Morgan Lewis

REPORT

# GLOBAL PRIVACY
## YEAR IN REVIEW

March 2023

**www.morganlewis.com**

Morgan Lewis

# GLOBAL PRIVACY YEAR IN REVIEW

The need for privacy and cybersecurity compliance measures has become a paramount consideration as businesses become more digitally driven, data breaches become more publicized, and regulation continues to increase. Morgan Lewis privacy and cybersecurity lawyers advise clients operating in the United States, Europe, South America, and Asia on compliance with privacy and cybersecurity regulations. This global privacy year in review takes an in depth look at privacy and cybersecurity updates around the globe.

Topics in this year in review include the following:

- In China, a series of new regulations and national standards on mechanisms for cross-border data transfers
- In the United States, updates to the state privacy law landscape, the latest wave of consumer class actions under state and federal anti-wiretapping laws, and developments in litigation involving the Illinois Biometric Information Act
- In the United Kingdom and European Union, developments in international data transfers, data breaches, regulation of cookies, and artificial intelligence
- In the United Arab Emirates, takeaways from the first comprehensive federal data protection law

# CHINA

Authors: Todd Liao and Sylvia Hu

## WHAT COMPANIES SHOULD DO FOR LAWFULLY TRANSFERRING DATA OUTSIDE OF CHINA

The China Cybersecurity Law (CSL), the Personal Information Protection Law (PIPL), and the Data Security Law (DSL) constitute the fundamental laws in China's data protection regime. The CSL, effective on June 1, 2017, is the first comprehensive law that forms the backbone of cybersecurity protection. The DSL, effective on September 1, 2021, mainly aims to ensure the security of all kinds of data during its collection, use, storage, processing, transfer, and disclosure. Both the CSL and DSL focus on the protection of data security, national security, and public interests, while the PIPL, effective on November 1, 2021, concentrates on the security of personal information and the protection of the personal information rights and interests of data subjects.

Under the umbrella of the fundamental laws above, the Chinese government has been working to roll out a set of regulations and national standards to implement cyber and data protection requirements and to strengthen data governance and enforcement efforts. The most noteworthy are a series of regulations and national standards released since 2022 on mechanisms for cross-border data transfer. By way of overview:

- Under the current legal framework, companies that are certified as critical information infrastructure operators (CIIOs) or processing important data or personal information exceeding certain volume thresholds must undergo a mandatory security assessment approved by the Cyberspace Administration of China (CAC-led Security Assessment).
- Companies that are not subject to the CAC-led Security Assessment should choose either of the following to lawfully transfer personal information outside of China:
  - Obtain certification from "qualified institutions" (Certification); or
  - Enter into a data transfer agreement (China standard contractual clause) with overseas data recipients based on the standard contract published by the Cyberspace Administration of China (CAC).

## MECHANISM 1: CAC-LED SECURITY ASSESSMENT

On July 7, 2022, the CAC released its long-awaited final version of the Measures for Security Assessment of Cross-Border Data Transfer (CBDT Measure) and responded to correspondents' questions (CAC Responses). The CBDT Measure, taking effect from September 1, 2022, provides a clear pathway for companies that need to send data overseas for their operations by outlining the specific requirements, steps, and procedures to go through a security assessment.

Under the CBDT Measure, companies engaging in cross-border transfers of data that reach any of the following thresholds must go through the CAC-led Security Assessment:

- Transferring important data outside of China
- Transferring personal information out of China by CIIOs or data handling entities that process the personal information of over one million individuals
- Transferring personal information out of China since January 1 of the prior year that exceeds the personal information of more than 100,000 individuals or the sensitive personal information of more than 10,000 individuals

### Important Data

The CBDT Measure, for the first time at the regulation level, defines the term "important data" as "any data that, once tampered with, sabotaged, leaked or illegally obtained or used, may endanger national security, economic operation, social stability, and public health and safety." However, detailed guidance in relation to the scope of important data is still pending.

### CIIO

CIIOs are defined by the Security Protection Regulations on the Critical Information Infrastructure (CII Regulation) as companies engaged in important industries or fields, such as public communication and information services, energy, transport, water, finance, public services, and national defense. Under the CII Regulation, if the network infrastructure or information system of an entity was designated by the industry regulators as "critical information infrastructure," the regulators in charge must notify the designated CIIO of such designation in a timely manner.

### Cross-Border Transfer

The CBDT Measure does not provide a definitive definition for the term "cross-border data transfer." Referring to the Guidelines for Cross-Border Data Transfer Security Assessment dated 2017, cross-border data transfer generally refers to any movement of personal information (and other restricted classes of data) outside of China.

In the CAC Responses relating to the CBDT Measure, the CAC set forth two "cross-border data transfer" scenarios that are subject to security assessment: (1) the data handlers transfer and store data collected and generated in China outside the territory of China; and (2) the data handlers store the data collected and generated within China, but overseas organizations and individuals would have remote access to them.

The security assessment requirements under the CBDT Measure, in particular, came into effect on September 1, 2022. The security assessment requirements have a retroactive effect on cross-border data transfers conducted prior to this date. Given the time required to complete the security assessment process, companies should plan ahead and start bringing their practices in line with these new requirements as soon as possible to prevent any interruptions to potential data transfer or business operations.

## MECHANISM 2: CERTIFICATION

China published the draft version of the Certification Specification for Cross-Border Processing of Personal Information (Draft Certification Specification) for public comments in November 2022, which provides guidance for companies to have their cross-border data transfer certified. Draft Certification Specification is intended to replace the previous version of the Technical Certification Specification for Certification of Personal Information Cross-border Processing released on June 24, 2022.

