The following is a selection of global COVID-19 developments compiled by the Thomson Reuters Data Privacy news team. This news bulletin covers technology developments, cybersecurity, proposed legislation, and other key data privacy updates relating to COVID-19.

Users can sign up to receive the Daily Bulletin for more news articles through Profile Settings – Preferences.

**Technology Developments**

*Facial Recognition Tech Better at Identifying People in Masks, NIST Says* U.S. (December 2, 2020)

Improvements in facial recognition technology since COVID-19 began now make it better at identifying people wearing masks, a report by the National Institute of Standards and Technology (NIST) found. The report, Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face Recognition Accuracy with Face Masks Using Post-COVID-19 Algorithms, is NIST's first study of facial recognition systems developed after COVID-19 began. It found improved accuracy in the newer systems.

*QR Codes For COVID-19 Detection: CDMX And Its Use of Mass Surveillance Technologies* Mexico (December 1, 2020)

The Mexico City government has announced changes to the Closed Space Contagion Identification System implemented as a strategy to control COVID-19. This system consists of QR codes generated by commercial and service establishments to be scanned with a cell phone by people who want to enter. The user then provides their phone number to be notified if they have been at risk of contagion. When this measure was first proposed in the city, it was intended to be mandatory in order to enter establishments. This generated controversy among CDMX individuals and forced the Digital Agency for Public Innovation to adhere to the guidelines established by the World Health Organization for proximity tracking technologies.

*The Israeli Privacy Protection Authority Objects To Compelled Use Of Contact-Tracing Technology* Israel (November 30, 2020)

The Israeli Privacy Protection Authority has raised concerns about the proposal to make it mandatory for Israelis to use contact-tracing technology before entering public places in light of COVID-19. The Authority expressed its strong objection to imposing an obligation on individuals. It states that it is a contravention of the current statute which provides that
use of contact-tracing technology shall be subject to the individual's informed and voluntary consent.


Massachusetts may soon join more than a dozen US states in offering a smartphone app that can warn users of possible exposure to people infected with COVID-19. However, it is far from clear that the highly touted technology will actually help check the spread of the disease. In the states where such apps are available, relatively few people use them. Flaws in the design of the apps make them prone to false positive results, according to Ryan Calo, co-director of the Tech Policy Lab at the University of Washington.

SEC Expands Use of Electronic Signatures on Documents Filed With It U.S. (November 23, 2020)

The Securities and Exchange Commission (SEC) will allow greater use of electronic signatures in documents sent to it, building on efforts it began in March because of the COVID-19 shift to home working. The SEC is making it easier for filers to use e-signatures without having to first submit a manual one for comparison. The SEC received feedback from the industry that the manual process was a burden due to many people working from home.


Jonathan Albright, Director of the Digital Forensics Initiative at the Tow Centre for Digital Journalism, released analysis he did into 493 COVID-19 related iOS apps. The results highlight how such apps routinely take more data than they need to, including unnecessary access to cameras and microphones. A lot of this data ends up in the adtech ecosystem for profit.

Cybersecurity

Hackers Targeting Covid-19 Vaccine Supply Chain, IBM Warns (December 4, 2020)

With multiple vaccines close to becoming available in a world gripped by the coronavirus pandemic, manufacturers have become the target of hackers trying to steal trade secrets or disrupt supply chains. IBM warned Thursday that it had uncovered a series of cyber-attacks, potentially carried out by state actors, against companies involved in the effort to distribute vaccine doses, which must be kept cold.

Cybersecurity and Digital Privacy in Zimbabwe Zimbabwe (December 3, 2020)

Internet Society's senior policy advisor for Africa, Verengai Mabika from Zimbabwe, supports the Cybersecurity and Data Protection Bill. The sudden increase in the number of online attacks has exposed Zimbabwe’s limited capacity and its lack of awareness about digital security. He also mentioned that in some African nations, the cyberattacks underwent a paradigm shift as they started impersonating the NGOs working in COVID-19 affected areas.

Data Gathering Capped as Centralized QR Check-In System Launches in South Australia Australia (December 1, 2020)

A mandatory QR code check-in system is rolled out across the state, and despite original suggestions it would require large amounts of personal information, the State Government is opting for a more limited approach to data gathering. The system has been rolled out to help contact tracers locate people who may have been exposed to COVID-19.
German Regulator Finds Serious Deficiencies Among Insurers in Meeting Cyber Security Requirements

Germany (November 30, 2020)

An inspection undertaken by the German financial regulator, BaFin, has identified several deficiencies, including some serious ones, in the implementation by insurance firms of the supervisory requirements for information security. BaFin inspected 16 insurance firms and found none of them fully complied with the requirements. With the increased data traffic as a result of COVID-19, it is an aggravating factor for cyber-attacks and raises data privacy concerns.

