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**

*Quebec Rejects COVID-19 Alert App*  
Canada (August 26, 2020)

The Quebec government has decided that it will not adopt a province-wide smartphone application designed to help stem the spread of COVID-19. The decision goes against the federal government's ambitions to have every province and territory use the COVID-19 Alert app which was made in Ontario.

*Privacy Risks And Implications of Contact Tracing Apps And Related Technologies*  

A review of Norway’s response to privacy issues regarding technology assisted contact tracing, including contact tracing apps. The county’s data protection authority raised its privacy concerns in June, determining that the app proposed a disproportionate threat to user privacy and requiring the country to entirely halt use of its nationwide contact tracing app.

*App to Track And Fight COVID-19 For Launch in Lagos*  
Nigeria (August 25, 2020)

The app was launched in Lagos to help organizations and individuals in the fight against COVID-19. The Managing Director OOK Group Nigeria Limited Omolara Svensson indicated that there is an individual subscription and a corporate subscription.

*Aarogya Setu Launches Open API Services Portal: All You Need to Know*  
India (August 22, 2020)

India’s open source COVID-19 contract tracing app, Aarogya Setu, has released an Open API Services Portal through which third party apps can check users' health status. The API terms and conditions state that only health status of registered app users with consent and no other personal data will be provided through the API. According to the service's terms and conditions, this API service is available only to organizations and entities which are registered, have operations in India, and have more than 50 employees/customers/users.
Cybersecurity

*Trend Micro Blocked 8.8 Million COVID-19 Threats in the First Half of 2020* Hong Kong (August 27, 2020)

Trend Micro Incorporated, the leader in cybersecurity solutions, released its annual mid-year roundup report, which reveals COVID-19 related threats as the single largest type of threat in the first half of the year.

*Hawaii Trails Behind Other States in The Data It Shares About COVID-19* U.S. (August 21, 2020)

Other states are publishing data and information that Hawaii lawmakers and the public have been clamoring for, but the Hawaii Department of Health has not been making public, often citing privacy concerns.

*Is the Right to Privacy Being Compromised in Fight Against Coronavirus?* India (August 21, 2020)

Authorities are taking on the COVID-19 pandemic through stringent containment measures and contact tracing through technological solutions. Among these, is the use of apps to track people with symptoms and the use of phone numbers to trace locations that one has visited, thereby tracking primary and secondary contacts. Recently, the Kerala police admitted to tracking patients and contacts through CDR (call detail records).

*COVID-19 Exposes UK’s Cyber Security Vulnerabilities – With Over 65,000 Attacks Taking Place Daily* United Kingdom (August 19, 2020)

The findings come from a new report by global recruiter Robert Walters and data provider Vacancysoft – Cybersecurity: Building Business Resilience – which claims that the cost of data breaches to UK companies is around £2.48 million per instance.

Proposed Legislation

*India Readies Draft Data Policy For Digital Health Mission* India (August 27, 2020)

The Indian government has released a draft health data management policy which will serve as the guiding principle for protecting the data privacy of people willing to enroll for the National Digital Health Mission (NDHM). The draft policy has been released on the website of the NDHM and will be available for public comments and feedback until September 3.

*Bipartisan House Bill Aims to Enhance COVID-19 Data Sharing, Cybersecurity* U.S. (August 26, 2020)

A bipartisan bill introduced in the House would promote secure COVID-19 data sharing among the Health and Human Services Department, the Centers for the Disease Control, and state and local health authorities.

Other Key Data Privacy Updates

*COVID Affected Oversight: Australian Prudential Regulation Authority* Australia (August 27, 2020)

The prudential regulator has admitted that remote monitoring has diminished the effectiveness of its oversight with financial institutions, as it detailed cybersecurity cracks in the sector's operational resilience through the COVID-19 pandemic, including employees sending sensitive data to their own personal emails.
App a Boon For Venues' Visitor Lists Australia (August 25, 2020)

Townsville Chamber of Commerce has stated that every venue should register for an innovative free contact-tracing platform that takes away the paperwork in meeting COVID-19 tracing requirements.

Wrong Number: Lab Pauses Test Texts Australia (August 24, 2020)

SA Pathology has put on hold the use of an SMS service sending COVID-19 test results after one was sent to the wrong person. Health Minister Stephen Wade said the error may have been due to a transcription error in the name or phone number.

A 'Regrettable Error.' University of Kentucky COVID-19 Data Left Vulnerable U.S. (August 23, 2020)

The University of Kentucky has learned that a spreadsheet containing negative COVID-19 test results and personal information of several hundred University of Kentucky students and a few employees was left vulnerable to viewing by anyone with an active UK email address. The vulnerable data has since been moved to a more secure and private location.


Officials involved with the creation of Pennsylvania's upcoming COVID-19 notification app are worried about privacy and whether an app will spur questions about government intrusion into our private lives. This has been a concern since the creation of a "tracking app" was first considered - a phrase officials involved with Pennsylvania's app do not like and ask reporters to refer to as a "notification app."


The Federal Bureau of Investigation (FBI) is investigating a data breach that may have exposed the identities of COVID-19 patients in the state of South Dakota. The data breach targeted servers belonging to a third-party database shared between the Department of Health and law enforcement.

Mask Switcheroo South Africa (August 20, 2020)

After years-long battles to ban face coverings in public, several countries have now ruled that masks are mandatory, to combat COVID-19. The mandatory wearing of masks in public raises intriguing questions around privacy, profiling, security, and even faith and identity.

Use of Call Records For Contact Tracing a Concern in India India (August 20, 2020)

The Kerala government's decision to collect the phone call records of COVID-19 patients in the state has sparked concerns in India about breaches of privacy becoming routine during the pandemic. By law, the police can collect call records only during a criminal investigation. However, officials in four states have commented that accessing call data records was a necessary and accepted method of contact tracing.