The Draft Certification Specification provides that, to obtain certification, companies should satisfy the following requirements:

- The data exporter and overseas recipients should sign a data transfer agreement that contains required clauses.
- The data exporter should conduct an internal procedure, the personal information protection impact assessment (PIPIA), before the cross-border data transfer takes place.

On November 4, 2022, the CAC and the State Administration of Market Regulation (SAMR) released the Implementation Provisions for Personal Information Protection Certification (PI Certification Provisions),

also providing key principles and requirements for certifying the collection, storage, use, processing, transmission, provision, disclosure, deletion, and cross-border transfer of personal information, which effectively supports the implementation basis for the certification rules in the cross-border transfers of personal information. According to the PI Certification Provisions, personal information handlers that carry out cross-border handling activities should meet the requirements of both the proposed Certification Specification and the PI Certification Provisions.

The Draft Certification Specification and the PI Certification Provisions are national standards that are not legally binding legislation in China, but they reflect the detailed legal requirements that the Chinese regulators will refer to when conducting certification and provide detailed guidance for organizations with which to comply in their data handling activities. However, the Draft Certification Specification has not been finalized yet, nor have qualified certification institutions been designated, which are pending further notification from the government and the impact of which on enforcement remains to be seen.

## MECHANISM 3: CHINA SCC

On February 24, 2023, the CAC released the final version of the standard contract for the cross-border transfer of personal information, considered China's standard contractual clauses (China SCC). Together with the final standard contract, China also released the final version of the Provisions on Standard Contract for Export of Personal Information (Standard Contract Provision), which provides additional obligations for companies that intend to use the China SCC mechanism.

Under the Standard Contract Provision, a data exporter is allowed to transfer personal information outside of China by way of the China SCC mechanism if all of the following conditions are satisfied:

- The data exporter is not a CIIO (typically covering entities in financial, energy, telecom, public utility, healthcare, transportation, and other similar industries); It has not processed the personal information of more than one million individuals.
- It has not conducted cross-border transfers of the personal information of more than 100,000 individuals in aggregate since January 1 of the prior year.
- It has not conducted cross-border transfers of the sensitive personal information of more than 10,000 individuals in aggregate since January 1 of the prior year[1].

For calculating the above data transfer volume, the Standard Contract Provision prohibits businesses from breaking down the data volume in batches to circumvent the CAC-led Security Assessment.

Under the Standard Contract Provisions, if the company intends to choose the China SCC mechanism to lawfully transfer personal information outside of China, the following conditions must be satisfied:

- The China SCC signed by the company and overseas recipients would need to be filed with the local branches of the CAC within 10 working days of the China SCC taking effect.
- The company should prepare a PIPIA report, which must take multiple factors into consideration, including without limitation to validity, necessity, and appropriateness for the data export; scope, category, volume, and sensitivity of the data export; obligations and technical/organizational measures taken; risk of data leakage and remedy channels available to data subjects; and data protection laws of foreign destination countries, etc. The PIPIA report should also be filed with the provincial branch of CAC within 10 working days of the China SCC taking effect.

[1] Data exporters who are CIIOs or processing personal information exceeding the above volume thresholds will still be subject to the CAC-led Security Assessment.

The Standard Contract Provision and China SCC will become effective on June 1, 2023. Companies having transferred personal information from China have a grace period of six months (ending on November 30, 2023) to rectify their data export practice.

Non-compliance after such grace period will be subject to penalties imposed in accordance with the PIPL. Such penalties can reach up to 5% of the last year's turnover of the company.

The China SCC closely resembles the EU SCCs, but also reflect the particulars and focus of China data privacy supervision. The China SCC only has one universal template, which applies to data exporters in China and overseas data recipients, regardless of the role and function of the data processing parties. The governing law must be Chinese law and dispute resolution must be in China. The parties must strictly follow the SCC template but may add supplemental provisions to the template as long as they do not conflict with the template terms.

Companies may want to review their cross-border data transfer workstreams based on the regulatory trend reflected in the Draft Standard Contract Provisions and make proper adjustments to the existing compliance measures if they were established mainly in accordance with the EU General Data Protection Regulation (GDPR).

China’s dynamic data protection regime continues to evolve. These developments will have an impact on nearly every company doing business in China. It is recommended that companies (especially for those that will involve cross-border data transfer) perform a data health check or data mapping project to understand the nature, volume, and stakeholders of their data processed in China in order to form a data compliance strategy, including whether to perform the CAC-led Security Assessment and select a suitable cross-border data transfer mechanism that fits into their respective business context as soon as possible.

# UNITED STATES

Authors: Kristin Hadgis, Ezra Church, Ben Kabe, Terese Schireson

# STATE CONSUMER PRIVACY LAWS

Influenced by California's Consumer Privacy Act of 2018 (CCPA), the most comprehensive, consumer-oriented privacy law in the United States, and the European Union's GDPR, a series of new consumer privacy laws have been enacted in states across the United States. The CCPA created an array of new consumer privacy rights that required many companies doing business in California to reassess their collection and use of personal information and modify their business processes to accommodate the new rights of consumers. The new state privacy laws expand upon those rights and obligations, resulting in a patchwork of compliance requirements. Businesses spent much of 2022 working toward compliance with these new laws, the effective dates of which range from January to December 2023.

## California

### California Privacy Rights Act

The California Privacy Rights Act (CPRA), effective January 1, 2023, expands consumers' rights under the CCPA by (1) preventing businesses from sharing personal information for "cross-context behavioral advertising," (2) allowing consumers to request to correct inaccurate personal information, (3) limiting businesses' use of "sensitive personal information"—including precise geolocation; race; ethnicity; religion; genetic data; private communications; sexual orientation; and specified health information, and (4) extending the look-back period for requests to know beyond 12 months.[2] In addition to offering consumers the ability to opt out of the sale of personal information, businesses must honor requests to opt out of "sharing" for the purposes of "cross-context behavioral advertising," which is the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or other services.

