
FUTURE AGENDA
Open Foresight
: Name
: Occupation
: Address
Information
THE WORLD IN 2030
Proof of Immunity
and the Demise of Privacy
Male
Age 25

Proof of Immunity and the Demise of Privacy

Public concerns about health security override worries about privacy. Governments integrate immunity and health data with national identities facilitated by digital identity platforms. Insufficient regulatory control risks the possibility of pervasive and invasive surveillance.

Share of all stored data that relates to health (2020)[1]	**30%**
Data points from smartphone facial scan (2019)[2]	**1200**

In recent years there has been a growing and global ambition to better manage, integrate and interrogate medical data. But, despite the technological achievements around data use in other industries, maximizing its potential for better healthcare has been slow, mainly because the vast majority remains proprietary, fragmented and scattered. There are valid reasons for this; insurers, providers, health record companies, government agencies, and researchers are all concerned about the ethics, not to mention commercial sensitivities, of sharing data.[3] And yet overcoming this mindset could provide huge benefits for diagnosis, integration and the personalisation of care, so there is growing momentum to scale and combine new sources of personal, societal and clinical information.[4] Support for this has accelerated given the pressing need to both manage and find a vaccine for Covid-19. Indeed, many agree that linking personal health data to identity would be a major step forward to better controlling the outbreak of disease.

A pragmatic response to a pandemic is to dial up tracking, tracing and wider bio-surveillance in order to isolate the virus and manage the contagion. But this may come at a cost. Privacy advocates warn that it is precisely in times of crisis that governments focus too much on short term need without robustly exploring the potential consequences; the impact on the right to a private life or the risk of greater surveillance, for example. This is particularly relevant in the midst of widespread efforts to develop national (and other) digital identities.[5] However, such is the pressure on healthcare systems, a significant number of experts we spoke to now expect that by 2030 unified health and identity datasets will be accepted in several regions and that 'proof of immunity' may well have become a core component of everyday life.

Exisiting Examples

The momentum towards this increased integration has been building over the past few years. Tech firms have been working in close partnership with healthcare providers, and offering, for example, a particularly strong use case for their AI technologies. Although there are several early examples worldwide, efforts in hugely populous countries such as India and China are the most notable.

India aims to unify and digitise its fragmented public health system by creating a national database for medical records linked to its Aadhaar national identity scheme. Legislated for in 2016, and building on national security and access ambitions, Indian residents are issued with a unique, 12-digit number that can linked to biometric and demographic data. The number, once authenticated, can then be used to access services across almost all government programs and is active across the entire 1.2bn population. A broad government / private sector IT partnership is evolving the platform to embrace a number of other fields of potential citizen benefits -such as financial inclusion, with a 2017 ambition to make Aadhaar ID mandatory for opening bank accounts.

Aadhaar is well placed to have a huge impact on the delivery of healthcare; indeed the Indian government estimates it can unlock over $500 billion in economic value via reduced transaction costs, increasing efficiency, preventing fraud and limiting inaccuracy, together with tremendous societal and governance benefits.[6] In a country with less than 1 doctor for every 1000 people and with the majority of clinics lacking access to reliable patient records, it is clear that the system could be used during every step of the healthcare journey, from patient registration to digitising medical records. It can also act as a tool for integrated delivery, linking hospitals with pharmacies, NGOs, blood banks, health insurance and medical companies.

However, there has been pushback by several academics and civil liberty activists who are concerned about potential privacy violations. They point to previous security breaches demonstrating how vulnerable Aadhaar is to exploitation both by government, technology companies and bad actors. It is certainly true that the government has a poor record on data security and privacy. In response however the Indian government insists that the Aadhaar health database will maintain strict safeguards. Indeed, the health ministry says that it will provide “universal health coverage in an efficient, accessible, inclusive, affordable, timely and safe manner.”[7]

In **China** citizen surveillance has been part of the wider system for many years and the recent growth in facial recognition technology is accelerating the mass interrogation of personal data across the whole population. It is now used for everything from picking up medication, taking public transport or buying a mobile phone. There are up to 1200 data points available from the typical smartphone facial scan so it can be used to interpret many health issues from body-mass index to emotional wellbeing. Ping-An, one of the world’s largest insurers, uses facial recognition not only to verify a customer’s identity, but to assess, and even measure, an individual’s health. It also claims to be able to record customers’ emotional and psychological states by analysing micro expressions.[8] The data gathered is fed into an automated system for calculating premiums, with discounts provided for those with a low BMI of under 30, and additional costs for those whose BMI is over 30. The technology is even used to approve lump-sum pay outs of up to one million yuan (€130,000) when a customer is diagnosed with any of 100 critical diseases.

The spread of facial recognition has led many Chinese people to worry about the speed of adoption. In 2019 a widely watched CCTV report exposed the black market for facial recognition data and cast doubt about the capability of network operators to store personal data safely.[9] The government has responded by acknowledging the need to introduce greater privacy protection standards. But, given their focus on national security, public health and technology innovation, few believe this will be taken very seriously.

Beyond India and China multiple start-ups are seeking to combine health data with identity technologies, albeit at smaller scale. In Africa, mobile use has been the focus of several notable developments.[10] For instance, Element has developed a mobile software-only solution for biometric recognition that creates a portable identity on mobile devices. Designed specifically for use in healthcare, patients can verify themselves with medical professionals who in turn have access to patient records, and can ensure that appropriate care is being administered, and that new assessments are placed in the correct health record, bringing the union of identity and health care data closer.

In the **US** too there has been significant activity - but so far without widespread public awareness. Google, for example, is working with Ascension, operator of the country's second-largest hospital system, and is using AI to read the health records of millions of patients to predict and quickly identify medical conditions.[11] However, several Ascension employees have raised concerns that it is not clear whether all of the Google's software complies with HIPAA, a federal privacy law that restricts how doctors, health systems and their business associations may handle identifiable patient data, and that the company has too much unfettered access to personal health data.

Tech firms have been working in close partnership with healthcare providers, and offering a particularly strong use case for their AI technologies.

Covid-19 Acceleration

Covid-19 has accelerated the integration of personal health with identity technologies as a number of platforms seek to take things further, faster. Although not yet the 'full-works' and largely focused on mapping and tracking connections, this is seen by some as a precursor to the complete integration of health data with surveillance and identity. Indeed, digital contact tracing has been a central part of the containment strategy in countries such as China, South Korea and Taiwan with a number of other governments looking on with envy.

In China, although shocking to many local Chinese, the existing surveillance operations allowed location data from mobile operators and transport networks to help the government track and contact people who had travelled through Hubei province during the early days of the virus. This enabled the National Health Commission to re-create the steps of virus carriers and identify those they may have encountered, and send them warnings directly via social media. In addition the government developed a Health Check app to run through portals in Alipay and WeChat. This takes self-reported data about places visited and symptoms displayed to generate a QR code in green, orange or red, which then controls an individual's movement across the city, where they work or how they travel, according to their likely level of infection; seven-day and 14-day quarantines.

Although sympathetic to the need to control disease outbreak some believe the Chinese government has used the coronavirus crisis to push for greater sharing of data from private and public sources. Soon GPS location data from mobile networks could be linked to personal data from Alipay (what you have purchased), Meituan (what you have eaten) and WeChat (who you know), as well as health information from Ping-An. Although this could be used to provide a full information set that truly acts as proof of immunity at a moment of crisis, privacy advocates fear that deeper surveillance could become permanent and allow for far less palatable governance in the future, and, for example, exert even greater control over minority groups.

That said, the current absence of a single repository for that data means that the extent of Chinese surveillance remains more limited than some might imagine. "Co-ordination between different areas of the public sector is often sporadic and sometimes marred by bureaucratic rivalries, and even in Beijing, there is concern about making so much information available. The CAC recently issued a notice warning government agencies not to share data for pandemic-prevention purposes that is out of line with data protection standards; private companies such as Tencent and Alibaba with international market ambitions have been reluctant to hand over personal data as it goes against their commercial interest."[13]

But China is not alone. The creation of significant surveillance databases is observed in multiple locations; indeed, a group of academics, developers and public-health officials from the World Health Organisation (WHO) and elsewhere are building a similar MyHealth app,[14] which again benefits from having stronger identity capabilities. In addition:

- In **South Korea** those in isolation used a customised app that sounds an alarm and alerted officials if they left home allowing government to alert others in the vicinity. But the volume of information led to some awkward moments and a growing concern about the social stigma attached to the illness. In addition, the authorities can require telecoms companies to hand over the mobile phone data of people with confirmed infections to track their location. This information has enabled the rapid deployment of a notification system alerting Koreans to the movement of all potentially contagious people in their neighbourhoods or buildings.

Digital contact tracing has been a central part of the containment strategy in countries such as China, South Korea and Taiwan.

- While not hugely accurate, in **Taiwan**, the mobile phones of quarantined individuals were tracked using data from cell-phone masts and compared to the GPS data from WhatsApp, Messenger and so on. In both countries those who did not comply with the rules faced hefty fines;

- In **Singapore** the Government Technology Agency and health ministry launched an app, TraceTogether, which uses Bluetooth technology to retrospectively identify people who have come within 2m contact with someone who has contracted Covid-19. This is particularly useful for those who don't know each other – someone you sat next to on a bus for example;

- In **Iran**, the government has urged citizens to download an app that helps diagnose coronavirus but at the same time allows the collection of their contact and location details;

- **India** may well use the capability within Aadhaar to scale up pandemic mitigation while increasing the overall level of citizen surveillance; and

- **Israel** has already passed an emergency law allowing the state to use mobile phone data to track people infected with Covid-19, as well as to identify and quarantine others they have come into contact with and who may also have been infected.[15] Citizens are receiving smartphone alerts when they have been near an infected person. Civil liberties campaigners have however warned that this move to monitor citizens' movements sets a dangerous precedent.[16]

The creation of significant surveillance databases is observed in multiple locations.

Although counter to long-established privacy values, several western commentators have noted that "we should get used to this: While it might appear draconian and uncomfortable for democracies to be turning outward-facing intel tools on to law-abiding citizens, almost every aspect of this global pandemic pushes us into unfamiliar territory."[17]

In the **US** Google and Apple have announced a previously unprecedented partnership while a host of other technologists have begun working on their own tracking apps. For example, X-Mode and Tectonix have already demonstrated how they can track the movement of people from one location across the country.[18] More significantly for some Clearview AI, a facial-recognition start-up that has previously caused controversy over its use by police departments, is in discussions with state agencies about using its technology to track infected patients.[19] Initiatives such as this have caused concern that "as the country scrambles to control the rapidly spreading coronavirus, government agencies are putting in place or considering a range of tracking and surveillance technologies that test the limits of personal privacy."[20] These initiatives are not only controlled by government, some are open source: MIT Media Lab is developing an app that will let people log their movements and compare them with those of known coronavirus patients, using redacted data supplied by the state or national public health departments.[21] Common to several is of that use decentralised models that keep as much sensitive data on users' phones as possible and uses a centralised server only to enable people to use their own devices to trace contacts.[22]

In the **UK**, teams at Oxford University have been working with the NHS and others on another app to track contacts. This aimed to have at least half the population on the platform by the end of April 2020.[23] Users register their symptoms or positive test results and their proximity to other users will then be logged using Bluetooth. Once a user reports symptoms or has a positive test result, the app can trace back through close contacts over the past seven days and alert those calculated to be at risk.

Alongside this the NHS is working to create a data store that brings multiple data sources needed to inform the Covid-19 response into a single, secure location. It will include data such as online/call centre data from NHS Digital and Covid-19 test result data from Public Health England. Microsoft is providing Azure to bring multiple data sources into a single, secure location while AWS is helping with infrastructure to enable the rapid and secure launch of the new Covid-19 response platforms.[24] Palantir is the CIA-backed data mining firm co-founded by Peter Thiel, who is also on the board of Facebook and an early investor in Clearview AI. It enables disparate data to be integrated, cleaned and harmonised. In the UK the organisation has been given access to the NHS dataset in order to help track and analyse the spread of Covid-19. In the US it is working with the Centers for Disease Control and Prevention to model the virus outbreak. Other companies that scrape public social-media data have contracts in place with the agency and the National Institutes of Health

This may all seem very Big Brother, but ethicists suggest that, even when public trust in government and big tech data collection is low, the circumstances of a pandemic allow people to set aside their reservations. Some governments recognise the concerns – the UK government for example state that the Covid -19 datastore will be closed when the pandemic abates but how long this will last once the immediate risk of infection has passed is unclear. Also, spotting renewed or future outbreaks will require vigilance and unprecedented forms of mass surveillance. Potential carriers of the virus need to be monitored, and their personal contacts traced and, to combat further outbreaks, it may also be necessary for countries to collaborate in new ways. As even ex-MI5 leadership warn, the systems that have created in haste and in response to a present danger may last a long time and give extraordinary power to those organisations which control and manage them.

Proof of Immunity and Health Identity

Moving beyond the Covid-19 pandemic, the wider knitting together of personal and health information is set to have great impact on society with more companies recognising both the social and financial value of medical data, particularly given that health-care budgets around the world are already stretched. According to the OECD the world creates 2.5 exabytes of data a day, 30% of that which is stored is about health. According to The Economist this data is worth about US$600bn a year – roughly the GDP of Sweden.[25] At a time when payers are desperate for insights that might enable them to cut healthcare costs while maintaining quality this offers a huge opportunity. Given this, expect more data-driven companies, more data-driven social innovations, more cyber-security incidents, more breaches of privacy, more artificial intelligences, more miraculous transformations of the ways we live, and more dramatic consequences of that transformation.

Personalised health data is set to be a significant growth area. Over the next decade healthcare providers will use the data platforms to provide patients with individual treatments delivered through clinical apps linked to technologies specialising in particular health issues.[26] To do this they will have to gather a lot of personal data including information about an individual's lifestyle and physiology. Brands such as Vitality already link the level of a customer's exercise to reduced gym fees and health insurance. To help further nudge behaviour, detailed obesity and BMI data could automatically configure more personalised pricing for fast-food restaurants or high calorie items in the supermarket. What a Ping-An and Alipay combination can achieve in China, a Visa / Wal-Mart partnership with Anthem or Aetna could deliver in the US. At a more extreme level, the price of controlled products like cigarettes, alcohol and cannabis could, for instance, be dynamically driven by individuals' health risks.

