THOMSON REUTERS®

DATA PRIVACY ADVISOR

COVID–19 Data Privacy Global News Coverage

July 17, 2021 – August 13, 2021

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

New York Vaccine Passport Reignites Online Privacy Debate U.S. (August 5, 2021)

New York announced it will soon require people to prove they have had at least one COVID-19 vaccine dose to enter companies. Vaccine passports, often in electronic form, will then show proof of vaccination. For months these records, also known as health passes or digital health certificates, have been discussed around the world as a tool to allow vaccinated people at less risk of COVID-19 to meet safely. But normalizing these credentials could also bring about an era of greater digital surveillance, according to privacy researchers. This is because vaccine passes can allow location tracking, while there are few rules on how personal vaccination data should be stored and can be shared. Existing privacy laws limit information sharing between healthcare providers, but there is no similar rule for when people enter their own data into an app.

Biometrics and BIPA Claims in Academic Testing U.S. (July 30, 2021)

COVID-19 accelerated digital transformations across every industry. From the growth of e-commerce and food delivery services to virtual workspaces and online learning, a seismic shift towards digitalizing day-to-day activities has become the new normal. One industry that proliferated across the country during the era of online learning has been online testing and proctoring services. Such online testing provides flexibility to academic institutions in administering exams; however, the collection of biometric data through online testing platforms potentially opens the doors to a litany of privacy concerns.

AI System to Detect Social Distancing Breach Australia (July 29, 2021)

Researchers developed and tested an AI video surveillance system that can detect social distancing breach in an airport. Due to COVID-19, there is an increasing demand for the technologies that can help ensure the protocols are being followed. Researchers from Griffith University have developed an AI video surveillance system that can detect social distancing breaches in an airport without compromising privacy of the travellers.

COVID-19 Apps in Colombia Moved from Tracking to Social Control Columbia (July 24, 2021)

During 2020, President Duque issued two declarations of a state of health emergency seeking to overcome the COVID-19 crisis. In addition, in a period of four months in the country not only did Coronapp emerge, an application that had the purpose of helping to detect areas and people affected by COVID-19, but other local platforms such as Medellín Me Cuida, Valle Corona and Bogotá Cuidadora. Although it is still too early to know if they played any role in reducing cases, a report by the Karisma Foundation indicates that they became more than an epidemiological tracking system; they became a tool of social control. The report found that the apps were disconnected from health authorities, so they were not effective, and that some ended up monitoring people's lives.

Cybersecurity

Cybersecurity May Stall Smartphone Vaccine Verification App Adoption, Harris Poll Shows U.S. & U.K. (August 7, 2021)

Anomali, the leader in intelligence-driven cybersecurity solutions, recently published its latest survey conducted by The Harris Poll. More than 2,000 adults in the U.S. and 1,000 in the U.K. revealed their cybersecurity fears related to COVID-19 digital vaccination cards. Key findings included 80% in the U.S. and 76% in the U.K. have cybersecurity concerns. 64% in both countries expect that digital vaccination cards will lead to a cyberattack causing "moderate to major" disruption to business, government, and consumers. Only 45% of Americans and 54% of Brits say they are very "likely" to use digital vaccination cards if they become a requirement for certain activities.

The Rise of Cyber Risks in the Healthcare Sector and How to Stay Protected U.S (August 3, 2021)

The healthcare sector has always been a targeted source for cybercrime. Hackers have several reasons for wanting to get into healthcare systems. Some want to disrupt the operation of services, while others want to steal medical records or financial information. Since the COVID-19 pandemic took the industry by storm in 2020, it's no surprise that cyberattacks targeting the healthcare sector have been on the rise. Unfortunately, most healthcare systems are relatively simple for cyber-attackers to gain access to due to various lapses in security.

Vaccination Status Questions Do Not Violate HIPAA, Consumer Health Expert Explains U.S. (August 1, 2021)

Recently, Georgia Congresswoman Marjorie Taylor Greene and Dallas Cowboys quarterback Dak Prescott declined to answer questions about their vaccination status, citing the Health Insurance Portability and Accountability Act that created standards to protect sensitive patient information.

Evolving cybercrime and data security challenges India (July 30, 2021)

Cybercrime has rapidly evolved, with newer forms of threat vectors plaguing many businesses. While companies and governments have amped up their preparedness to tackle this menace, the incidents are still rising. In the 16th edition of the World Economic Forum's Global Risks Report 2021, cybersecurity alongside COVID-19 pandemic, climate change and debt crisis were a key threat for the next decade. The report ranks India third after the US and the UK when facing major cyberattacks during 2006-2020. While the pandemic weakened the existing cybersecurity frameworks of many organizations, the frequency and sophistication of cyberattacks further affected the cybersecurity infrastructure of several businesses.

ICO publishes further update to its regulatory approach during the pandemic UK (July 28, 2021)

The updated document includes minor amendments and a change in emphasis from the ICO on the importance of fully complying with the rights of individuals to information under data protection and freedom of information laws. There is a raised expectation for organizations to get to grips with reducing any backlogs of complaints received from members of the public relating to their information rights, within a reasonable period.

