AN A.S. PRATT PUBLICATION
MAY 2022
VOL. 8 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 4** **May 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [113] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Current Developments

*By Sharon R. Klein, Alex C. Nisenbaum, Harrison M. Brown, Nicole Bartz Metral and Karen H. Shin**

STATE AND LOCAL LAWS AND REGULATIONS

By Karen H. Shin

Flurry of State Comprehensive Laws Introduced

States continue to introduce and consider comprehensive privacy laws in their 2022 legislative sessions. Indiana, Oklahoma and Florida are currently in the running to becoming the fourth state to enact a comprehensive privacy law, after California, Virginia and Colorado. Indiana's Senate unanimously passed its privacy bill[1] and the Oklahoma House of Representatives passed the Oklahoma Computer Data Privacy Act.[2] Meanwhile, a Florida comprehensive privacy bill[3] with a private right of action has become eligible for a vote on the house floor.

The Wisconsin Assembly greenlit its privacy bill,[4] but it is unclear whether the Wisconsin Legislature will complete its work on the bill before its March deadline for consideration on the floor. The Massachusetts Senate's Joint Committee on Advanced Information Technology, the Internet and Cybersecurity advanced the Massachusetts

---

* Sharon R. Klein (sharon.klein@blankrome.com) is a partner at Blank Rome LLP advising businesses on risks related to the privacy and security of personal data, ownership, and commercialization of data artificial intelligence; planning, drafting, and implementing privacy, security, and data protection policies and "best practices"; compliance with global, federal, and state privacy and security laws, regulations, and rules; data governance; and breach response, crisis management, and remedies for non-compliance. She is certified as an information privacy professional by the International Association of Privacy Professionals. Alex C. Nisenbaum (alex.nisenbaum@blankrome.com) is a partner at the firm advising clients on data privacy and information security laws and regulations, including compliance with HIPAA/HITECH; Gramm-Leach-Bliley; the California Consumer Privacy Act; cross-border data transfer; and state privacy, data protection, and breach notification requirements. Harrison M. Brown (harrison.brown@blankrome.com) is an associate at the firm whose practice encompasses a range of business litigation and class action defense, with an emphasis on consumer fraud and privacy claims. Nicole Bartz Metral (nicole.metral@blankrome.com) is an associate at the firm focusing on complex corporate and commercial litigation in both state and federal courts. Karen H. Shin (karen.shin@blankrome.com) is an associate at the firm focusing on a range of data privacy and information security matters, including compliance with various privacy laws and regulations.

[1] http://iga.in.gov/legislative/2022/bills/senate/358/#document-94d6d82c.

[2] http://www.oklegislature.gov/BillInfo.aspx?Bill=hb1602&Session=2200.

[3] https://www.myfloridahouse.gov/Sections/Bills/billsdetail.aspx?BillId=76556.

[4] https://docs.legis.wisconsin.gov/2021/proposals/reg/asm/bill/ab957?mkt_tok=MTM4LUVaTS0wNDIAAAGCdF0H5CwHlkuM5bTkDaZXW38ZOPVvWiUSJh1VRJwcWllAXHgeuf5-65SFuaBIJmsG_4xKSqj9D2PtIM5tydPJ5McnbnXAc_CucU-VdzTssBqx.

Information Privacy and Security Act,[5] the Alaska House of Representatives advanced the Alaska Consumer Data Privacy Act,[6] and the Ohio House Government Oversight Committee advanced its privacy bill.[7] Arizona,[8] Connecticut,[9] Iowa,[10] Maine,[11] and Utah[12] all introduced their respective privacy bills. At least 24 states are now considering comprehensive privacy legislation.

California Legislature Introduces Age-Appropriate Design Code Act

The Age-Appropriate Design Code Act[13] ("AB 2273") was introduced in the California Assembly. Modeled on the UK's Age Appropriate Design Code,[14] AB 2273 would require businesses that provide goods, services, or product features that are likely to be accessed by a child under the age of 18 to consider the "best interests of [the child]" when designing, developing, and providing such services and products over the business' commercial interests.

AB 2273 also requires covered businesses to maintain the highest level of privacy possible for children by default and use age-appropriate language in its terms of service and privacy policies and prohibits collecting and retaining such information that is not necessary to provide the business' products or services. If passed, the law would go into effect on July 1, 2024.

California Legislature Introduces Bills to Extend Employee and B2B Information Exemption under the CCPA/CPRA

Two bills (AB 2871[15] and AB 2891[16]) were introduced in the California Assembly that propose to extend the exemption for employee and business-to-business ("B2B")

---

[5] https://malegislature.gov/Bills/192/S2687.

[6] http://www.akleg.gov/basis/Bill/Detail/32?Root=HB%20159.

[7] https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA134-HB-376.

[8] https://apps.azleg.gov/BillStatus/BillOverview/77859.

[9] https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?InMyBill=True&selBillType=Bill&bill_num=SB00006&which_year=2022&UID=jduball@iapp.org&mkt_tok=MTM4LUVaTS0wNDIAAAGCg8zkEpwbvU_OqbpzY09M6pYqYPxBQWdeq-LvDHxiX9ekWskGxGaeguRRhrBAzZoSqrkfIgaybXyGCT7LNjEH3y3Ilt3v_lo7YHSf5SPPyHXc.

[10] https://www.legis.iowa.gov/legislation/BillBook?ga=89&ba=HSB674&mkt_tok=MTM4LUVaTS0wNDIAAAGCg8zkE9DC7YOhw4mAM9ucp4DGPPCtTEVy5e0_JbM3rc8Oo5zFz9a-Hi4irdjDHd_MlL54yVhWuTE1ROQq7lEZrbHBdeEYsrERMJ5B-_xlMFhQ.

[11] https://legislature.maine.gov/LawMakerWeb/summary.asp?ID=280082811.

[12] https://le.utah.gov/~2022/bills/static/SB0227.html?mkt_tok=MTM4LUVaTS0wNDIAAAGCwaMCtD9PQNVX_LhSMTNpiAQkpTxPAI_dwt3OHOaS7nD6EbiDWmQjZTc4tTlvRZUE98ceD2uC6meyH16-hhJSP1Ul7iCdxPOj7QSvERBsvfgW.

[13] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

[14] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/information-commissioner-s-foreword/.

[15] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2871.

[16] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2891.

information currently provided under the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"). Currently, personal information collected in the employment and B2B contexts are exempted from the CCPA, except with respect to its private right of action and, for employee information, notice obligations. AB 2871 proposes to extend these exemptions indefinitely, while AB 2891 proposes to extend these exemptions until January 1, 2026. If passed, the bills may be challenged as inconsistent with the purpose and intent of the CPRA. The CPRA was approved as a referendum by California voters and the California Constitution only allows the California Legislature to amend a statute passed by referendum if the statute permits. While the CPRA does so, the CPRA further requires that the amendments be consistent with and further the purpose and intent of the CPRA.

California Legislature Introduces Biometric Privacy Law

The California Legislature introduced a biometric privacy law[17] ("SB 1189") similar to the Illinois Biometric Information Privacy Act ("BIPA"). SB 1189 would broaden the definition of biometric data under California law to include a person's physiological, biological, and behavioral characteristics used to establish individual identity. SB 1189 would supplement the CCPA/CPRA, but would cover any "private entity" ("an individual, partnership, corporation, limited liability company, association, or similar group, however organized" but does not include University of California) and requires companies to provide notice to consumers and obtain a consumer's consent prior to collecting information. SB 1189 includes a private right of action, which would certainly fuel significant litigation like its BIPA counterpart. If enacted, SB 1189 would go into effect January 1, 2023, potentially putting significant time pressure on companies doing business in California to prepare biometric privacy compliance programs before the end of the year.

CPRA Regulations Delayed

California Privacy Protection Agency ("CPPA") Executive Director Ashkan Soltani indicated in a CPPA public meeting that formal rulemaking proceedings will continue into the third quarter of 2022 with rulemaking likely to be completed in the third or fourth quarter of 2022. The CPRA provides a deadline of July 1 for regulations to be finalized. With regulations expected to be extensive, companies may have a short time following release of final regulations to adjust compliance programs to account for regulatory requirements. The CPPA made no announcement regarding a delay in enforcement activity as a result of the delayed rulemaking process.

[17] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB1189.

Florida Considers Amendments to Mini-TCPA

Lawmakers in Florida are currently considering legislation to amend the state's Telephone Solicitation Act ("FTSA"). The Senate bill would change the statute's definition of an autodialer to be more consistent with the definition under the federal Telephone Consumer Protection Act ("TCPA"), making click-to-dial and human-selection systems permissible. However, a recent amendment to the House bill conflicts with the Senate's proposed definition and would prohibit the use of such systems. In the absence of clarifying legislation, class action lawsuits under the FTSA, especially ones focusing on text message systems, have continued to pile up. Businesses are advised to consult counsel and ensure that there are procedures in place for obtaining prior consent before using any new system to make calls, text messages, or ringless voicemails to persons in Florida.

Oklahoma Introduces Mini-TCPA Legislation

Lawmakers in Oklahoma are currently considering the Telephone Solicitation Act of 2022.[18] The Oklahoma bill mimics Florida's mini-TCPA law. The Oklahoma bill aligns its definition of an autodialer with the generally accepted interpretation of an autodialer under the federal TCPA as it was before the U.S. Supreme Court clarified and substantially narrowed the definition in *Facebook, Inc. v. Duguid.* The Oklahoma bill recently advanced out of a House committee by a unanimous vote. If passed, the Oklahoma legislation would become effective in November 2022.

Washington and Georgia Consider Changes to "Do Not Call" Laws

Lawmakers in Washington and Georgia are considering changes to their Do Not Call ("DNC") laws which would increase penalties and make violations enforceable by private litigation. The Washington House of Representatives is reviewing a bill that would amend the state's Commercial Electronic Mail Act ("CEMA") by doubling penalties to $1,000 and providing a private right of action. In addition, the bill would redefine the current definition of an automatic dialing and announcing device by making it broader and specifically prohibiting ringless voicemails. In Georgia, a recently passed Senate bill would authorize a private right of action for violation of its DNC law. Moreover, the Georgia bill specifically removes as an affirmative defense that the defendant did not make the call or was not aware that such call was in violation of the statute, if such call was made by a vendor on behalf of the defendant, effectively making businesses liable for rogue callers.

[18] http://www.oklegislature.gov/BillInfo.aspx?Bill=HB3168&Session=2200&Tab=0.

FEDERAL LAWS AND REGULATIONS
By Sharon R. Klein

U.S. Senate Homeland Security Committee Reintroduces Legislation on Reporting Cybersecurity

The U.S. Senate's Homeland Security Committee re-introduced the Strengthening American Cybersecurity Act of 2022[19] ("SACA"), which requires critical infrastructure operators to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency ("CISA") no later than 72 hours after the incident is reasonably believe to have occurred and within 24 hours of any ransomware payment being made. Critical infrastructure operators must also continue to submit supplemental written reports with any updates on the incident until the incident has been fully mitigated and resolved. Additionally, SACA attempts to update the cybersecurity guidelines within the Federal Information Security Modernization Act, which has not been amended in seven years. SACA further codifies the General Services Administration's Federal Risk and Authorization Management Program ("FedRAMP"), which aims to certify the security of cloud products and services used by federal agencies.

Federal Legislation Introduced to Study Modernization of Health Data Privacy Laws

The Health Data Use and Privacy Commission Act[20] was introduced in the U.S. Senate. The Act would establish of a commission in charge of providing recommendations to Congress about updates to health-related privacy laws. The introduction of this Act would consider, among other things, whether laws are needed to regulate health-related apps that allow individuals to create and share health data. The Health Insurance Portability and Accountability Act ("HIPAA") only covers health data created and maintained by covered entities such as healthcare providers and payers.

SEC Proposes Cybersecurity Rules for Investment Advisers and Funds

The Securities and Exchange Commission ("SEC") voted to propose rules[21] related to cybersecurity risk management for registered investment advisers, registered investment companies, and business development companies. The proposed rules would require advisers and funds to adopt and implement written cybersecurity policies and procedures, report significant cybersecurity incidents to the SEC, and comply with new recordkeeping requirements designed to improve the availability of cybersecurity related information and facilitate SEC inspection and enforcement. The proposed rule would also require advisers and funds to publicly disclose cybersecurity risks and significant

[19] https://www.govinfo.gov/app/details/BILLS-117s3600pcs.
[20] https://www.congress.gov/bill/117th-congress/senate-bill/3620?s=1&r=2.
[21] https://www.sec.gov/rules/proposed/2022/33-11028.pdf.

cybersecurity incidents that occurred in their last two fiscal years in their brochures and registration statements.

NIST Seeks Input on Updates to Cybersecurity Framework

The National Institute of Standards and Technology ("NIST") has issued a request for information[22] to gather information about evaluating and improving resources for the NIST Cybersecurity Framework ("CSF"). The CSF is one of the leading information security frameworks for private sector cybersecurity programs, and NIST's goal for revising the CSF is to keep the CSF current and align it with other tools that are commonly used in the private sector, including by small companies. Comments to the NIST request for information were due by April 25, 2022.

U.S. LITIGATION
By Nicole Bartz Metral

Illinois Supreme Court Rules BIPA Claims Not Barred by Workers' Compensation Law

The Illinois Supreme Court ruled that the state's Workers' Compensation Act does not preempt statutory damages claims under the BIPA. The Court held that claims for liquidated damages for collection of biometric data in violation of BIPA don't qualify as a workplace injury that occurred on the job that would be subject to the Workers' Compensation Act. A significant number of BIPA lawsuits brought by employees against employers had been paused pending the Court's ruling on the preemption issue. Those cases are now set to proceed. The ruling emphasizes the need for companies that use biometric information in the employment context to put in place a compliance program meeting BIPA requirements or risk significant liability for violations of the law as the flood of BIPA lawsuits continues unabated.

Claims Alleging Wiretap Violations for Website's Collection of Analytics Dismissed

The U.S. District Court for the District of Delaware dismissed a proposed class action alleging that General Motors' ("GM") website had violated the Federal Wiretap Act and the California Invasion of Privacy Act by using third-party software that recorded user mouse and keyboard movements and the date, time, and IP address associated with the user's interaction with the website. The district court judge distinguished the case from a case in which Facebook has reached a proposed settlement for $90 million because

[22] https://www.nist.gov/cyberframework/request-information-about-evaluating-and-improving-cybersecurity-resources.

GM only recorded user information while users were on GM's own website, no personal information was obtained from users and no allegations were made that GM attempted to sell or monetize the collected information in any way. The court further held that the plaintiffs did not have a reasonable expectation of privacy in the data captured by the software and consequently did not suffer any concrete injury that could support the claims.

Weight Loss Company Reaches $56 Million Settlement

Noom, Inc. agreed to pay $56 million and an additional six million dollars in subscription credits to settle a putative class action in the U.S. District Court for the Southern District of New York, regarding Noom's trial period and autorenewal billing practices. Noom is a popular subscription-based mobile app for tracking food intake and exercise habits, while encouraging healthy choices for weight loss. The class members alleged that Noom "actively misrepresents and/or fails to accurately disclose the true characteristics of its trial period, its automatic enrollment policy, and the actual steps customer need to follow in attempting to cancel a 14-day trial and avoid automatic enrollment" and that Noom made it difficult for consumers to cancel their subscription before the trial ended, resulting in consumers paying nonrefundable lump sums for up to eight months at a time. Regulators at the state and federal level have been focused on similar "dark patterns" that direct consumers into enrolling for subscriptions or make it difficult to cancel.

