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

Are COVID-19 Tracking Apps Effective or Dangerous? France (July 28, 2020)

Tracking applications have become a useful tool for many governments looking to mitigate and reduce COVID-19 contagion outbreaks, according to a study by the Massachusetts Institute of Technology. 50 governments around the world implemented such tracking apps, however analysts agree on the risks of using these applications in terms of privacy.

Data-Privacy Challenges for California COVID-19 Contact-Tracing Technology United States (July 27, 2020)

Developers, governments, and regulators must work with the cybersecurity industry to apply rigorous standards to contact-tracing apps to make sure that the societal impact of COVID-19 doesn't extend into personal privacy.

Officials Use Uber Data to Track COVID-19; Public Health Units Seek Rider Information Canada (July 22, 2020)

Ten Canadian public health units have made a total of 145 requests for data from Uber since the ride-hailing giant launched a tool that lets health officials quickly access personal information on riders and drivers who may have come in contact with someone infected.

Western Cape Has Piloted COVID-19 Track-and-Trace System South Africa (July 20, 2020)

The Western Cape has piloted a national track-and-trace system that will soon be launched by the national government. However, the national Department of Health says that at present nobody is being digitally monitored by the state.
**4 Tech-driven Approaches to Flatten the Curve On COVID-19** United Kingdom (July 17, 2020)

A Digital Data Capture and Management System can increase surveillance and detect cases promptly. This would provide an effective response for contact tracing, rapid diagnosis and vaccine monitoring.

**Cybersecurity**

**Why Businesses Need to Focus on Cybersecurity** UAE (July 31, 2020)

The current pandemic has exposed existing vulnerabilities in systems and created new cybersecurity dangers as work forces connect to corporate networks remotely, share data and access applications in the cloud.

**SMEs Appear Ill-Prepared for Greater Risks of Cyberattacks as Online Workforce Rises** Singapore (July 29, 2020)

Small and medium-sized enterprises face greater risks of cyber-attacks and data breaches than they realize, as more of their employees work from home during the pandemic.

**Eat Out to Help Out Scheme Prompts GDPR Fears** United Kingdom (July 29, 2020)

A data company has warned hospitality venues to ensure their track and trace systems are watertight before the government's Eat Out to Help Out scheme starts next week.

**A New Privacy Headache: Virginia’s COVID-19 Workplace Safety Rule is Poised to Impact Privacy** United States (July 27, 2020)

Virginia's Safety and Health Codes Board adopted an emergency regulation designed to establish requirements for employers to control, prevent and mitigate the spread of the virus.

**COVID-19 and COPPA: Children’s Internet Privacy in a New, Remote World** United States (July 27, 2020)

For many businesses, engaging children online may be a new frontier, and one in which they are unwittingly wading into regulated waters for the first time. Online services directed to children under 13 years old are regulated by the Children's Online Privacy Protection Act.

**Proposed Legislation**

**Alabama Bill Would Provide COVID-19-Related Privacy Protections** United States (July 27, 2020)

A proposed Alabama state Senate bill would provide privacy protections for individuals who have tested positive for COVID-19 and others whose personal information is being collected through contact tracing.

**COVID-19 Inspires Federal Consumer Privacy Act** United States (July 17, 2020)

As mobile device and other monitoring services are being considered for employers and retail, because of the COVID-19 pandemic, the U.S. Senate announced a bill, which would apply to the collection of American health, geolocation, and proximity information.
Other Key Data Privacy Updates

Hackers Quickly Adopt COVID-19 Parlance United States (July 28, 2020)

Cyber security experts, who studied cyber threats as the viral infection broke out, found that the situation offers a fertile ground for cyber breaches as organisations and people took to digital platforms to carry on businesses and even did day-to-day purchases online.

COVID-19 Contact Tracing Scams United States (July 25, 2020)

With state and local governments reducing restrictions on business operations and public gatherings during the COVID-19 pandemic, their public health strategy often relies on robust contact tracing to help slow the spread of the disease by informing people who have had contact with someone who has tested positive. However, scammers can take advantage of this vital information tracking to prey on consumers.

Remote Workers, SMMEs, Health Sector More at Risk of Cyber Threats South Africa (July 24, 2020)

The COVID-19 pandemic and lockdown has created new vulnerabilities that fraudsters and cyber criminals have been quick to exploit. Top targets for fraud and cybercrime include home users, SMMEs and the health sector. Home users were particularly vulnerable because remote working users were seemingly more relaxed at home than they were at the office, following the notion that cyber-attacks only happen at the office.

Privacy Concerns Linger Over COVID-19 App Ireland (July 23, 2020)

The new COVID-19 contact tracing app in Ireland has been a major success but it has also raised questions about data privacy. Researchers at Trinity College Dublin have raised concerns about the data collected by the Android system using a piece of software that runs in the background on users' phones, known as Google Play Services.

Cybercriminals Exploiting the Pandemic Through COVID-19 Themed Malicious Apps, Phishing Campaigns, And Malware India (July 22, 2020)

There has been an average of 375 new threats per minute and a surge of cybercriminals exploiting the pandemic through COVID-19 themed malicious apps, phishing campaigns, malware, and more, according to McAfee's COVID-19 Threat Report: July 2020. The report examined cybercriminal activity related to COVID-19 and the evolution of cyber threats in Q1 2020.