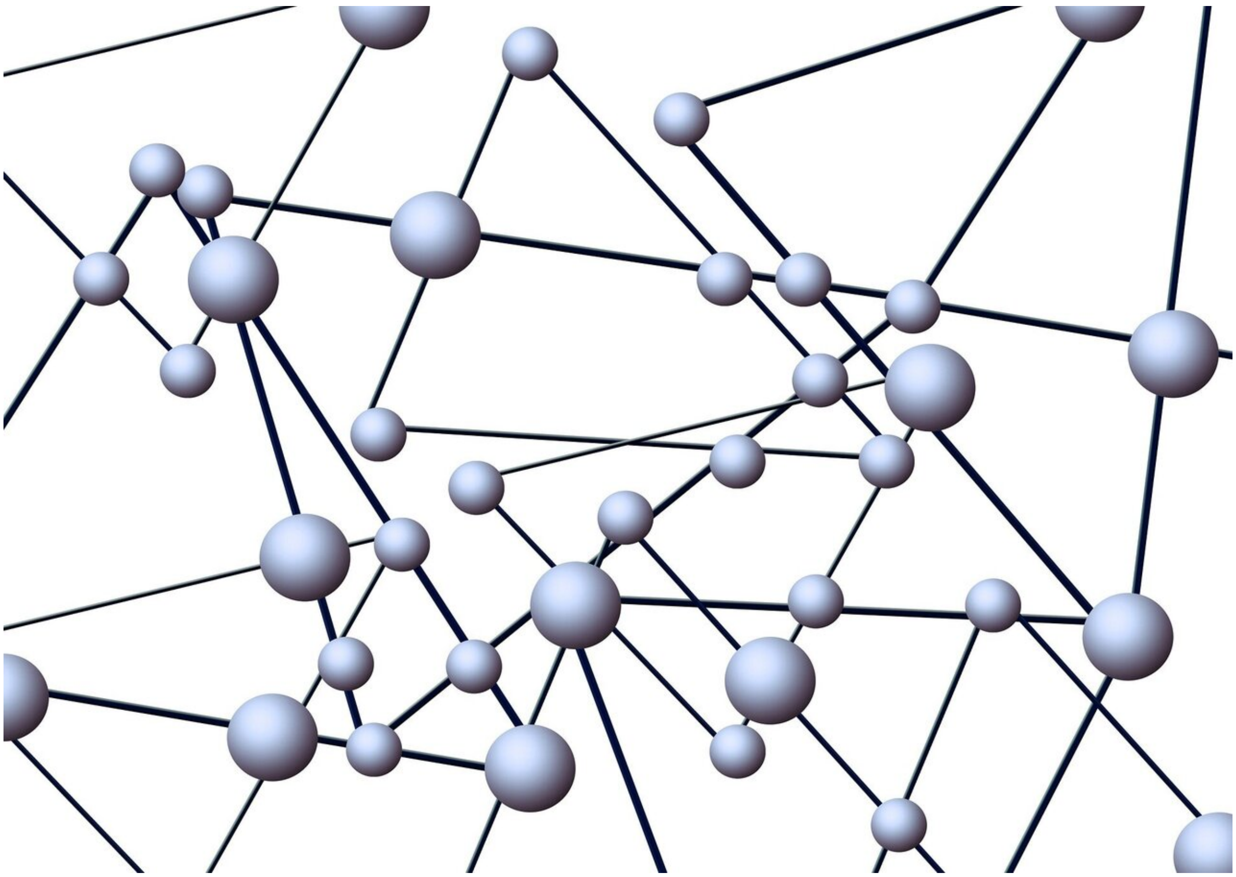
Researchers design more secure mobile contact tracing

February 19 2021, by Jessica Sieff



Credit: Pixabay/CC0 Public Domain

For public health officials, contact tracing remains critical to managing the spread of the coronavirus—particularly as it appears that variants of the virus could be more transmissible.

The need for widespread contact tracing at the start of the pandemic led tech giants Apple and Google to announce a plan to turn iOS and Android phones into mobile "beacons" that alert users who opt in of potential exposure to COVID-19. Health officials in some states have used the technology in their pandemic response efforts, as have other countries around the world, but researchers at the University of Notre Dame say contact tracing apps created by third-party developers could leave users vulnerable to a host of privacy and security issues.

"The purpose of contact tracing apps is to inform users of a potential of infection, to let them know if they've come in contact with someone who could have exposed them to COVID-19, but these apps release more information than is necessary—potentially, tracking data of COVID-19 patients—which could put the privacy of those patients at risk," said Aaron Striegel, a professor in the Department of Computer Science and Engineering and affiliate member of the Wireless Institute at Notre Dame. "Your security is only as good as your weakest link, so the question is, can we trust the people who are creating these apps to do it right?"

Striegel believes one concern is the potential for individuals to create havoc by registering fake illnesses or intentionally creating hysteria around big events, such as an election. "The idea is you protect that by allowing only the health agency to identify the individuals who have been officially diagnosed with coronavirus," he said, "which means the developer needs to work that into the program and have a way to protect it, because those vulnerabilities are targets for malicious actors."

Another concern with COVID-19 tracing apps is the fact that users have to opt in for the services to work but at some point, as vaccinations continue and the threat of the pandemic passes, they need to remember to opt out—or the app keeps running.

"I think the broader concern is, how do you put the genie back in the bottle?" said Striegel. "From a civil liberties perspective, does this approach give people a false sense of security? What's still inconclusive right now is, does the use of these apps outweigh the privacy or ethical concerns in a broader sense?"

Striegel and Taeho Jung, an assistant professor of computer science and engineering at Notre Dame specializing in applied cryptography, are designing an effective and secure framework for mobile contact tracing. "Our goal is to limit the potential for nefarious privacy tracking through these apps, and provide relevant, information-rich data to public health officials that can be used to mitigate the spread of the virus," said Jung.

The proposed framework would include specialized encryptions for data sets coming in to health officials and privacy protection. Users would also be able to monitor how their data is being used. Once completed, the research could impact how public health organizations respond to future pandemics, creating a more effective and efficient way to reach registered users with significantly reduced threats to their privacy.

The team will use prototype software to be implemented on various devices, including computer servers, laptops and mobile devices.

"The software will allow users with mobile devices to be promptly informed when they are potentially exposed to COVID-19, without the possibility of public health organizations or malicious actors tracking individuals," Jung said. "We believe this could be an important step towards instilling increased public confidence as to the safety of such digital tools."

Provided by University of Notre Dame