Leak Exposes Personal Data For Millions of Brazilian COVID-19 Patients

Brazil (November 28, 2020)

Brazilian newspaper Estadao has learned that a Sao Paolo hospital worker uploaded a spreadsheet with login details for two government databases to GitHub, exposing personal data for millions of COVID-19 patients. The E-SUS-VE and Sivep-Gripe data sets included patients’ names, addresses, identification and medical histories.

Cyber Attacks on Finance Sector Soar During COVID-19 Crisis

UK (November 24, 2020)

Personal data breaches caused by cyber-attacks on financial companies have surged during the COVID-19, new figures reveal, potentially exposing investors’ sensitive information to criminals. Between January and June, the finance, insurance and credit sector reported at least 122 cyber security incidents to the UK regulator under the General Data Protection Regulations, an increase of more than 54 per cent on the same period last year.

Other Key Data Privacy Updates

Digital COVID-19 ‘Health Passports’ Should Not be Rolled Out, in Order to Protect Human Rights

UK (December 3, 2020)

A report has warned digital health passports should not be introduced on a mass basis in order to protect data privacy and human rights. Digital health passports, also known as immunity passports, are digital credentials which when combined with identity verification allow people to prove their health status.

Microsoft 365 Allows Your Boss to Track How Often You Send Emails And Use Your Camera

UK (November 29, 2020)

A new Microsoft 365 feature enables employers to track employee’s productivity whilst working from home during the COVID-19 lockdown. The new feature is a ‘productivity score’ tool which analyses 28-day periods and uses a wide range of criteria to award workers with a productivity score out of 800. Factors Microsoft 365 looks at includes how regularly you use your e-mail, Word, Microsoft Teams and even how often an employee switches on their camera during a Teams meeting. Questions have been raised about whether the tool could be used legally in EU countries.

The COVID-19 Data Spies Paid to Know All Your Secrets

UK (November 28, 2020)

A private firm has signed lucrative deals with local authorities to garner data which can be used to predict who is likely to break self-isolation rules. The information is culled from council records and includes family debt levels, living arrangements, income, school absences and exclusions. It is fed into a profiling system called COVID OneView to create a risk analysis for households. Town halls have said the aim is to help identify those most at risk from COVID-19, however, a council previously presented slides at a video conference showing the information could be used to predict who might break isolation
rules. MPs and campaigners said the system lacked transparency and it was not clear why so much information was needed about residents’ lives.

Use of staysafe.ph App Now a Must For Local Government Units And National Government Agencies Philippines (November 28, 2020)

The government panel handling the country’s pandemic response has made use of the staysafe.ph contact-tracing application mandatory for national government agencies and local government units, and said all data collected through digital applications would be sent to a centralized hub. The Inter-Agency Task Force for the Management of Emerging Infectious Diseases, also said the staysafe.ph application would be promoted for use in all private establishments, and those with existing contact-tracing applications are asked to integrate their systems with the existing staysafe.ph system. Experts had expressed concern about the privacy of data collected through the staysafe.ph application but government officials said there were enough safeguards to prevent the abuse and misuse of the collected data.

COVID-19 Data Collection Scheme Highlights Many Privacy Issues India (November 27, 2020)

The government’s response mechanism to contain the virus outbreak consisted of collecting personal data of COVID-19 patients and their relatives, gathering data through contact tracing, and seeking data from the public through the Aarogya Setu mobile application. However, little regard has been given to individual’s privacy and insufficient effort has been made towards protecting data and collecting it in a secure manner. The app has already drawn criticism regarding data safety and its alleged use for surveillance purposes. Furthermore, there are concerns in relation to how the health data collected through the app is going to be used after the pandemic is over.

Watchdog Releases QR Code Guidelines Australia (November 23, 2020)

The Office of the Australian Information Commissioner has released draft guidelines for how providers should capture and store the data collected when patrons use a QR code check-in system. The draft guidelines suggest personal information collected under the check-in system should only be used for contact tracing purposes, should be stored securely and should be deleted after 30 days. QR codes are more widely used than the federal government contact tracing app, COVIDSafe and concerns have been raised over whether the private providers offering restaurants and cafes the service are selling off that data to third parties. However, most small businesses with an annual turnover of less than $3 million are not covered under the Privacy Act which limits the privacy watchdog’s power to investigate and determine if the Act has been breached.