Katten Privacy, Data and Cybersecurity *Quick Bytes*
Issue 1 | January 2023

Editor's Note: Welcome to the inaugural issue of Katten's Privacy, Data and Cybersecurity *Quick Bytes*. Each month, *Quick Bytes* will highlight the latest news and legal developments involving privacy, data and cybersecurity issues across the globe.

You Meta Believe the GDPR Penalties Are No Joke!

By Sarah Simpson and Tegan Miller-McCormack

On 4 January 2023, Meta Ireland Limited (Meta Ireland) was fined €390 million (€210 million in respect of Facebook and €180 million in respect of Instagram) by the Irish Data Protection Authority (Irish DPA) and has been directed to bring its data processing operations into compliance within a period of three months of the decision. Meta Ireland was slapped with these eye-wateringly high fines because it failed to comply with its obligations found at the heart of the EU General Data Protection Regulation (GDPR), specifically that personal data must be processed lawfully, fairly and in a transparent manner, for a suitable legal basis.

The Irish DPA undertook their investigation into Meta Ireland as a result of two complaints filed on 25 May 2018 (the day the GDPR came into force!). It concluded its investigations, but following disagreements between Concerned Supervisory Authorities around the initial draft decision, the European Data Protection Board (the EDPB) issued binding determinations on the matter. The final decision issued concluded that (i) Meta Ireland had not provided sufficient clarity to users around what processing operations were being carried out on users' personal data, for what purposes and on what legal basis; and (ii) Meta Ireland was not entitled to rely on the "contract" basis for processing personal data for the purposes of behavioral advertising.

Interestingly, the EDPB additionally directed the Irish DPA to conduct a new investigation into all of Meta Ireland's processing operations and use of special category data. However, there are questions around whether the EDPB has jurisdiction to instruct and direct an authority to engage in an "open-ended and speculative investigation". It is yet to be seen for Meta whether this is all over, or whether they need to prepare for further investigations and top up their rainy day pot for possible future fines!

Financial Institutions Require More Oversight of Cybersecurity Risk under NYDFS

By Trisha Sircar

The New York Department of Financial Services (NYDFS) in November 2022 published a proposal to amend its cybersecurity rules, which will require regulated companies to notify the

NYDFS of a third-party cybersecurity incident within 72 hours.

A draft version of the proposal released earlier in 2022 required financial institutions to notify regulators about such incidents within 72 hours. This newer proposal includes this notice requirement, along with an amendment that notice be provided to NYDFS within 24 hours of making a ransom payment to hackers. Furthermore, financial institutions will be required to outline why a ransom payment was necessary, which alternatives were considered, and how federal sanctions implications were assessed.

In addition, the proposals mandate boards of directors at financial institutions to have more oversight into the organization's cybersecurity risks. Boards at banks, insurance companies, and other financial institutions meeting a certain size threshold, will be required to approve cyber policies. Also, financial institutions will have to disclose whether their boards have expertise to oversee cybersecurity risks or identify if they will rely on outside consultants. These mirror the proposed requirements from the Securities and Exchange Commission (SEC). *Read NYDFS Press Release.*

Complaint Brought Against Massachusetts for Installing Covid App Tracking Software Collecting Location and Health Data

By Trisha Sircar

On November 14, 2022, Massachusetts residents Robert Wright and Johnny Kula filed a proposed class action lawsuit in the US District Court for the District of Massachusetts against the Massachusetts Department of Public Health and the Commissioner of the Massachusetts Department of Public Health, alleging that they illegally installed Covid-19 tracking software on over one million Android phones without owner permission to collect location and health data.

According to the complaint, the Massachusetts Department of Public Health worked with Alphabet Inc.'s Google to install the exposure notification software via Android phone settings. The plaintiffs allege that the contact tracing app was automatically installed without warning to collect location and health data in violation of the Fourth and Fifth Amendments to the US Constitution, violation of Article X and Article XIV of the Massachusetts Declaration of Rights, violation of the Computer Fraud and Abuse Act, common law trespass to chattels, ultra vires government action, unauthorized access to computer systems and invasion of privacy.

The potential class size is estimated to be over one million individuals. The plaintiffs are seeking $1 in damages and injunctive relief to prevent further installations of the app without permission and uninstall the app from Androids with nonconsenting users.