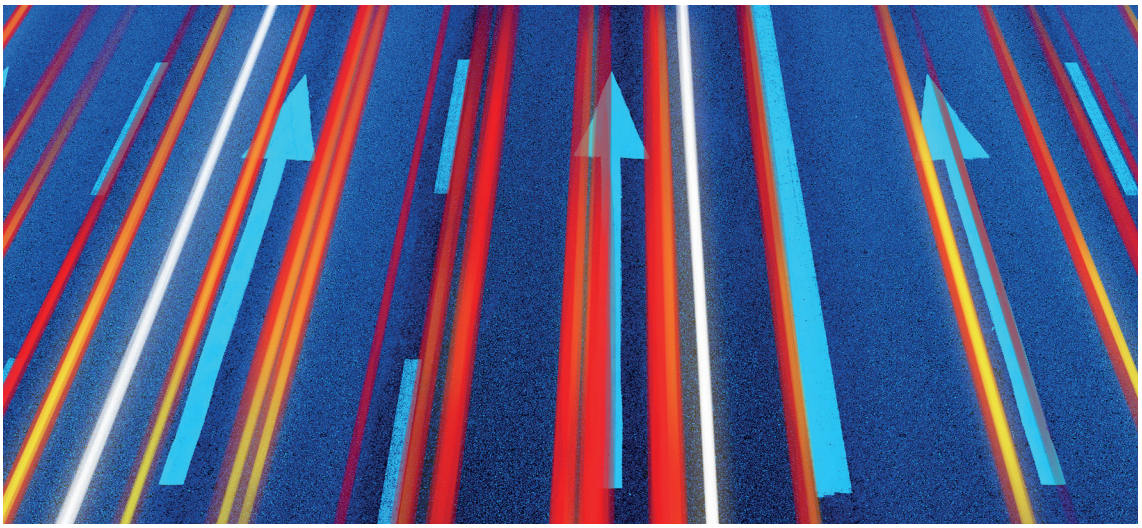
Until now the sharing of this kind of information has been predicated on the basis that it remains private and secure but if governments choose to fully integrate this sort of data with strong identity technologies, then the door is opened to the more complex, but potentially impactful, predictive diagnosis at the individual level. For example, with enough data covering different behaviours it will be possible to identify "digital biomarkers" capable of predicting the risk of Alzheimer's or a heart attack. Although hugely beneficial on one level, controlling who has access to this information is a job for skilled regulators and policy makers. Within the healthcare sector, questions are already being asked around what kinds of pricing and reimbursement models could be applied in such personalised healthcare eco-systems. To date these have largely been at a systemic level but by linking heath provision, medical records with wider behavioural and lifestyle data, it will be possible to provide more focused and effective care and business models need to be considered in that context.

Increased personalisation will also allow for easier proof of immunity, but whether or not individuals are given control of this integration may depend on the political system within a country or the political will of its leaders. Will the databases be centralised or decentralised? And to what extent will individuals be allowed the freedom to share or not share this highly sensitive information? In some countries legislation such as GDPR and CCPA provide a degree of personal control, however, the balance between surveillance, proof of being healthy and access to people and places is likely to become increasingly blurred. In a post-Covid-19 world, concern about a future risk of contagion may well see many nations follow China and others in creating and indelible link between proof of immunity and proof of identity via, for example, a smartphone app which in turn may control personal access to infrastructure, employment, education and health services. In ten years' time it may well be considered normal to have a digital health passport in order to use public transport, enter a supermarket, visit a cinema, or even be present within a city.

Leading in 2030

Given the pressures on healthcare around the world, the value of medical data, the risk of global pandemics and the extraordinary economic consequence that this entails, it is unsurprising that governments and technology companies alike have been exploring ways in which to monitor individual health needs and use this information to control the spread of disease.[27] It is also unsurprising that there is widespread public support for this and recognition of the potential need to link individual identities with immunity. But although it is possible to collect millions of data points which can help protect public health, this comes with serious risk of misuse and potentially the erosion of democratic norms. It is risky to allow a pandemic and the natural demand for better healthcare to normalise mass surveillance. In the hands of a bad actor, either corporate or government, entire populations could be vulnerable to abuse, discrimination and manipulation.

Looking ahead, while proof of immunity is just one way in which the merging of health and identity technologies can be used, it is also the catalyst for wider change. This will not only be about creating and sharing new kinds of health data but also about new access credentials.[28] Indeed, being asked for proof of immunity could well see people being limited in their freedom of movement, not on the basis of citizenship or wealth, but on their individual health. Given the maelstrom of interlinked issues from privacy and freedom to surveillance and the monetisation of health data, what is clear is that governments and companies seeking to turn up the dial will have to navigate a complex path. Balancing wider public benefit with individual freedoms will vary from one nation to another. Getting this wrong and overstepping the line could well drive major political and social pushback.