Vendor of Employee Biometric Data Collection Tools Settles BIPA Class Action

Kronos, Inc., a provider of time and attendance solutions to employers, agreed to a $15.3 million settlement relating to claims that it violated BIPA by collecting fingerprints for its employer customers' timekeeping purposes. Plaintiffs alleged that Kronos violated BIPA when its software collected fingerprints through its software without providing notice and obtaining consent from the individual employees. The settlement highlights the risk to vendors with products and services that collect biometric information, even where the vendor's customers, rather than the vendor itself, maintain the direct relationship with the individuals from whom the biometric information is collected.

U.S. ENFORCEMENT

By Harrison M. Brown

Colorado Attorney General Issues Data Security Guidance

The Colorado Attorney General published guidance[23] on data security best practices. The guidance highlights nine key steps to protecting personally identifiable information,

[23] https://coag.gov/app/uploads/2022/01/Data-Security-Best-Practices.pdf.

including inventorying the types of data collected and establishing a system for how to store and manage that data, developing a written information security policy, adopting a written data incident response plan, managing the security of vendors, and following the Colorado Department of Law's ransomware guidance.[24] Notably, the guidance recommends that an entity's written information security policy follow industry-accepted information security standards relevant to the type of information the entity seeks to protect (e.g., PCI-DSS, ISO/IEC 27000, CIS controls, etc.), which tracks the growing consensus among regulators regarding adherence to industry accepted standards as the requisite standard of care for data protection under state and federal data security laws.

BBB National Programs Digital Advertising Accountability Program Announces Compliance Warning Regarding Device Fingerprinting

The BBB National Programs Digital Advertising Accountability Program ("DAAP") issued a new compliance warning about the use of device fingerprints in connection with the collection of cross-app data. DAAP is a program that enforces industry self-regulation principles for data privacy in websites and mobile advertising. Companies are now on notice that DAAP will treat any combined information used to uniquely identify a device or a user for internet-based advertising ("IBA") as the same as an advertising ID in evaluating if a company is collecting or using cross-app data. Under the Digital Advertising Alliance Principles, cross-app data is data collected from a particular device regarding application use over time. If a company collects this type of data and uses it for IBA, or allows another entity to do so, that company may need to provide notice, enhanced notice, or consent to the user.

Texas Attorney General Brings Enforcement Action against Meta for Biometric Data Collection

The Texas Attorney General brought a lawsuit against Meta (formerly Facebook) over the use of biometric data of Texans without their consent to do so. The Texas Attorney General alleges Meta has been storing biometric identifiers (such as retina scans, fingerprints, voiceprints, records of hand or face geometry) from photos and videos uploaded by consumers without their consent and in violation of Texas' Capture or Use of Biometric Identifier Act and the Deceptive Trade Practices Act.

New York Attorney General Fines Vision Benefits Company for Failure to Comply with State Data Security Law

The New York Attorney General announced[25] an agreement with vision benefits company EyeMed resulting in a $600,000 fine stemming from a 2020 data breach that

[24] https://coag.gov/press-releases/7-29-21-2/.

[25] https://ag.ny.gov/press-release/2022/attorney-general-james-announces-600000-agreement-eyemed-after-2020-data-breach.

affected 2.1 million consumers, including almost 100,000 New York residents. The New York Attorney General found that EyeMed violated New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), which requires businesses to maintain a data security program that includes a number of specific administrative, physical and technical safeguards. Specifically, the New York Attorney General found EyeMed had failed to implement multifactor authentication for a compromised e-mail account that was accessible via the web and contained a large volume of sensitive information, failed to implement sufficient password management, and failed to maintain adequate logging, which hampered investigation of the incident. In addition to the fine, EyeMed agreed to enact a number of measures to improve its information security program and bring it in line with SHIELD Act requirements.

