IDME911 & SMART911 REGISTRATION SERVICES

JULY 30TH, 2020

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ the Urban Justice Center
40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

July 30th, 2020

IDMe911 & Smart911 Registration Services

In 2018, ID Me 911, LLC launched the IDMe911.com registration service ("IDMe911") with the aim of helping law enforcement to identify and locate missing persons. The service solicits civilians to provide identifying and medical information for themselves or relatives. IDMe911 then can provide this information if requested by law enforcement agencies. It joins another existing service, Rave Mobile Safety's Smart911, which collects similar personal information and provides it to 911 operators and law enforcement when the user calls 911. Both services raise serious concerns about the privacy of their users' data, though IDMe911's business model and lack of an established track record make it particularly worrying. Alarmingly, as the nation grapples with the COVID-19 outbreak, municipalities across the country are furthering their use of these services, encouraging their residents to sign up and record any potential symptoms of the coronavirus.

While IDMe911's benefits appear quite tenuous, the risks are imminent. As an initial matter, unlike Smart911—which only transmits users' data, through the app, to the 911 call receiver when a user calls 911—IDMe911's users' information can seemingly be accessed by law enforcement at any time, because information supplied by users is stored in an IDMe911 database supplied to law enforcement. The company's website does not specify the actual mechanics of a law enforcement officer accessing the database, leaving access control questions (e.g., limits on when, how, information can be retrieved) up to speculation. It is additionally unclear if IDMe911 notifies users when their account information has been accessed.

This is particularly concerning because it's also unclear if IDMe911 prevents officers from using information for non-police purposes, though the website states that "Data and information will not be utilized by Law Enforcement for the purposes rendering [sic] aid with criminal investigations" and that "Law Enforcement users are prohibited from sharing user names and passwords with others including Law Enforcement agencies." Officers have frequently misused other police databases to get information on romantic partners, journalists, and business associates, and there's no apparent reason such misuse would be less common with IDMe911. Past examples include an officer who used information in an official database to stalk an ex-girlfriend and another who used it to dig up dirt on a journalist who wrote an unflattering story.

One similarity shared by both IDMe911 and Smart911 is that they create tempting targets for an array of unauthorized users. IDMe911 promises that data is "completely secured," but details are sparse. Documentation is particularly limited for how the IDMe911 mobile app technically connects officers to the service's database. IDMe911 simply states that "information is transmitted to Law Enforcement users utilizing additional third-party vendors." The website specifies that it uses third-

party cloud service provider Caspio, which runs on Amazon Web Services, to store and transmit "all data and information." But it also states that the company utilizes "additional third-party vendors" to transmit data and information to law enforcement users. (Again, specifics are unclear; perhaps the data is supplied by the user into a database hosted by Caspio, and then transmitted via another service to law enforcement?) Even worse than ambiguity on the actual mechanisms and processes through which law enforcement can access the database of user information, the terms continue that all "third-party vendors are subject to change without notice." Without knowing what vendors may access user data, it is impossible to know if IDMe911's security measures are adequate.

IDMe911 documentation suggests that users simply need a "department code" from a participating enforcement agency to register a law enforcement account. It is easy to imagine how such a code could be compromised, as other passwords are frequently obtained by attackers. In turn, officers' IDMe911 account credentials could also be compromised, giving an attacker access to the database.

In theory, hackers could be detected via IDMe911's access log, but it's unclear if IDMe911 or participating law enforcement agencies will actively monitor the access log to identify suspicious activity. Similarly, there is no evidence IDMe911 evaluated the efficacy of these features with penetration testing or third-party security tests. After users upload their information, what happens if they change their mind and want to take it back? Not so fast. According to its terms of service, "[a]ll data and information become the property of ID Me 911, LLC."

Smart911, which again shares user information through a phone app when a user dials 911, provides similarly little detail about its security measures. It claims to have been "subjected to intrusion prevention testing," but once again specifics are sparse. When one digs into the details of their privacy policy, the results are less than reassuring, noting that they "cannot guarantee the security of user account or other personal information," and that "[u]nauthorized entry or use, hardware or software failure, and other factors, may compromise the security of user information at any time." Even worse, the fine print binds users' hands, barring any legal claims for "invasion of the right of privacy caused…by the disclosure of any subscriber information."

So what do you get in exchange for these risks? Frankly, not much. Family members already are able to provide this information to police at the time they contact 911. More importantly, much of the information uploaded to these services may never be passed along to police.

That's because users from around the country are free to register IDMe911 or Smart911 accounts, but law enforcement agencies must pay for access. This issue is particularly salient for the newcomer IDMe911; at the time of publication, reports indicate that the Wolcott, New York Police Department is IDMe911's first customer, beginning the service in February 2020. This means that almost every time a user outside the 4,000-person hamlet uploads their intimate details, they get no benefits in return.

Smart911's coverage is substantially better; 45 million people live in areas subscribed to the service. Of course, that still means that 86% of Americans receive no benefit; even if they create an account, their local 911 center will never be able to see that information.

Smart911 is seizing on the current COVID-19 epidemic as an opportunity to increase sale, asking users to report any quarantine conditions. The services' government partner, including Chicago, are also imploring residents to sign up during the outbreak. They say that registering a COVID-19 positive diagnosis in the app enables firefighters and paramedics to wear proper PPE while answering your 911 call. Of course, this could be just as easily accomplished by simply telling the 911 operator that you have COVID-19. But even more importantly, since 80% of COVID-19 patients were infected by someone who didn't know they were sick, first responders need to take the same precautions on *all* calls, not just those where a person has registered as COVID-19 positive.

Certainly, both IDMe911 and Smart911 are premised on laudable goals. There can be no doubt that keeping first responders healthy is incredibly important. And IDMe911 aims to locate missing persons with "autism, dementia, and other intellectual disabilities." But North Korean-style surveillance databases are not the way to achieve these goals. Paramedics will only be protected from COVID-19 if they have adequate PPE on *all* calls. And simple ID bracelets can be much more effective for identifying and caring for those with dementia. High tech solutions may be more invasive, but that doesn't make them better.

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT