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 App Downloads Hit 5 Million Canada (November 2, 2020)

An official with the COVID Alert Task Force says downloads of the app designed to alert Canadians if they have been exposed to COVID-19 is expected to have hit 5 million downloads. Director General Lucie Vignola said that new features on the app provide a more accurate timeline as to when someone was most contagious.


As the COVID-19 pandemic forced lockdowns across the globe, there has been a dramatic increase in the use of digital technologies in various aspects of human life. Restrictions in mobility, closing of economic activities, and shutting down of education and health services have all led to people moving to digital platforms to stay connected with each other.

APAC Businesses Urged to Invest More in Digital Technology Philippines (October 27, 2020)

Businesses in the Asia-Pacific region are urged to continue investing in digital technology to survive and thrive amid the COVID-19 pandemic. During the Asia-Pacific Economic Co-operation (APEC) Business Advisory Council (ABAC) Philippines forum on digital innovation, Aboitiz Group president and chief executive officer Sabin Aboitiz stressed APECs main recommendation to member economies to improve technological infrastructure.

B.C. Still Hesitant to Adopt COVID Alert, The App Isn't Seen as Useful Yet Canada (October 27, 2020)

British Columbia's provincial Health Officer Dr Bonnie Henry is not ready to adopt Canada's COVID Alert app just yet, despite a record number of COVID-19 cases. Dr Henry told the media that there are some parameters built into the federal app that do not work which would cause more concern and frustration as witnessed in some other provinces.

Cybersecurity
As Consumers Shift Online, There Is Greater Need For Cyber Security Services  India  (November 4, 2020)

As the lines between digital and physical continue to blur, especially amid the COVID-19 pandemic, contactless payments and digital transactions have become the new norm. A report published by IBEF said that the Indian e-commerce market is growing at a steady pace and is expected to be valued at $200 billion by the year 2026. In the same report, it was stated that internet users in the country will increase to 829 million by the year 2021. While this sounds promising, the threat of cyber security is requiring immediate attention.


The COVID-19 pandemic seems to have ushered in a resurgence of state-backed hacking. The hacking was targeted at COVID-19-related data. In April 2020, security experts at Google sent 1,755 warnings to users whose accounts were targets of government-backed attackers. These hackers targeted business leaders in financial services, consulting, and healthcare around the world, including in the United States.


The Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Department of Health and Human Services issued a joint cybersecurity advisory (the Joint Cybersecurity Alert) to warn the healthcare sector that there is "credible information of an increased and imminent cybercrime threat to US hospitals and healthcare providers."

As Vaccine Work Starts, DRL Hacked  India  (October 24, 2020)

Dr Reddy's Laboratories (DRL) was the target of a cyber-attack less than a week after it received approvals to start Phase II and III trials of the Russian Covid-19 vaccine Sputnik V in India. Although the company refused to say if the hackers tried to steal vaccine-related data, the attacks have come at a time when Covid-19 vaccine developers across the world have been facing similar threats.

Proposed Legislation

PH Leads New Global Working Group on Data Privacy Policy Amid Pandemic  Philippines  (October 27, 2020)

The Global Privacy Assembly (GPA) has chosen the Philippines, represented by its National Privacy Commission (NPC), to lead a new working group in influencing global policy discussions on data privacy amid the COVID-19 pandemic.

Other Key Data Privacy Updates

Get Rid of Covid Posters Outside Homes: SC  India  (November 6, 2020)

The Supreme Court has frowned on the practice of pasting posters outside homes individuals infected with COVID-19 as it violated their right to dignity and privacy. The Delhi Government has agreed to do away with the practice as a bench of Supreme Court Justices have commented that the Centre must ensure it is discontinued in the entire country.


The Alabama Department of Public Health has launched a new COVID-19 dashboard that includes the number of positive cases among students and staff members in local school
systems. To protect individual privacy, systems reporting 1-4 new COVID-19 cases will show "<5" in the display, and those numbers will be included in the state level totals. In another effort to protect privacy, the dashboard does not narrow positive cases down to individual schools.

Privacy Concerns as South Australia Becomes Latest State to Flag QR Code Contact Tracing Australia (November 3, 2020)

A health technology expert has raised concerns about the privacy of consumer data as South Australia becomes the latest state to consider using QR codes for coronavirus contact tracing. However, South Australia COVID-19 State Coordinator and Police Commissioner Grant Stevens said consumer data from the scans would be "dumped" every 28 days and would be used for no other purpose than contact tracing.

Cybersecurity Post COVID-19: How to Ensure Safe Return to Work? India (November 2, 2020)

The COVID-19 pandemic has created many challenges for businesses across the globe. At first, it was employees working from home and the related cyber risks. However, as people adapt to the 'new normal', many are looking to make the transition back to the office and there are a new set of challenges to ensure a safe return to work. This article discusses steps organizations may wish to take to improve cybersecurity as employees return to the workplace.

Erie County's Reluctance to Identify COVID-19 Clusters Does a Public Disservice U.S. (November 1, 2020)

Erie County's Health Department, which reports to County Executive Mark Poloncarz, is maintaining its policy of keeping outbreaks of COVID-19 cloaked in secrecy. The Health Department claims in doing so it is abiding by the federal Health Insurance Portability and Accountability Act which protects the privacy of individuals from having personal health information disclosed. However, that does not mean public officials cannot identify an institution with many COVID-19 cases.

The QR Code Has Turned COVID-19 Check-Ins Into a Golden Opportunity For Marketing And Data Companies Australia (October 31, 2020)

Millions of Australians visiting cafes, restaurants, and pubs are unwittingly entering their COVID-19 check-in details into platforms owned by marketing companies. Privacy and cybersecurity experts are warning that the lack of due diligence in vetting providers has left the system and the "gold standard" personal data it manages vulnerable to exploitation.

Businesses' Collection of Information For COVID-19 Contact Tracing Raises Privacy Concerns For Customers Tasmania (October 28, 2020)

Business owners have called for the Tasmanian Government's assistance with the collection of information for contact tracing because of concerns over how companies can use people's personal details. Questions are being raised over the privacy of COVID-19 contact tracing at Tasmanian hospitality venues following allegations that personal information is being used for promotional purposes.