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**

**The Pandemic Also Generated Work in Digital Fields** U.S (March 9, 2021)

The COVID-19 pandemic generated a mandatory digitization in many sectors of the economy. While it represented difficulties for a large part of the population who lost their jobs, for others in technology-related areas, the situation represented a job opportunity.

**Four Global Trends Driving Post-Pandemic Business Recovery** South Africa (March 8, 2021)

Four trends have emerged as South African companies contemplate post COVID-19 recovery, including new thinking on talent and skills retention, embracing technology, incorporating sustainability in business models, and investing more in employee well-being, benefits, and engagement. These were the findings from the South African edition of Mercer’s Global Talent Trends 2020-2021 report.

**COVID-19 App Flaws Meant Pubs Broke Privacy Rules** U.K (March 4, 2021)

Pubs and restaurants were asked to carry out contact tracing calls to customers in breach of data protection rules, leaked documents reveal. Confusion within the Test and Trace system and failures of the £40 million COVID-19 app prompted desperate health officials to co-opt hospitality businesses into warning patrons about outbreaks despite it being unlawful.

**'No Use at All': Finnish COVID-19 Tracking App Criticized for Low Efficiency** Finland (March 3, 2021)

There have been few benefits from the Finnish smartphone-based COVID-19 tracking app, Coronablinker, according to experts surveyed by national broadcaster Yle. The app cost the state around $7.3 million to develop and gathered 2.3 million downloads in the country of 5.6 million people. About 12,000 people have used the app to report they tested positive for COVID-19.
Cybersecurity

The COVID-19 Vaccine and Privacy for Employees  Australia (March 10, 2021)

With the imminent introduction of the COVID-19 vaccine into workplaces across Australia, it is important for employers to know that their privacy obligations will extend accordingly to employee information related to the vaccine.

Worldwide Plans for Apps and Cards to Prove Your Vaccination Status: Are There Privacy Concerns?  Israel (March 6, 2021)

Israel's vaccine passport was released on February 21, 2021. Vaccinated people can download an app that displays their Green Pass when they are asked to show it. The app can also display proof that someone has recently recovered from COVID-19, which also allows passage. However, the Green Pass and other passport programs may also raise big privacy concerns.

Proposed Legislation

Coronavirus Bill Includes Nearly $2 billion to Secure and Improve Government Tech  U.S. (March 10, 2021)

The proposed Coronavirus Relief Bill was passed on the evening of March 10, 2021. It includes a $1.9 trillion coronavirus stimulus package that includes nearly $2 billion in funding to secure and improve aging government technology that has crippled efforts to disperse relief to struggling Americans. The legislation is the first coronavirus package to highlight cybersecurity as a key part of the economic recovery.

Surge in Cybercrime During the Pandemic Requires Response From Illinois  U.S. (March 8, 2021)

Small businesses in Illinois have had to move their operations increasingly online and remote in the past year, due to the COVID-19 pandemic, leading to a dramatic increase in cybercrime. State Rep. Keith Wheeler of Oswego believes the need for the Illinois government to act is more urgent than ever. Wheeler filed the Cyber Security Compliance Act, a bill that would ask businesses and state institutions in Illinois to create a cybersecurity program to safeguard personal information. Businesses that did so could then mount an affirmative defense to protect them against liability in any lawsuits resulting from acts of cybercrime

Other Key Data Privacy Updates


An individual who received his first COVID-19 vaccine had concerns that the consent form, which he signed, may have allowed his personal information to be sold or violated the Health Insurance Portability and Accountability Act (HIPAA). However, it has been confirmed that signing the COVID-19 vaccine consent form does not give the vaccination clinic, a coalition of local health care providers, the right to sell your personal information. The consent form allows organizations running the clinic such as WVU Medicine, Mon Health, and the Monongalia County Health Department, to access patient data and follow-up with the patients about the vaccine.
5 Ways The COVID-19 Pandemic Has Forever Changed Cybersecurity  Canada (March 4, 2021)

The COVID-19 pandemic has meant homes, rather than offices, have become workplaces but this shift to working from home creates new cybersecurity threats. This article discusses the five ways that cybersecurity has forever been altered.

Legalities of Monitoring Employees Who WFH  South Africa (March 3, 2021)

The COVID-19 pandemic has accelerated, and for some, cemented, the work from home trend. However, no employer wants to pay someone to watch television, or scroll through their social media while lying on the couch during work hours. As a result, many employers are increasingly turning to employee monitoring technology to replace the physical employee oversight once enjoyed in the office. The increasing suite of surveillance technology available to employers offers everything from allowing employers to view login times, measure keystrokes, track live locations, monitor, and track internet, email, and video, and take screenshots of employees' desktop throughout the day.

Ontario's Plans for COVID-19 Contact Tracing Wearable Devices Threaten Freedom and Privacy  Canada (March 3, 2021)

The Ontario government recently announced it had invested $2.5 million in wearable contact tracing technology to help curb the spread of COVID-19. These wristbands are being tested and considered for wide use in long-term care homes, a First Nation community, airlines, schools, and construction sites. They work by communicating with other devices through a combination of Bluetooth and Wi-Fi, sending an alert to any employee who has been in close contact with somebody who has tested positive for the virus. The wristbands also enforce social distancing by vibrating or beeping whenever they are within two meters of each other. However, these wristbands have not received the extensive level of public consultation compared to other contact tracing applications, thus raising concerns over transparency, privacy, and data security.

Israel's Supreme Court Bans Unlimited Mobile Phone Tracking of COVID-19 Carriers  Israel (March 1, 2021)

The Supreme Court of Israel has banned the government from sweeping use of mobile phone tracking of COVID-19 carriers, calling the measure a grave infraction of civil liberties. In its ruling, the court said it feared the mobile phone tracing, imposed as a temporary emergency measure, was slowly becoming permanent. It gave the government until March 14, 2021 to end indiscriminate use of the surveillance and limit it to confirmed COVID-19 carriers who refuse epidemiological questioning.

INAI Asks Not to Photocopy or Photograph Identifications of Those Who go to COVID-19 Vaccination  Mexico (March 1, 2021)

The National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) has called on health authorities and auxiliaries for the implementation of the national COVID-19 vaccination program to refrain from requesting a copy or photo of the voter's credential or any other means of identification of citizens who come to receive their dose. This new measure, among others, aims to reduce the possibility of citizens' personal data being misused and ensure the protection of personal data and the self-determination of all people during the vaccination process.

Close to 90% of Eligible Residents on TraceTogether  Singapore (February 27, 2021)

Close to 9 in 10 eligible residents have joined the Government's digital contact tracing program, despite a recent public backlash over privacy and trust issues. About 4.7 million
people have the TraceTogether app or have collected the TraceTogether tokens, and this has allowed the authorities to shave days off the contact tracing process. This update comes on the heels of a public outcry earlier in 2021 when it was revealed that TraceTogether data could be used for criminal investigations, despite earlier assurances that the data would be used solely for contact tracing.