Utah's Shiny Surveillance Technology to Address COVID-19 Fails Miserably

Utah's flopped attempt to question all travelers entering the state is a lesson for government leaders nationwide.

Jason Stevenson, Strategic Communications Manager
April 30, 2020
Link: https://www.aclu.org/news/privacy-technology/utahs-shiny-surveillance-technology-to-address-covid-19-fails-miserably/

How many times have you failed to get a new digital device working properly the first time? While toddlers can (amazingly) master iPhones in minutes, some tech gadgets require many troubleshooting attempts to activate. And even then, they might fizzle.

Last month, the state of Utah learned that simple tech lesson in a very public way.

As part of a series of measures to respond to the coronavirus outbreak, Utah Gov. Gary Herbert issued an executive order requiring every adult crossing the Utah border to submit an electronic State of Utah Travel Self-Declaration Form with details about their contact information and health status. To implement the order, the state set up nine virtual border checkpoints positioned across major roads and highways. When crossing one of the checkpoints, motorists were supposed to receive a text message directing them to complete a survey form with their name, address, phone number, email, and any potential symptoms or exposure to COVID-19.

According to the state, the personal and health data collected by this survey was transferred securely from the Utah Department of Transportation (UDOT) to the Utah Department of Health (UDOH) in the event that health investigators needed to follow-up with any respondents about self-quarantining.

At least, that was how the system was supposed to work.

Instead, people sitting at their kitchen tables dozens of miles from the border were receiving text messages to fill out the entry form. One resident of Myton, Utah — located 60 miles from the Colorado border — told *Deseret News* she received 80 text messages from the system in one morning. Simply put, Utah's Wireless Emergency Alert (WEA) system, also called a "geofence," had a lot of holes. In addition, the alert system couldn't distinguish between motorists entering or leaving the state, so many people received the alert while driving from Utah to Nevada or Idaho.
The Utah Department of Emergency Management was forced to cancel the entry alert system within less than 72 hours of its launch. In those hours, the government made several attempts to narrow the wireless zones, but failed to stop the wayward text messages going to people located miles from the state border.

"We knew that this was going to be kind of an experiment and we were trying to do something innovative," Joe Dougherty, public information officer for the Utah Division of Emergency Management, told the *Deseret*

News.

Still, Dougherty went on to note, about 35 percent of the people who received a text message completed the entry form and the state received about 10,000 responses during the 72 hours the system was operational.

That's 10,000 people who provided their personal and health information — including their date of birth, cell phone number, and status as a state resident or visitor — to government agencies likely in error, or without much thought or explanation about how it could be used.

What's most troubling, however, is that Utah's experiment with virtual border checkpoints was canceled not because of concerns about state overreach that infringed privacy, but because of hundreds of complaints from Utah residents whose smartphones got jammed with surveillance spam. The problem wasn't that Utahns were concerned about the government wanting to know personal details about thousands of people entering the state. The problem wasn't the state's threat that it could "take subsequent steps" if travelers entering the state did not comply with the order. Nor was the problem that many people in Utah's immigrant community correctly feared implementation of this new surveillance system given the state's troubled history with the secret sharing of personal data with outside law enforcement agencies, as well as data breaches of sensitive information held by the Department of Health.

The state of Utah's failed experiment with this technology and short-lived plan to infringe on people's privacy should serve as a lesson for government leaders nationwide. It should also serve as a lesson for all of us to scrutinize government actions — even in times of crisis — more closely.

In an effort to justify the privacy-invading system, state and local leaders resorted to hyperbole. They claimed in an FAQ, for instance, that "these are extraordinary times, and Utah is taking extraordinary measures like using this technology (which we have never used in an instance like this before). There may be some kinks here and there, but it's absolutely essential to help us stop the spread of the coronavirus, COVID-19."

Extraordinary times.
Extraordinary measures.
Absolutely essential.

Those phrases jammed into a single, excitable paragraph are certain clues that this effort shifted the crucial balance between state authority and personal privacy too far towards the state. Besides being unworkable, the implementation of this wireless alert system was an unnecessary infringement on personal privacy. It was neither prudent nor effective. And it should not be re-implemented in the future.

Concern over travelers spreading the coronavirus was a significant concern during early stages of the COVID-19 pandemic, but most experts agree that threat is significantly reduced now that 97 percent of the U.S. population is under orders to stay at home or shelter in place and that the virus is already widespread.

State and local leaders would be better served — and would better serve their constituents — if they stick to proven public health measures, not shiny new surveillance technologies that invade our privacy all while wasting precious time and resources.