The CPRA also expands the private right of action under the CCPA to cover (1) nonredacted and nonencrypted information, *and* (2) email addresses with a password or security question and answer that would permit access to the account. The CPRA makes clear that security measures implemented after a breach do not constitute a cure of that breach. Additionally, the CPRA adds requirements for the protection of personal information by businesses, including (1) minimizing data collection, (2) limiting data retention, (3) protecting data security, and (4) conducting privacy risk assessments and cybersecurity audits. The CPRA expands upon the CCPA's privacy notice requirements to require disclosures regarding whether personal information is sold or shared, data retention periods, and disclosures about the collection and use of sensitive personal information.

The CPRA also establishes the California Privacy Protection Agency to enforce and implement consumer privacy laws and impose fines. Although the CPRA took effect on January 1, 2023, enforcement will not begin until July 1, 2023.

### Employment and Business-to-Business Information

As of January 1, 2023, California is the first state to provide expansive privacy rights to employees. In addition, new privacy rights will apply to personal information collected in the context of a business "providing or receiving a product or service to or from" another business.

[2] Cal. Civ. Code § 1798.100 et seq. The CPRA applies to businesses that (1) as of January 1 of the calendar year, exceeded $25 million in gross revenue in the preceding calendar year, (2) buy, sell, or share the personal information of 100,000 or more consumers or households, or (3) derive 50% or more of annual revenue from selling or sharing consumers' personal information.

The CCPA previously imposed limited obligations on employers with respect to employee data if they qualify as "businesses" subject to the law. Two bills had been introduced in the California Legislature that would have extended or made permanent exemptions for employee and business-to-business (B2B) data, but neither bill had been enacted when the legislature's session expired on August 31, 2022. Accordingly, the definition of "consumer" under the CCPA no longer exempts employees or B2B contacts.

**CPRA Regulations**

The California Privacy Protection Agency has issued draft CPRA regulations that provide a glimpse into where privacy regulation is likely headed in California and, by extension, the United States. Although not yet final, the draft regulations provide extensive guidance and make clear that the CPRA intends to build upon its already stringent requirements. Requirements set forth in the draft regulations include the following:

- A requirement that consumers' privacy choices be "easy to execute" and that businesses not add unnecessary burden or friction to the consumer request process. The regulations also prohibit the use of "dark patterns"—user interfaces that have the effect of substantially subverting or impairing user autonomy, decision making, or choice—as consumer consent.
- A requirement that businesses engaging in the sale or sharing of personal information process universal opt-out preference signals, which will allow consumers to communicate a request to opt out of the processing of their personal data across multiple websites at once.
- A requirement that a business's collection, use, retention and/or sharing of a consumer's personal information be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed. A business must obtain a consumer's explicit, opt-in consent before collecting, using, retaining, and/or sharing personal information for unrelated or incompatible purposes.
- Expansion of the required terms for agreements between businesses and service providers, contractors, and third parties. The draft regulations also provide incentives for businesses to conduct due diligence of service providers and contractors: a business that never exercises its rights to audit or test a service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intended to use personal information in violation of the CCPA.
- A requirement that contracts with service providers and contractors must specify the business purpose for which personal information is being collected; a generic description is not sufficient.

The California Privacy Protection Agency is required to finalize the CPRA Regulations by July 1, 2023.

## Virginia

Virginia is the second US state to pass a comprehensive data privacy law. The Virginia Consumer Data Protection Act (VCDPA), which took effect on January 1, 2023, follows a similar framework as the CCPA, CPRA, and GDPR, with some noteworthy differences.[3] The VCDPA will require companies doing business

[3] Va. Code Ann. § 59.1-575 et seq. The VCDPA applies to businesses that (1) control or process the personal information of 100,000 or more state residents, or (2) control or process the personal information of 25,000 or more state residents and derive over 50% of gross revenue from the sale of personal information.

in Virginia to reassess their collection and use of consumer personal information and modify their business practices to account for Virginia's new requirements.

The VCDPA gives Virginia consumers the right to request to access, correct, or delete their personal information. The law also provides consumers a right to opt out of the processing of personal data for purposes of targeted advertising, the sale of their personal data to third parties, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. "Targeted advertising" means "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests." Finally, in contrast to the CPRA, the VCDPA affords consumers the right to appeal the denial of their request.

The VCDPA also prohibits businesses from processing "sensitive data" without first obtaining a consumer's consent, and "consent" is defined as a "clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement." This is a higher standard than that required under the CPRA and has more in common with the consent standard established by the GDPR. The VCDPA also requires businesses to provide a privacy notice with certain disclosures, minimize the use of personal information, and conduct data protection assessments for certain processing activities. In contrast to the CCPA, controlling or processing personal data in the B2B or employment context falls outside the scope of the VCDPA, and the VCDPA does not establish a private right of action. The VCDPA will be enforced by the Virginia Attorney General, with civil penalties up to $7,500 per violation.

## Colorado

By enacting the Colorado Privacy Act (CPA), which takes effect on July 1, 2023, Colorado became the third state to enact comprehensive privacy legislation.[4] Like the CCPA and VCDPA, the CPA will grant consumers the rights to request access to, correct, or delete their personal information. Like the VCDPA, it will also require companies to allow consumers to opt out of targeted advertising, the sale of their personal information, and profiling decisions, and also establishes a right of consumers to appeal the denial of a request. Similar to the CPRA, the CPA will require that businesses recognize universal opt-out signals beginning July 1, 2024.

Colorado will require companies to provide a privacy notice with certain disclosures, conduct data protection assessments for certain processing activities, minimize use of personal information, and process sensitive personal information only after obtaining consent. As with Virginia, controlling or processing personal data in the B2B or employment context falls outside the scope of the CPA.

The CPA does not create a private right of action. The CPA will be enforced by the Colorado Attorney General, with violations considered to be deceptive and unfair trade practices and carrying civil penalties of up to $20,000 per violation.

In September 2022, the Colorado Attorney General's Office published proposed CPA regulations that provide guidance on consumer requests, privacy notice requirements, and data protection assessments, among other topics.

[4] Colo. Rev. Stat. Ann. § 6-1-1301 et seq. The CPA applies to businesses that (1) control or process the personal information of 100,000 or more state residents, or (2) control or process the personal information of 25,000 or more state residents and derive revenue or receive a discount on the price of goods or services from the sale of personal information.

## Utah

Utah is the fourth state to pass a comprehensive consumer data privacy law, having enacted the Utah Consumer Privacy Act (UCPA) in March 2022.[5] The UCPA will take effect on December 31, 2023. Although similar to the privacy laws that preceded it, Utah's law has a few distinctive features that make it the most business-friendly state privacy law yet.

The consumer rights established by the UCPA are largely similar to those established by the CCPA, CPRA, CPA, and VCDPA, although there are some key differences. Under the UCPA, consumers have the rights to request access, deletion, portability, and to opt out of the sale of personal data, targeting advertising, and the processing of sensitive data. In contrast to the other state privacy laws, the UCPA does not provide consumers with the right to correct inaccuracies in their data. Unlike the CPA and VCDPA, the UCPA does not allow consumers to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer, nor does it grant consumers the right to appeal the denial of a request.

The UCPA does not require that businesses obtain consent prior to processing sensitive data; in order to process such sensitive data, the businesses must first present the consumer with clear notice and an opportunity to opt out. Businesses subject to the UCPA must minimize the use of personal information and provide a privacy notice that includes certain disclosures, including about consumer rights. Similar to the VCDPA and CPA, the UCPA exempts employment-related and B2B data.

In contrast to the other state consumer privacy laws, the UCPA does not require that businesses conduct data protection assessments. There is no private right of action under the UCPA, and violations of the UCPA carry civil penalties up to $7,500 per violation.

## Connecticut

Connecticut became the fifth state to enact a comprehensive consumer privacy law in May 2022. The Connecticut Data Privacy Act (CTDPA), which draws heavily from the VCDPA and CPA, will take effect and become enforceable on July 1, 2023.[6]

The law includes many of the same rights, obligations, and exceptions as the consumer privacy laws in California, Colorado, Utah, and Virginia. Connecticut grants consumers the rights to access personal information collected about them, correct inaccuracies in their personal information, delete their personal information, obtain a copy of their personal information, and opt out of the use of the sale of their personal information, the use of their personal information for targeted advertising, and the use of their personal information for profiling that may have a legal or other significant impact.

Businesses will be required to provide "clear and conspicuous" links on their websites that give consumers the choice to opt out of the above types of processing. Similar to the CPRA and CPA, under the CTDPA, universal opt-out mechanisms must be recognized by businesses as valid consumer requests

[5] Utah Code Ann. § 13-61-101 et seq. The UCPA applies to businesses that (1) have $25 million in gross revenue and control or process the personal information of 100,000 or more state residents, or (2) control or process the personal information of 25,000 or more state residents and derive over 50% of gross revenue from the sale of personal information.

[6] Conn. Gen. Stat. Ann. § P.A. 22-15, § 1 et seq. The CTDPA applies to businesses that (1) control or process the personal information of 100,000 or more state residents (excluding personal information controlled or processed only for payment transactions), or (2) control or process the personal information of 25,000 or more state residents and derive over 25% of gross revenue from the sale of personal information.

beginning January 1, 2025. Like the VCDPA and CPA, the CTDPA grants consumers the right to appeal a business's decision denying a consumer rights request.

Similar to the VCDPA and CPA, the CTDPA prohibits businesses from processing sensitive data without consent. As in Virginia, Colorado, and Utah, controlling or processing personal data in the B2B or employment context falls outside the scope of the CTDPA. The CTDPA will require companies to provide a privacy notice with certain disclosures, minimize the use of personal information, and conduct data protection assessments for certain processing activities.

There is no private right of action under the CTDPA and violations carry civil penalties up to $5,000 per violation. The CTDPA provides for a 60-day cure period, which will sunset on December 31, 2024.

We have prepared helpful checklists on the CCPA and state privacy laws. Additionally, below is a list of recent Morgan Lewis thought leadership on state privacy laws. Please visit Morgan Lewis's US Consumer Privacy Acts page for more information.

- Virginia Enacts Broad Data Privacy Law, Second in US After California: What It Means for Businesses
- California Consumer Privacy Act: Employee and B2B Exemptions Expire January 1, 2023
- Utah Passes More Business-Friendly Consumer Data Privacy Law

# WIRETAPPING CLASS ACTIONS

2022 brought a new wave of consumer class actions against ecommerce companies and third-party analytics companies under state and federal anti-wiretapping laws. Wiretapping statutes, although traditionally intended to prohibit the recording of phone calls, have in recent years been used to target commonplace web technologies used by consumer-facing companies. The laws vary somewhat across states, but generally prohibit the interception of communications without consent.

The recent wave of cases is focused on two types of technology that are increasingly common on consumer-facing websites: (1) "session replay" technology, which tracks consumer activity on websites to monitor customer behavior, improve customer experience, and study how website visitors interact with the website, and (2) chat features that record conversations with consumers via instant message. Wiretapping class actions are concentrated in states with all-party consent laws—requiring that all parties to a conversation or interaction to consent to be recorded—such as California, Florida, and Pennsylvania.

Plaintiffs in these cases generally allege that because they did not affirmatively consent to the use of session replay technology or a chat feature, website operators and, in some cases, their marketing partners, violated the applicable state's wiretapping statute. Wiretapping statutes typically provide for statutory penalties upwards of $5,000 per violation, resulting in significant potential exposure.

## Key Decisions in 2022

Two recent decisions in California and Pennsylvania have generated renewed interest in session replay and other website tracking claims under wiretapping statutes in those states.

In May 2022, the Ninth Circuit held, in an unpublished decision, that the California Invasion of Privacy Act (CIPA) requires prior consent and rejected the defendants' argument that California's wiretapping statute allows a business to obtain consent to the use of session replay software after a recording has begun. The court remanded the case to the district court to consider whether, based on the complaint's allegations, the plaintiff had consented to the collection of data through session replay software.

The plaintiff in *Javier v. Assurance IQ, LLC*, alleged that he visited an insurance-quoting website that uses third-party software to record a video of users' interactions with the website.[7] After filling out an insurance-quote questionnaire on the website, the plaintiff "viewed a screen that stated that clicking the 'View My Quote' button would constitute agreement to Assurance's Privacy Policy" and clicked the "View My Quote" button.[8] The plaintiff later filed a putative class action, claiming that the website owner and third-party software company violated the CIPA by recording his interactions with the website without his consent.[9]

The district court held that the plaintiff's claims lacked merit because he had retroactively consented to the use of session replay technology by agreeing to Assurance's privacy policy.[10] The Ninth Circuit reversed, holding that a plaintiff's consent to a privacy policy after providing his personal information was

[7] No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022).

[8] *Id.*

[9] *Id.*

[10] *Id.*

not sufficient, and that *prior* consent is instead required under CIPA.[11] The Ninth Circuit remanded the case for a determination regarding whether the plaintiff impliedly consented to the use of session replay technology.[12]

Several months later, in August 2022, the Third Circuit reversed a district court's dismissal of a putative class action based on the use of session replay technology.[13] In *Popa v. Harriet Carter Gifts Inc.*, the plaintiff alleged that while she was browsing Harriet Carter Gifts' ecommerce website, Harriet Carter Gifts used session replay technology supplied by a third-party digital marketer (NaviStone) to record her movements.[14] The plaintiff claimed that the rerouting of her communications to NaviStone constituted an illegal interception under Pennsylvania's Wiretapping and Electronic Surveillance Control Act (WESCA). The district court granted summary judgment in favor of the defendants, holding that there had been no interception under WESCA because NaviStone was a direct recipient of the plaintiff's communications, and to the extent any interception did occur, it occurred outside of Pennsylvania's borders and thus outside the scope of WESCA.[15]

In a precedential decision, the Court of Appeals for the Third Circuit reversed, ruling that (1) the defendants could not avoid WESCA liability merely by showing that NaviStone directly received the challenged communications from the plaintiff, because the only direct-party exception under WESCA applies to certain law enforcement activities, (2) NaviStone's alleged "interception" of the plaintiff's online communications occurred at the point where it routed the plaintiff's communications to NaviStone's servers, even if NaviStone ultimately received those communications outside of Pennsylvania, and (3) because the district court granted summary judgment on other grounds without reaching the issue of consent, whether the plaintiff gave prior consent to the challenged interception of her communications required further consideration from the district court on remand.[16]

Many consumer-facing businesses have websites that rely upon third-party coding like NaviStone's to enable digital advertising and to deliver a tailored experience to their customers. Under the *Popa* decision, third-party marketing services facing litigation in Pennsylvania cannot rely on a direct recipient exception to WESCA liability, and they are potentially subject to the statute's reach based on the location of the plaintiff's website browser, even if they received allegedly intercepted communications outside of Pennsylvania.

## Rise of Wiretapping Litigation Based on Chat Features

A more recent surge in putative wiretapping class actions focuses on the customer support chat features prevalent on many consumer-facing websites. Plaintiffs in these cases allege that the information gathered and shared with vendors who provide chatbot technology is recorded and intercepted without a user's consent in violation of state wiretapping statutes. Although these cases are in their early stages,

---

[11] *Id.* at *2.

[12] *Id.*

[13] *Popa v. Harriet Carter Gifts Inc.*, 52 F.4th 121 (3d Cir. 2022). In October 2022, the Third Circuit issued a revised opinion following the defendants' motion for a rehearing, upholding the panel's original holdings. *Id.*

[14] *Id.* at 124.

[15] *Id.*

[16] *Id.* at 131-132.

courts appear hesitant to decide whether wiretapping statutes apply to these claims without the benefit of discovery.[17]

## Key Takeaways and Issues to Watch in 2023

Given the prevalence of third-party data sharing and the availability of liquidated damages under certain state wiretapping statutes, the pending district court rulings in California and Pennsylvania regarding whether prior consent to interception may be implied through privacy policy disclosures will likely affect future wiretapping cases.

In the coming year, issues not addressed in *Javier* or *Popa* are likely to play out in the courts. For example, various courts have dismissed session replay claims for failure to allege interception of the substance or contents of communications, and it will be interesting to see if this trend continues in 2023.[18]

Many consumer-facing businesses have websites that rely upon third-party software to deliver a tailored experience to their customers and to facilitate customer service chats. This recent wave of litigation serves as a reminder for website operators, digital marketers, and their partners to review their online marketing practices, privacy disclosures, contractual terms with vendors, buy-flow processes, and consent mechanisms, and reevaluate how easily they could demonstrate consent to third-party data sharing at an early stage of litigation if faced with a putative class action under state or federal wiretapping laws.

