspots, and better deploy potentially scarce resources. Clearer data about diagnosis, spread, and social distancing could be utilized by policymakers and public health officials to better tailor responses and allow a quicker economic recovery by more narrowly tailoring the most extreme responses.

Government access to already available data could help enable more specific responses around the pandemic regarding needed public health measures and an improved understanding of the disease. A recent Duke Margolis Center for Health Policy white paper lays out how in addition to improved testing, improved methods of tracing the spread of the pandemic and individual contacts are also needed for successful containment. The paper suggests that such surveillance be coordinated by government health authorities such as the Center for Disease Control and Prevention (CDC) and local public health authorities. This health data would be key not only in better understanding the spread of the disease to improve containment, but it could also be useful in providing better information about where additional resources are likely to be needed.

Beyond initial containment, a data-informed approach could also help when considering reopening businesses and a gradual reduction of current restrictions. As a proposal by former Food and Drug Administration Administrator Scott Gottlieb discusses, a data-based approach would enable a phased approach to reopening by

allowing the lifting of certain restrictions (such as the closing of schools and businesses) on a state, county, or city level based on trends and containment. Under the proposal, officials could then determine when to move between phases based on data about infection spread and containment. This data-informed approach allows policymakers to make decisions on a more narrowly tailored level and can provide important benchmarks for determining when it is less risky to remove certain restrictions. A data-based approach could also illustrate the benefits of different policies by illustrating different aggregate behaviors as a result of nuances in stay-at-home orders, allowing policymakers to make more informed decisions regarding any number of variables.

Technical Solutions to the Privacy Problem

But could such information be obtained without significant government intrusion or knowledge of the details of an individual's every movement? Many of the public health goals could be achieved with the use of aggregate and deidentified data rather than detailed information on individuals. As Stand Together's Neil Chilson notes, "Such data can help researchers assess how well populations are practicing social distancing, identify hotspots of activity that raise the risk of spreading the disease, and study how the disease has spread." In some cases, private companies have already stepped up to provide such information in this less risky form. For example, tech companies such as Facebook and Google have been able to provide aggregate and de-identified data for academic researchers working on issues regarding COVID-19.

But individual contact tracing for infected individuals will need more detailed information to be successful and would require policymakers to carefully balance privacy concerns with the current public health risks. Google and Apple recently announced a partnership on a new system that would work with public health apps to enable contact tracing through Bluetooth. Bluetooth technology has fewer concerns regarding privacy, because the signals used in such a system do not track physical location, but instead rely on anonymous exchange beacons for phones that have been close to each other rather than the precise location of the devices. The proposed system, which is expected to launch next month, would allow a diagnosed individual to consent to having an alert sent to devices that had been involved in such an exchange. Those individuals notified would then need to take appropriate steps. There are still plenty of questions regarding how this system would work, but this voluntary approach using a more privacy-sensitive technology at least initially appears to balance the need to alert exposed individuals and the risks of less privacy-sensitive tracking. There are some pitfalls that could occur such as concerns about the possibility of false reports. The companies are trying to limit such potential abuse and are partnering with public health officials for validation of diagnoses to build a system that users can find trustworthy.

Safeguarding Civil Liberties in Government Data Collection in a Crisis and Beyond

Even in a pandemic, policymakers should consider ways to ensure that the government's collection and use of personal information is not a gateway for potential civil-liberty abuses. As the Cato Institute's Matthew Feeney argues, crises can prompt policy responses that can curtail freedoms in ways that later prove to be ineffective and unnecessary, so policymakers should ask tough questions and cautiously approach these policy changes. With the difficulty of the situation at hand and the potential benefits of data in the pandemic response, there are some important limitations, such as sunsetting the emergency policies, policymakers can place on both government collection and usage that can provide the information needed for an informed response while still protecting individuals from the potential for government surveillance abuse.

When possible, data used for public health purposes in the pandemic should be aggregated and deidentified or anonymized to the extent possible. This information is likely sufficient for many of the benefits of government use of such data such as tracking the spread, identifying clusters, and determining the effectiveness of different

restrictions. State and local officials might use data on a more specific county or city level, for example, to determine where “stay-at-home” orders or additional medical resources are necessary. The data utilized for pandemic purposes should whenever possible be obtained through voluntary consent and have a transparent purpose for the data collection and usage. This can be seen, for example, in surveys that individuals complete to inform researchers about their current behavior and by allowing infected individuals to opt-in to the sharing of information with their contacts.

Policymakers should also establish appropriate limitations on the use of data to prevent its exploitation beyond the pandemic that could result in surveillance or other damage to civil liberties. Policies allowing the government collection of personal health or location information should have clear restrictions regarding its use only for COVID-19 related responses. As civil liberties advocates suggest this would include preventing the use of the data collected for law enforcement or immigration purposes that could result in potentially unconstitutional government surveillance and monitoring. In addition to limitations on what such data could be used for, policies should be accompanied by clear timetables that sunset such provisions at the crisis’s end. Such provisions prevent regulatory creep that in this case risk significant changes in expectation of protection form government intrusion into an individual’s health and home.. Creating sunsets would require further debate for similar collection or uses in any future emergencies and help limit the possibility of such information being used for oppressive purposes outside of a crisis.

Conclusion

Data can help policymakers craft a more targeted response to the current pandemic and could lead to a tailored policy that allows a faster reopening where safe, benefiting many individuals and businesses. Current technologies may enable a voluntary response through data opt-ins that would better inform public health officials and communities in making decisions and responding to the pandemic. Still, it is of the utmost importance that policymakers considering using personal information, even in a crisis like the COVID-19 pandemic, establish clear guardrails on its use and collection to prevent surveillance or other abuses.