Other Key Data Privacy Updates

CCPA Compliance Concerns for Employers as California Employees Return to the Workplace U.S. (August 10, 2021)

As California reopens from the COVID-19 pandemic and workers begin returning to work in-person, many employers have begun requesting their employees provide, sometimes on an ongoing basis, certain health information before returning to the workplace. This includes information such as temperature checks, health surveys, COVID-19 test results, or proof of vaccination status. Given the likelihood that collecting this information will trigger certain requirements under the California Consumer Privacy Act (CCPA), employers should take certain measures to ensure they remain in compliance with the CCPA as their workplaces reopen.

'All Options on Table' for Jab Passport Australia (August 9, 2021)

New South Wales has called for a national -approach to protect businesses that try to force employees and customers to be vaccinated against COVID-19. Health Minister Brad Hazzard has said that while it was possible, he could use state public health orders to override privacy legislation and allow disclosure of a person's vaccination status, the federal government should take the lead at this stage. The reach of the federal Privacy Act is central to whether a "vaccination passport" can be enforced by retailers and other companies and whether employers can require staff to reveal if they have had a jab.

National Privacy Commission Says Suspending Data Privacy Rules Won't Boost Contact Tracing Efforts Philippines (August 6, 2021)

The National Privacy Commission (NPC) has a written a letter to the Employers Confederation of the Philippines (ECOP), criticizing the business group's request to suspend data privacy rules for contact tracing. ECOP President Sergio R. Ortiz-Luis Jr. has been recommending that the government identify people who have tested positive for COVID-19, encouraging close contacts to disclose exposure, and minimizing government spending on contact tracing. However, NPC Commissioner Raymund E. Liboro said there is no scientific basis supporting the premise that suspending provisions of the law would be an effective anti-pandemic measure.

Data Privacy in China: Zhejiang Province Proposes Rule to 'Destroy' Personal Data Collected During Emergencies China (August 5, 2021)

China's eastern province of Zhejiang, which is leading the country in applying big data technology to administration, has drafted rules stipulating that personal data collected during a public emergency should be either "sealed" or destroyed after use, a decision that would put certain checks on government agencies.

The Ministry of Health Leaks the Private Data of More Than One and a Half Million Ecuadorians Ecuador (August 1, 2021)

Measures against COVID-19 have hit people's health, economy, and freedom, but in Ecuador it has gone a step further, it has also bypassed privacy. More than one and a half million people had their first and last names exposed, where they live (parish of address), id number (identification), telephone, profession, ethnic self-identification, date of birth, medical history number, medical diagnosis (regardless of whether they were positive or not) and other private data, after having been tested for COVID-19.

The COVID-19 Vaccination and Privacy Rights New Zealand (July 29, 2021)

The vaccine is an essential part of New Zealand's response to COVID-19 and there is significant interest in the immunisation programme. This interest often has privacy implications. A person's vaccination status is personal information and so falls under the protections laid out in the Privacy Act 2020. However, there are limited situations where an employer can ask for the vaccination status of an employee where they have a legitimate need to know. Justifiable reasons to ask for this can include a legitimate health and safety concern, or where certain roles must be performed by a vaccinated worker, such as staff at an MIQ facility.

The Balancing Act Between Employers' Legitimate Interest to Monitor Employees and Employees' Right to Data Privacy European Union (July 29, 2021)

As a result of COVID-19 many businesses have been compelled to shift their workforce to operate remotely from the safety of their own homes. With this transition in mind, employers had to seek alternative ways aimed at ensuring the uninterrupted productivity of employees working outside the employer's appointed premises. There are multiple tools which enable employers to exercise a level of oversight over the employees' activities when working remotely, less invasive technologies include simple monitoring of connection to Virtual Private Network (VPN) and/or by accessing computer usage. However, more draconian measures, such as installing location determination devices, video surveillance through the employees' webcams, might raise certain legal questions.

Can Employers Require Their Staff to Be Vaccinated Against COVID-19? Malta (July 29, 2021)

Amid a third wave of the COVID-19 pandemic, with vaccines being hailed as the only way to control the rising number of positive cases, a common question that is often asked is whether employers can request their staff's personal data in relation to their vaccination status, and whether/how the employer can store such personal data. The Office for the Information and Data Protection Commissioner (the 'IDPC') has published guidelines on the data protection aspects related to the collection of employees' COVID-19 vaccination status (the 'Guidelines'). This article will briefly explain the Guidelines and shall attempt to answer certain questions which should be on every employer's mind.

Vaccine Passports Have Precedent Canada (July 29, 2021)

When the premier, the health minister and other provincial officials discuss their reluctance to require people to show proof of COVID-19 vaccination to attend sports, concerts, and so on, they often cite "privacy" as an issue. It isn't. There's a well-established, global precedent for vaccine passports. Many countries require travellers to be vaccinated against diseases such as Yellow Fever, and proof of such protection is provided via the Yellow Card, the certificate of vaccination introduced by the International Sanitary Convention in 1944 and administered today via the World Health Organization. This vaccine passport is universally accepted, and has been for almost eight decades, because it has saved literally

millions of lives and prevented potential pandemics by controlling the transmission and spread of deadly diseases.

Remote Working and Data Protection: A Pandemic Year in Review U.S. (July 19, 2021)

The COVID-19 pandemic caused a massive shift toward remote working in 2020. Generally, this shift was smoother than expected, with most companies indicating that the transition to working from home had been successful and productivity had remained the same or improved during the pandemic. The transition, however, also presented several challenges, particularly in the fields of data protection and privacy.