Restarting the Economy and Avoiding Big Brother:
We need to know who is immune and employ them in the front line

Alex Pentland, MIT
pentland@mit.edu

Summary: Digital identity that allows certification of the user's health status, similar to today's payment acceptance mechanism, can create safe working environments and consumer experiences (restaurants, hotels, meetings) while protecting personal privacy.

A New Economic Resource to help Restart the Economy

Soon we expect to have more than 30% unemployment, and repeated waves of infection for at least two years, preventing normal economic recovery. Finance, government, travel, hospitality, and manufacturing will be devastated, with widespread bankruptcies and business closings. We are going to have to restart the economy starting from a depression-level situation. But how?

One economically significant consequence of these waves of infection is creation a "safe worker" workforce. This workforce consists of people who have been infected and then recovered, so that they can be certified as less likely to become re-infected. This disease-resistant workforce will generally young, but also generally from the poorer communities that are being disproportionally affected.

Can we use these "safe workers" to help restart the economy? To make use of this resource we need to certify who is recovered (or, eventually, who is has antibodies or is vaccinated). As testing become common, fast, and inexpensive we could also certify people who recently tested negative. This is similar to how we already certify that food workers don't have certain infectious diseases, and that childcare workers have their immunization shots. At the same time, this sort of data makes early detection of infection and contact tracing much, much easier, eventually preventing successive waves of infection.

A crude, brute-force version of this idea has been behind the most successful efforts at suppressing the disease (Taiwan, Korea, Singapore). They 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. Similarly, for international travel you have to have certified immunizations, although such certifications are paper-based and the system fragmented.

In democratic countries the use of "big brother" data methods is feared because of the danger that it will continued to be used by government after the immediate emergency.

Consequently, sophisticated institutions are turning to more sophisticated methods of computing that preserve privacy and data ownership[i]. Some countries and companies already use these sorts of methods, and the EU government has committed to migrate to such technology.

A Plan: Start By Making Safety Easy

Imagine a society where credit unions, banks, or other civic institutions serve as repositories for citizens' health data, much as they already do for their financial, identity, educational and operating license status. This personal forms the basis of each citizen's *digital identity*, and determines their ability to legally perform various actions (e.g., making a credit card payment, employment as doctor, entering a bar). In this society a citizen can certify their health status to a participating merchant or employer in the same way their credit card or identity is certified. They can also see which places are safe to go (e.g., places that are uncrowded, recently cleaned), and where the risk is higher, and even get immediate notice if they have been exposed to infection, all without endangering their personal privacy.

Moreover, with such certification available government could offer financial incentives for employment of safe workers, and to motivate safe workers to take jobs that require customer contact. They could also provide incentives for uninfected workers to take jobs that have less exposure to infection, and help make sure they stay safe. Similarly, merchants could (for instance) certify that their business has only safe employees in customer-facing positions.

This health certification also allows for extremely fast and accurate infection contact tracing and individual-level infection avoidance information without threatening personal privacy. Individuals with health certification can have their mobile phone automatically check the status of people around them without sending personal data off of their phone or identifying the people around them. This is accomplished by use of either sophisticated methods such as Secure Multiparty Computation (already nearly universally deployed for some types of updates on mobile phones) or simple "risk maps" aggregated from anonymized data and appropriately sanitized using differential privacy methods (such as employed by the U.S. Census Office).

The major hurdle to implement this vision is sharing of health data certifications to citizens, data which is held by the hospital, state, their credit union, bank, or similar organization. This sort of certification is familiar: we standardly certify that that people working with vulnerable populations have their immunization shots current. Mobile certification is similar to current digital payments, and is easily integrated into the digital identity infrastructure that is already used for authenticating payments, and we at MIT are releasing a USA-wide "safepath.mit.edu" and contact tracing facilities this week. This system helps people stay safe, and can help restart our economy in multiple ways. To help kick-start use of this process government or large employers can provide financial incentives to, for instance, visit newly open merchants, to

employ “safe workers” in customer-facing positions, and for merchants to obtain “safe environment” certification.

[iii] An illustrative example is our Open Algorithms platform and employing Secure Multi-Party Computation, which provably maintains privacy and auditability of fairness and fraud (see trust.mit.edu).