References

1 https://www.economist.com/technology-quarterly/2020/03/12/the-way-people-live-their-lives-can-be-mined-too

2 https://www.wsj.com/articles/what-your-face-may-tell-lenders-about-whether-youre-creditworthy-11560218700

3 https://www.brookings.edu/blog/techtank/2016/05/18/health-care-data-as-a-public-utility-how-do-we-get-there/

4 https://www.futureofpatientdata.org

5 https://www.futureagenda.org/focus-on/future-of-digital-identity/

6 https://economictimes.indiatimes.com/tech/internet/make-data-with-history/articleshow/74683861.cms?from=mdr

7 https://www.ft.com/content/4fbb2334-a864-11e9-984c-fac8325aaa04

8 https://www.wsj.com/articles/what-your-face-may-tell-lenders-about-whether-youre-creditworthy-11560218700

9 https://www.ft.com/content/7c32c7a8-172e-11ea-9ee4-11f260415385

10 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/04/Innovative-mobile-solutions-linking-health-and-identity-Web.pdf

11 https://www.nytimes.com/2019/11/11/business/google-ascension-health-data.html

12 https://www.wsj.com/articles/how-china-slowed-coronavirus-lockdowns-surveillance-enforcers-11583868093?mod=article_inline

13 https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca

14 https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic

15 https://www.gpsworld.com/covid-19-israels-citizens-now-tracked-by-their-smartphones/

16 https://www.english.acri.org.il

17 https://www.forbes.com/sites/zakdoffman/2020/03/14/coronavirus-spy-apps-israel-joins-iran-and-china-tracking-citizens-smartphones-to-fight-covid-19/#2037ddd4781b

18 https://edition.cnn.com/2020/04/04/tech/location-tracking-florida-coronavirus/index.html

19 https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841

20 https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841

21 https://www.wired.com/story/phones-track-spread-covid19-good-idea/

22 https://www.theguardian.com/commentisfree/2020/apr/11/for-non-intrusive-tracking-of-covid-19-smartphones-have-to-be-smarter

23 https://www.theguardian.com/uk-news/2020/mar/31/nhs-developing-app-to-trace-close-contacts-of-coronavirus-carriers

24 https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/

25 https://www.economist.com/technology-quarterly/2020/03/12/the-way-people-live-their-lives-can-be-mined-too

26 https://techcrunch.com/2019/08/27/why-one-app-to-rule-them-all-is-not-the-future-of-digital-health/

27 https://www.futureagenda.org/foresights/global-pandemics/

28 https://www.futureagenda.org/focus-on/the-future-of-patient-data/

FUTURE AGENDA
Open Foresight

The World in 2030

This is one of 50 global foresights from Future Agenda's World in 2030 Open Foresight programme, an initiative which gains and shares views on some of the major issues facing society over the next decade. It is based on multiple expert discussions across all continents and covers a wide range of topics. We do not presume to cover every change that will take place over the next decade however we hope to have identified the key areas of significance. Each foresight provides a comprehensive 10-year view drawn from in-depth expert discussions. All foresights are on https://www.futureagenda.org/the-world-in-2030/

Previous Global Programmes

The World in 2020 was published in 2010 and based on conversations from 50 workshops with experts from 1500 organisations undertaken in 25 countries as part of the first Future Agenda Open Foresight programme. This ground-breaking project has proven to be highly accurate in anticipating future change and the results have been used by multiple companies, universities, NGOs and governments globally. Rising obesity, access not ownership, self-driving cars, drone wars, low cost solar energy, more powerful cities and growing concerns over trust were just some of the 50 foresights generated. For more details: https://www.futureagenda.org/the-world-in-2020/

Five years on, the World in 2025 programme explored 25 topics in 120 workshops hosted by 50 different organisations across 45 locations globally. Engaging the views of over 5000 informed people, the resulting foresights have again proven to be very reliable. Declining air quality, the growing impact of Africa, the changing nature of privacy, the increasing value of data and the consequence of plastics in our oceans are some of the foresights that have already grown in prominence. For more details: https://www.futureagenda.org/the-world-in-2025/

About Future Agenda

Future Agenda is an open source think tank and advisory firm. It runs the world's leading Open Foresight programme, helping organisations to identify emerging opportunities, and make more informed decisions. Future Agenda also supports leading organisations on strategy, growth and innovation.

Please contact us via:
douglas.jones@futureagenda.org

Future Agenda
84 Brook Street
London W1K 5EH
www.futureagenda.org
@futureagenda