---

[17] *See, e.g.*, *Makkinje v. Extra Space Storage*, 2022 WL 80437 (M.D. Fla. 2022) (denying motion to dismiss in chatbot case and distinguishing chat feature from session replay "because Defendant's use of session replay software during [plaintiff's] visit to its website recorded more than just her non-substantive browsing movements.").

[18] *See, e.g.*, *Jacome v. Spirit Airlines Inc.*, No. 2021-000947-CA-01, 2021 WL 3087860 (Fla. Cir. Ct. June 17, 2021) (holding that "mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff, and pages and content viewed by Plaintiff . . . is precisely the type of non-record information that courts consistently find do not constitute 'contents' under the Federal Wiretap Act or any of its state analogs because it does not convey the substance or meaning of any message"); *Yale v. Clicktale, Inc.*, No. 20-CV-07575-LB, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) (dismissing wiretapping claim and stating, "the plaintiff predicates her claim in part on information—such as IP addresses, locations, browser types, and operating systems—that is not content"); *Johnson v. Blue Nile, Inc.*, No. 20-CV-08183-LB, 2021 WL 1312771, at *2 (N.D. Cal. Apr. 8, 2021) (dismissing wiretapping act claim for same reason); *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021) (dismissing wiretapping act claim for same reason); *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318 (S.D. Fla. 2021) (dismissing wiretapping act claim because "Plaintiff's purported communications contained no substance").

# THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

This Illinois Biometric Information Privacy Act, 740 ILCS 14/1 et seq. (BIPA), governs the use of "biometric identifiers"—retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry—and "biometric information"—information derived from biometric identifiers that can be used to identify an individual. 740 ILCS 14/10. It was enacted to serve "[t]he public welfare, security, and safety … by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5. To that end, the BIPA imposes various restrictions and requirements on private entities that possess, collect, capture, purchase, receive through trade, or otherwise obtain biometric identifiers or biometric information. 740 ILCS 14/15. The statute also provides for a private right of action and damages. 740 ILCS 14/20. Specifically, the BIPA permits damages in the amount of "$1,000 or actual damages, whichever is greater" for each negligent violation, and "$5,000 or actual damages, whichever is greater" for each intentional or reckless violation. *Id.*

The BIPA went into effect on October 3, 2008. The statute lay dormant for many years, until the first BIPA class actions were filed in 2015.[19] Since then, BIPA lawsuits have proliferated, particularly after the Illinois Supreme Court's 2019 decision in *Rosenbach v. Six Flags Entertainment Corp.*[20] In *Rosenbach*, the court held that a party is "aggrieved" under BIPA—and thus has standing to sue—even if that party alleges no injury beyond a technical violation of the statute.[21]

## Key BIPA Issues in 2022

State and federal courts addressed important issues under the BIPA in 2022, although many questions remain unanswered.

### Extraterritoriality

Under Illinois law, state statutes do not apply extraterritorially unless the statute explicitly provides otherwise. The BIPA does not contain any explicit provision permitting extraterritorial application. This issue was litigated in two class actions brought by the same plaintiffs in the US District Court for the Western District of Washington: *Vance v. Microsoft Corp.*, No. C20-1082JLR (W.D. Wash.), and *Vance v. Amazon.com Inc.*, No. C20-1084JLR (W.D. Wash.).

In each case, the plaintiffs—residents of Illinois—alleged that the defendant violated the BIPA through its alleged use of the IBM "Diversity in Faces" dataset, which contained photos of the plaintiffs they had previously uploaded to the photo-sharing website Flickr.[22] In both cases, the defendants argued that any download or use of the dataset took place outside of Illinois, and that the BIPA therefore did not apply under the extraterritoriality doctrine.[23] The court agreed. It rejected the plaintiffs' argument that the defendants' conduct occurred "primarily and substantially" in Illinois, as required by the extraterritoriality

[19] Emma Graham, Burdened By BIPA: Balancing Consumer Protection and the Economic Concerns of Business, 2022 U. Ill. L. Rev. 929, 931 (2022).

[20] 129 N.E.3d 1197 (Ill. 2019).

[21] *See id.* at 1206.

[22] *See, e.g., Vance v. Microsoft Corp.*, 2022 WL 9983979, at *1 (W.D. Wash. Oct. 17, 2022).

[23] *Id.* at *6.

doctrine, because they were Illinois residents who were allegedly injured in Illinois.[24] The court instead considered the allegedly unlawful conduct—the acquisition of the plaintiffs' data—and held that that conduct did not "occur primarily and substantially in Illinois."[25]

These cases provide some clarity for companies dealing with biometric data wholly outside of Illinois, even if some data subjects happen to be Illinois residents. Still, companies must exercise caution, as it is not always clear where relevant conduct takes place given the often-complicated facts involved in BIPA cases.

**Preemption by Transportation Regulations**

It remains uncertain whether the BIPA applies to companies in certain highly regulated industries, such as transportation. Transportation defendants have argued that the BIPA is preempted by myriad regulations imposed on them by the federal government, with mixed results. In March 2022, a court in the Northern District of Illinois held that the plaintiff's BIPA claim against an airline was preempted by the Airline Deregulation Act (ADA).[26] The *Kislov* court concluded that the BIPA impermissibly "expand[s] obligations" that are not otherwise required by federal law and that claims like the plaintiff's under the BIPA are therefore preempted. Importantly, the court noted that Congress copied the Federal Aviation Administration Authorization Act's (FAAAA) preemption provision from the ADA.[27]

That same month, however, another court in the same district found that the FAAAA did not preempt the BIPA in a plaintiff's claim against a railroad.[28] The court found that "the impact of the BIPA on motor carrier prices, routes, or services [was] 'too tenuous, remote, or peripheral' to give rise to FAAAA preemption."[29] The court also rejected the railroad's preemption arguments under the Federal Railroad Safety Act and the Interstate Commerce Commission Termination Act.

