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

**COVID-19 Accelerates Cloud Transformation For Nearly Half of Organizations: Study** India (October 20, 2020)

Nearly half of IT decision makers in companies had to accelerate their cloud migration plans and IT modernization overall during the COVID-19 pandemic, according to a Centrify-Censuswide study. As they evolve to meet current and future requirements, the top two modernization priorities for the next 12 months are maintaining flexibility and security for remote work and digitizing more processes using cloud-native services.

**Digital Health ID Not Mandatory For Accessing COVID-19 Vaccine: Health Ministry** India (October 20, 2020)

A digital health identity under the National Digital Health Mission (NDHM) will not be mandatory to get vaccinated when immunization against COVID-19 is available, the Union Health Ministry announced. The ambitious NDHM program was announced by Prime Minister Narendra Modi during his Independence Day speech. As per the program, everyone enrolled for the mission will get a Health ID that will ease access to medical services.

**Federal Government Wants B.C. to Allow Contact-Tracing App** Canada (October 15, 2020)

The federal government wants British Columbia to join the majority of Canadian provinces in making use of its COVID-19 tracing smartphone app. Prime Minister Justin Trudeau's office sent out a news release saying Quebec had joined Ontario, Manitoba, Saskatchewan, Prince Edward Island, New Brunswick, Newfoundland, and Labrador in allowing health authorities to make use of the COVID-19 Alert app. The app notifies users if they have been exposed to someone who has tested positive for COVID-19.

**Most Healthcare Apps Have Weak Security, Report Finds** India (October 13, 2020)

A recent assessment of some of the most popular mobile healthcare apps has revealed serious security vulnerabilities across the board. Among them are COVID-19 tracking apps, of which 85% were found to leak data. Software firm Intertrust Technologies analyzed 100
apps using testing based on the Open Web Application Security Project mobile app security guidelines.

**UK's Test And Trace 'Having Marginal Impact': Which Countries Got it Right?** UK (October 13, 2020)

The newly released assessment by the UK government's scientific advisers that the test and trace program is marginally reducing COVID-19 transmission has refocused attention on how other countries are faring. Since test-and-trace programs were first raised around the world at the outset of the pandemic, they have been troubled by privacy issues and public support.

**Cybersecurity**

**ERISA/Cybersecurity Considerations in The COVID-19 Age** U.S. (October 21, 2020)

Given the trillions of dollars held by employee benefit plans, these plans are prime targets for cybercriminals. Plan participants are also increasingly accessing their information online but are not always reviewing their account history for accuracy. Plan participants, administrators, and service providers are also prime targets for cybercrime, especially as a result of issues caused by COVID-19. In fact, since the rollout of the Coronavirus Aid, Relief, and Economic Security Act, there has been a dramatic increase in the number of 401(k) plan participants seeking distributions and loans.


Cybersecurity Month has arrived amidst an increase in scams by 400% since March, making COVID-19 the largest-ever cybersecurity threat. While the global lockdown may have been good news to online retailers and remote-based businesses, it also provided an environment ripe for cybercriminals to benefit lucratively.

**The Urgent Needs For a Robust Cyber-Security Infrastructure in The Indian Healthcare Sector** India (October 16, 2020)

India has proved itself to be one of the fastest-growing digital economies over the past few years and the recent pandemic has further enhanced this growth. The Indian Healthcare segment is one such prominent sector, which has gained rapid growth in digitization after the COVID-19 outbreak. From e-consultations, guided video examinations, email prescriptions, and even e-retail of medicines, digital became a way of medical practice.

**What Are The Updates on Cybercrime Law in UAE During COVID-19?** UAE (October 14, 2020)

Legal Consultants of Dubai have observed numerous changes in the laws and regulations throughout the pandemic situation and has implemented several measures to prevent its further spread. The cybercrime department, police authorities, and other relevant authorities are in a difficult situation, needing to investigate and control serious and cybercrime offenses, considering the use of vast technology during the pandemic to ensure the safety of residents in the country.

**Proposed Legislation**

**House Bill Aims to Boost K-12 Cybersecurity** U.S. (October 22, 2020)

The Enhancing K-12 Cybersecurity Act would direct the Cybersecurity and Infrastructure Security Agency (CISA) to establish a K-12 cybersecurity clearinghouse to disseminate information, highlight best practices, and grant opportunities to improve cybersecurity,
the lawmakers said. Reps. Matsui and Langevin noted that the COVID-19 pandemic has resulted in larger numbers of K-12 students attending classes remotely, enlarging the cyber-attack surface for hackers.

**Other Key Data Privacy Updates**

**1M Pinoys Apply For PhilSys ID** Philippines (October 23, 2020)

More than a million Filipinos have applied for a national identification card in the first eight days of registration despite fears that the Philippine Identification System (PhilSys) may be used to suppress civil liberties or violate privacy laws.

**Telefonica Deploys Facial Recognition System at La Vuelta Cycle Race** Spain (October 20, 2020)

Telefonica said it will be implementing an innovative facial recognition algorithm at Spain's La Vuelta cycle race, the third and final Grand Tour of the summer race season, from 20 October to 08 November. The anti-COVID-19 technology will serve to eliminate the signing-in process at the beginning of each stage.

**COVID-19 Apps Raise Issues Over Personal Data** U.K. (October 19, 2020)

Mobile apps designed to reduce the spread of COVID-19 have now been rolled out across the UK, including Scotland, which released the Test and Protect app on September 10, two weeks ahead of the Track and Trace app for England and Wales. These apps are part of a global effort to contain the spread of the pandemic, however, as we've seen in other parts of the world, their introduction has been controversial, partly due to concerns over the potential misuse of personal data. Part of these concerns stem from the tracking app initially proposed for England and Wales as it was storing the data centrally, collecting a high level of it, including location data, and retaining it for longer than required for tracing purposes.

**Protecting And Promoting Privacy And Information Access Rights in Sharp Focus in 2019-20** Australia (October 15, 2020)

The COVID-19 pandemic has focused attention on privacy and created opportunities for greater transparency through the proactive release of government information, according to the 2019–20 annual report from the Office of the Australian Information Commissioner (OAIC).

**National Privacy Commission Probes 11 Establishments For Alleged Data Breach** Philippines (October 13, 2020)

The National Privacy Commission (NPC) has announced that 11 establishments are under investigation after complaints surfaced that the personal data of customers was being used for purposes other than for contact tracing, such as marketing. The establishments may face penalties for unauthorized processing.

**Kuwait Hit by 1,305 Cyber-Attacks Tied to COVID-19 During H1 of '20** Kuwait (October 11, 2020)

A report has indicated that Kuwait was exposed to 1,305 cyberattacks related to the COVID-19 pandemic during the first half of 2020. As cases of COVID-19 continue to increase, many attackers and hackers on the Internet are taking advantage of the word "coronavirus" or "COVID-19" to launch more cyber-attacks, including spam attacks, breach of corporate email addresses, malware, ransomware, and malicious domains.