Importing BIPA to New York: Biometric Law Enforcement on the Horizon

By Geoffrey G. Young, Charles A. DeVore, Trisha Sircar and Christopher T. Vazquez

In an article published by the *New York Law Journal*, partners Geoffrey G. Young, Charles A. DeVore, Trisha Sircar and associate Christopher T. Vazquez discuss the increasing influence of the Illinois Biometric Information Privacy Act (BIPA) and what the law means for New York. In the article, the attorneys review the history of BIPA, the patchwork of laws developing across the country, and recent cases, including a $228 million verdict in a case alleging violations of the Illinois' groundbreaking 2008 law.

The authors explain why companies using and relying on biometric technologies need to be paying close attention to developments; the continuing rise in biometric technology use has prompted lawmakers to focus more on regulation and led to an increase of private rights of action. The article discusses the state of New York City's biometric privacy law. It also reviews statewide legislation that would set a standard of care for handling information and mirrors the Illinois BIPA private right of action and damages scheme. *Read "Importing BIPA to New York:*

Biometric Law Enforcement on the Horizon." (Learn more about Katten's Biometric Litigation practice.)

California Consumer Privacy Act's Employee and B2B Exemptions to Expire on January 1, 2023

By Trisha Sircar, Jose Basabe, Catherine O'Brien and Rachel Schaub

The California Consumer Privacy Act (CCPA) is California's groundbreaking legislation that seeks to give California consumers certain rights over how a business handles "personal information" collected about its consumers. On October 11, 2019, California Governor Gavin Newsom signed AB 25 into law, which provided businesses with temporary relief by exempting personal information that is collected in certain employment contexts and in a business-to-business (B2B) context from the scope of the CCPA until January 1, 2021. As previously reported, Governor Newsom signed AB 1281 into law on September 29, 2020, providing a one-year extension to the partial employee and B2B exemptions to January 1, 2022, applicable only in the event that the California Privacy Rights Act (CPRA) ballot initiative failed. When the CPRA was approved during the 2020 election by California voters, the exemptions were extended one final time to January 1, 2023. On August 31, 2022, the California legislature adjourned without extending the exemptions, which automatically expire on January 1, 2023 in conjunction with the CPRA effective date. *Read Katten's full advisory.*

December 9 Looms as Compliance Date for Private Investment Funds and Certain Investment Advisers to Comply With New Cybersecurity Requirements

By David Dickstein, Vlad Bulkin, Wendy Cohen, Richard Marshall, Trisha Sircar, Allison Yacker and Lance Zinman

As discussed in our March 3, 2022 Advisory, on October 27, 2021, the Federal Trade Commission (FTC) announced revisions (the 2021 Revisions) to its information "Safeguards Rule" (the Rule) adopted under the Gramm-Leach-Bliley Act (GLBA). The Rule was first enacted in 2002 to ensure that financial institutions under the jurisdiction of the FTC protect nonpublic personal information (NPI) of their natural person clients and investors (each, a Customer). Financial institutions under the FTC's jurisdiction include private investment funds (Private Funds) and ***any investment advisers that are not registered with the Securities and Exchange Commission (SEC) such as state registered investment advisers***. The 2021 Revisions were adopted in response to the significant harm caused to consumers, including monetary loss, identity theft and other forms of financial distress as a result of data breaches and other cybersecurity concerns.

The 2021 Revisions became effective on December 9, 2021, with an initial compliance date of December 9, 2022, for most substantive changes. However, for various reasons, including lack of personnel and supply chain equipment issues, on November 15, 2022, the FTC extended the compliance deadline until June 9, 2023 for several aspects of the 2021 Revisions. Nonetheless, the compliance date for other aspects of the 2021 Revisions remains December 9, 2022. Below are the 2021 Revisions for those requiring compliance by December 9, 2022 and for those which compliance was delayed until June 9, 2023. *Read Katten's full advisory.*

Looking Ahead to 2023

By Christopher Hitchins, Brigitte Weaver and Emma Williams

There have been discussions regarding the potential replacement of the UK General Data Protection Regulation (GDPR). If enacted, the Data Protection and Digital Information Bill would amend the current data protection and privacy framework.

The Information Commissioner's Office (ICO) is currently consulting on monitoring at work and information about workers' health. Both consultations close in January 2023. It will be interesting

to see whether the ICO implements any changes to its guidance based on the consultation responses. *Read Katten's full advisory.*

CONTACTS

For questions about developments in the Privacy, Data and Cybersecurity industry, please contact the following Katten attorney.

Trisha Sircar

Partner, Co-Privacy Officer
Quick Bytes Editor
vCard