In July 2022, another judge in the Northern District rejected a preemption argument by a facial recognition technology provider for interstate motor carriers.[30] The defendant argued that the BIPA interfered with a "uniform scheme of federal regulation of truck safety technology."[31] The court, however, agreed with the plaintiff's argument that the defendant's references did "not create a uniform regulatory scheme such that the clear, preemptive purpose of Congress is evident."[32]

The Seventh Circuit has not yet weighed in on these issues.

---

[24] *Id.* at *7.

[25] *Id.* at *8.

[26] *Kislov v. Am. Airlines, Inc.*, No. 17 C 9080, 2022 WL 846840, at *7 (N.D. Ill. Mar. 22, 2022).

[27] *Id.*

[28] *Rogers v. v. BNSF R'y Co.*, No. 19 C 3083, 2022 WL 787955, at *6 (N.D. Ill. Mar. 15, 2022).

[29] *Id.*

[30] *Karling v. Samsara Inc.*, No. 22 C 295, 2022 WL 2663513 (N.D. Ill. July 11, 2022).

[31] *Id.* at *2.

[32] *Id.* at *3.

**Section 15(a) Policy Timing**

BIPA Section 15(a) requires private entities "in possession" of biometric data to develop and publish a publicly available policy, including statutorily prescribed biometric retention and deletion guidelines, and to comply with those guidelines. *See* 740 ILCS 14/15(a). The Seventh Circuit has held that an allegation under the first portion of the Section 15(a)—i.e., the public policy requirement—rather than an allegation of an entity's failure to comply, does not support Article III standing.[33] Since the Seventh Circuit's ruling, many Section 15(a) claims have severed from claims under other provisions of the BIPA that do support Article III standing, to be litigated in parallel proceedings in state and federal court. The delineation between the duty to publish a BIPA policy and the duty to comply with that policy, however, left an important question unanswered. Section 15(a) does not explicitly address *when* a private entity must establish a public policy.

The Appellate Court of Illinois, Second District, answered this question in *Mora v. J&M Plating Inc.*[34] In *Mora*, the defendant began collecting the plaintiff's biometric data in September 2014, implemented a retention schedule in May 2018, and destroyed plaintiff's biometrics within two weeks of her employment ending in January 2021.[35] The issue before the court was whether the defendant satisfied Section 15(a)'s public policy requirement by publishing its policy *after* coming into possession of the plaintiff's biometrics. The court held that, "[h]ere, defendant began collecting plaintiff's biometric data in September 2014, and this triggered its obligation under section 15(a) to develop a retention-and-destruction schedule. Defendant did not have a schedule in place until May 2018, or nearly four years later. Thus, it violated section 15(a)."[36]

**Third-Party Vendors**

Third-party vendors of products or services that plaintiffs allege involve biometrics have increasingly become targets of BIPA lawsuits. These entities—for example, cloud computing service providers, identity verification companies, and biometric-hardware sellers—are often at least one step removed from the putative class members. Plaintiffs in these cases allege that an intermediate entity, like an employer, used the defendant's goods or services to collect or possess their biometrics. Courts are split on whether third-party vendors who provide biometric technology, such as biometric operating systems, must comply with Section 15(b).[37] And it is often unclear how a third-party vendor can comply with Section 15(b)'s notice and consent requirements where they lack any direct relationship with end-users.

Recently, federal and state courts weighed in on this issue. In *Ronquillo v. Doctor's Associates LLC*, a court in the Northern District of Illinois suggested that third-party vendors could comply with Section 15(b) by requiring their customers to agree to comply with the BIPA as a contractual precondition to using their devices.[38] Based on *Ronquillo*'s logic and the BIPA's statutory purpose, an Illinois court dismissed a plaintiff's claim against a third-party vendor with prejudice, finding that the vendor complied

---

[33] *See Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146 (7th Cir. 2020); *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617 (7th Cir. 2020).

[34] 2022 WL 17335861 (Ill. App. 2 Dist., Nov. 30, 2022).

[35] *Id.* at *3.

[36] *Id.* at *9.

[37] *Mayhall on behalf of D.M. v. Amazon Web Servs. Inc.*, No. C21-1473-TL-MLP, 2022 WL 2718091, at *10 n.4 (W.D. Wash. May 24, 2022).

[38] 2022 WL 1016600, at *3 (N.D. Ill. 2022).

with the BIPA by contractually requiring its customer to provide notice and obtain consent under the BIPA.[39]

Another court in the Northern District of Illinois recently dismissed a BIPA claim against a third-party cloud storage provider, noting that "[a]lthough several courts have extended BIPA to apply to third-party providers that supply biometric collection technology and services, no case has extended BIPA to vendors for such third-party providers." *Jones v. Microsoft Corp.*, No. 22-CV-3437, 2023 WL 130495, at *4 (N.D. Ill. Jan. 9, 2023). The court held that merely providing cloud storage services, even to third-party biometric vendors, did not equate to collecting, capturing, or otherwise obtaining biometric data under BIPA Section 15(b). *Id.*

## BIPA Issues Recently Addressed in Illinois Supreme Court

The Illinois Supreme Court recently decided two key issues under the BIPA.

First, on February 2, 2023, the Illinois Supreme Court addressed the statute of limitations under the BIPA. In *Tims v. Black Horse Carriers Inc.*, 2023 IL 127801, the Illinois Supreme Court heard an appeal from the Illinois First District Appellate Court's decision that a one-year statute of limitations applies to BIPA Section 15(c) and 15(d) claims, and that a five-year statute of limitations applies to BIPA Section 15(a), 15(b), and 15(e) claims. The Illinois Supreme Court "acknowledge[s] that the one-year statute of limitations could be applied to subsections (c) and (d)" but also looked at the intent of the legislature. The court held "because the Act does not have its own limitations period; because the subsections are causes of action 'not otherwise provided for'; and because we must ensure certainty, predictability, and uniformity as to when the limitations period expires in each subsection, the Act is subject to the default five-year limitations period found in section 13-205 of the Code."