INTERNATIONAL LAWS AND REGULATION
By Alex C. Nisenbaum

CNIL Rules Use of U.S. Website Analytics Tool Violates the GDPR

The French data protection authority, the Commission Nationale de l'Informatique et des Libertés ("CNIL") ruled that the transfer of personal data of EU residents through the use of a U.S. website analytics tool violated the General Data Protection Regulation's ("GDPR") cross-border transfer requirements. The CNIL ruled that the additional measures taken by the U.S. website analytics service provider to regulate its website analytics tool's data transfers were insufficient to protect EU personal data from being accessed by U.S. intelligence services. In its press release, the CNIL has recommended website analytics tools only be used to produce anonymous statistical data. The CNIL's ruling, which follows a similar ruling by the Austrian data protection authority in January 2022, was made in cooperation with its European counterparts and thus similar decisions from data protection authorities in other EU Member States can be expected.

UK ICO Publishes Data Transfer Documents

The UK Information Commissioner's Office ("ICO") published[26] the UK International Data Transfer Agreement[27] ("IDTA") and an Addendum[28] ("Addendum") to the

[26] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/?mkt_tok=MTM4LUVaTS0wNDIAAAGCUE8H0k_9i8hdSU-jQKfoCjXJx5vLcaK_Nb0gDGYPFAg3IS5C4_BVthNmPLRBfMC8JDZw7dmwSV2Hr-DQolCh_uLhZEMmm5wfrGAatkMIJQ9E.

[27] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F4019536%2Fidta.docx&wdOrigin=BROWSELINK.

[28] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F4019535%2Faddendum-international-data-transfer.docx&wdOrigin=BROWSELINK.

European Union's new Standard Contractual Clauses ("New SCCs"). The IDTA and Addendum replace the old Standard Contractual Clauses ("Old SCCs") and align UK contractual data transfer mechanisms with the New SCCs and EU requirements following the Court of Justice of the European Union's *Schrems II* decision. Contrary to the modular approach of the New SCCs, the IDTA is a single agreement that applies regardless of the role of the parties, with the exception of certain clauses. The Addendum allows entities to use the New SCCs for UK data transfers by adding terms to the New SCCs tailored for UK data transfers. Companies may use the Old SCCs for new agreements until September 21, 2022. Companies will have until March 21, 2024, to migrate all UK data transfers to the IDTA or Addendum.

CNIL Publishes Enforcement Priorities for 2022

The CNIL published[29] a summary of enforcement priorities for the coming year, citing three priority topics. The CNIL named commercial prospecting and data brokers who resell marketing lists, monitoring tools used to monitor employees working remotely, and the use of cloud computing, particularly as it relates to transfers of data outside the EU and data breaches as priorities. The CNIL has been a particularly active EU data protection authority, issuing several notable enforcement decisions relating to cross-border data transfer and obtaining consent of individuals to the placement of cookies on end user devices and browsers.

European Commission Proposes Data Act

The European Commission (the "Commission") proposed[30] the Data Act, which aims to give users of connected devices access to the data generated by them and would require manufacturers to share data with third parties such as other providers and aftermarket services. The proposed Data Act also sets out general rules applicable to obligations to make data available, requiring any conditions under which data is made available to be fair and nondiscriminatory and that any compensation charged must be reasonable. Compensation set for small and medium-sized enterprises cannot exceed the costs incurred for making the data available. The proposed Data Act may have an enormous impact for companies that manufacture internet-connected equipment and that have invested significant amounts in data generation and collection. The proposed Data Act will be presented to the European Parliament and Council of Ministers, which will negotiate a final text of the Data Act to be considered by the European Parliament. The process is expected to take 18 months to two years.

---

[29] https://www.cnil.fr/en/priority-topics-investigations-2022-commercial-prospecting-cloud-and-telework-monitoring.

[30] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113?mkt_tok=MTM4LUVaTS0wNDIAAAGCxst4pj6fL9YrglvV42rLxOf4EAo0UgDFWO_LGtEW4FRSlhy3xDpHOakkQR3s4ktR_R7OV8HOQexDcQ_Ay3IsOhiI6t22BwW1u4FL6z-m7129.