TechXplore

How technology can help identify a 'safe' workforce and protect personal privacy

April 21 2020

Credit: CC0 Public Domain

As policymakers and business leaders grapple with how to restart the economy and bring employees back to work in the shadow of the deadly COVID-19 pandemic, a new white paper by MIT Professor Alex "Sandy" Pentland suggests that digital tools that certify a person's health status can be used to create "safe" environments for workers and customers—while also protecting people's personal privacy.

The paper arrives amidst a raging debate about how to leverage technology in the face of the ongoing health crisis. Public health officials say that collecting personal data may be the only to track the virus to understand who is healthy and able to return to work and who is most at risk. But privacy advocates have voiced concerns about how

that data will be used and by whom, as well as how and where it's stored.

"Digital tools are an important part of the solution to create a safe workforce that will help reopen the country, but patient privacy shouldn't be sacrificed as a result," says Prof. Pentland, the Toshiba Professor of Media Arts and Sciences and the Director of MIT Connection Science. "More sophisticated methods of computing that preserve health data privacy and data ownership are needed."

Prof. Pentland is working with the United Nations and the Club de Madrid, a consortium of former democratic presidents and prime ministers, on this issue.

The economic devastation caused by the coronavirus has been swift. The U.S. has lost 22 million jobs in four weeks; retail sales have collapsed; and industrial production has fallen precipitously. But even as the government remains focused on containing the virus and caring for the sick, policymakers are starting to plan when and how to reopen the economy.

Restarting the economy requires using blood tests to certify people who are verifiably immune from the illness or vaccinated, and therefore "safe" to rejoin the workforce. This sort of certification is familiar: we already require tuberculosis test documentation for food workers and proof of vaccinations for childcare workers, for instance.

"A safe workforce could be cleared to go back to work in front-of-house, public-facing jobs, which would allow companies, governments, and hospitals to hire workers who are safer—both for the customers but also for themselves," says Prof. Pentland. "These people could staff customer-facing services, while more at-risk workers could perform back-room functions with less human contact."

The creation of a safe workforce is what's behind some of the most successful efforts at suppressing the disease in certain Asian countries, including Taiwan, Korea, and Singapore. These nations relied on "big brother" use of personal data, and authoritarian enforcement of quarantine and isolation. As the disease and recovery progresses, these countries now have a certified group of safe workers that can help restart the economy. But in democratic countries, this approach is seen as a threat to civil liberties.

To protect personal privacy, Prof. Pentland proposes that hospitals, credit unions, banks, and other civic institutions serve as repositories for people's health data, much as they already do for their financial and other personal information. This would form the basis of citizens' "digital identity," and would determine their ability to work and perform other activities. A key point is keeping personal data in local institutions that already have a "need to know" or are under direct citizen control and avoiding the creation of national or state-wide registries since these are tempting targets for misuse.

This health certification, which could be easily integrated into the digital identity infrastructure that is already used for authenticating payments, could also help decide what sort of businesses are safe to reopen, and make contact tracing more efficient, without jeopardizing personal privacy. This could be accomplished by the use of either high-tech methods, such as Secure Multiparty Computation, which is already deployed for some types of updates on mobile phones, or the creation of simple "risk maps" aggregated from anonymized data and appropriately sanitized using differential privacy methods, such as the ones used by the U.S. Census Bureau.

"With this kind of digital identity, people can certify their health status to merchants and employers in the same way their credit card or identity is verified," says Prof Pentland. "They can also see which places are safe to go—for instance, places that are uncrowded or recently cleaned, and where customer-facing employees are infection-free, all without compromising their personal privacy."

Financial incentives could help kick-start the process. The government, for instance, could offer tax breaks to companies that employ safe employees. Businesses, meanwhile, could offer increased pay to motivate safe workers to take public-facing jobs. What's more, businesses could certify that they hire only safe employees in public-facing positions, which would inspire customer confidence.

"Getting people back to work safely is imperative," he says. "Certifying immunity in a way that preserves personal privacy is the first step toward helping people stay safe and healthy, reducing hospital costs, and restarting our economy.

Provided by MIT Sloan School of Management

Citation: How technology can help identify a 'safe' workforce and protect personal privacy (2020, April 21) retrieved 17 June 2024 from https://techxplore.com/news/2020-04-technology-safe-workforce-personal-privacy.html