Second, the Illinois Supreme Court issued the long awaited *Cothron* decision addressing claim accrual under the BIPA. In a 4-3 decision, the court held "that the plain language of section 15(b) and 15(d) shows that a claim accrues under the Act with every scan or transmission of biometric identifiers or biometric information without prior informed consent." (emphasis added). Importantly, the court also held that damages under the BIPA are discretionary and not mandatory and that courts have equitable discretion to fashion appropriate damages awards.

Cothron, a manager at White Castle, alleged she was required to submit her fingerprint repeatedly as part of her employment. White Castle filed a motion for judgment on the pleadings, arguing that Cothron only suffered an injury under the BIPA in 2008, the first time the company collected or disclosed her biometric data without consent, and not on every occasion on which she scanned her finger. White Castle argued that Cothron's claim was therefore barred by the statute of limitations. The federal district court denied White Castle's motion, holding that a statutory violation occurred and Cothron was injured every time her biometrics were collected. The district court then certified the question to the Seventh Circuit, which certified the question to the Illinois Supreme Court.

The court acknowledged that its per-scan approach could lead to massive statutory damages but held that this was largely an issue for the legislature. The court did state, however, that statutory damages under the BIPA are discretionary, not mandatory, and that courts can fashion damages awards that "(1) fairly compensat[e] claiming class members and (2) includ[e] an amount designed to deter future violations, without destroying defendant's business." The court further added that "there is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business."

[39] *Guszkiewicz v. Beelman Truck Co.*, No. 2021-L-1248 (DuPage Cnty., Ill., Nov. 2, 2022).

Morgan Lewis

# EUROPEAN UNION & UNITED KINGDOM

Authors: Pulina Whitaker, William Mallin

# INTERNATIONAL DATA TRANSFERS

The governance of international transfers of personal data continues to develop in the European Union and the United Kingdom.

Given the relative strength of the GDPR in comparison to privacy legislation in other countries and regions, EU- and UK-based individuals risk losing the protection of their personal data under European privacy legislation when their personal data is transferred to other countries. As a result, the EU and UK GDPR contain rules about international transfers of personal data where the receiver is a separate controller or processor and legally distinct from the exporter. If the transfer is not covered by an adequacy decision, the transfer must be covered by an appropriate safeguard. One commonly adopted example of an appropriate safeguard is the European Commission–approved EU SCCs.

## New EU Standard Contractual Clauses (EU SCCs)

On June 4, 2021, following the Court of Justice of the European Union's judgment in the high-profile *Schrems II* judgment, the European Commission issued modernized standard contractual clauses under the EU GDPR replacing the three sets of SCCs that were adopted under the previous EU Data Protection Directive. Since September 27, 2021, it has no longer been possible to conclude contracts incorporating the earlier set of SCCs.

Until December 27, 2022, controllers and processes could continue to rely on those earlier SCCs for contracts that were concluded before September 27, 2021, provided that the relevant processing operations remain unchanged.

## UK Standard Contractual Clauses (UK SCCs)

In light of Brexit, the new EU SCCs were never valid for use with respect to UK personal data transfers outside of the UK to third countries. Controllers and processors were expected to rely on the prior version of the EU SCCs until the UK published its own version.

On February 2, 2022, two sets of UK SCCs were laid before parliament: (1) the new International Data Transfer Agreement (IDTA); and (2) the new International Data Transfer Addendum to the EU SCCs (the Addendum).

Transitional provisions were put in place that allowed controllers and processors to use the old EU SCCs implemented before September 21, 2022 until March 21, 2024, unless the underlying processing operations changed before March 21, 2024. Since September 21, 2022, controllers and processors transferring personal data outside of the UK to third countries have had to incorporate either the IDTA or the Addendum.

The IDTA is best used where only personal data of UK data subjects is being transferred to a third country (i.e., a country that does not benefit from an adequacy decision from the UK's privacy regulator). Where personal data of both UK- and EU-based persons is being transferred within the relevant processing arrangements, the UK Addendum to the EU SCCs is the more practical choice. The Information Commissioner's Office (ICO) guidance and tools on how to use the IDTA, and on each clause of the IDTA, is expected in the first half of 2023.

Morgan Lewis

## *Schrems II* Undermining the EU-US Privacy Shield – Future Reform?

### Background

The judgment in *Schrems II* on July 16, 2020 found that the EU-US Privacy Shield framework no longer provides adequate safeguards for the transfer of personal data to the United States from the European Economic Area (EEA). Many organizations have continued (or at least their privacy documentation suggests that they continue) to rely on the EU-US Privacy Shield framework as their method of transferring personal data between the EEA and the United States, despite this being invalid.

### EU-US Transatlantic Data Privacy Framework

On March 25, 2022, the European Commission and US President Biden announced that they had reached an agreement in principle on a new EU-US Data Privacy Framework. It was suggested that this new framework would address the concerns raised in the *Schrems II* decision. On October 7, 2022, President Biden signed an executive order on "Enhancing Safeguards for United States Signals Intelligence Activities". This executive order implements into US law the agreement in principle announced in March 2022. The executive order introduces new binding safeguards to address all the points raised in the *Schrems II* decision, limiting access to EU data by US intelligence services and establishing a Data Protection Review Court.

On December 13, 2022, the European Commission published its draft adequacy decision. Once approved, following a consultation process that involves obtaining an opinion from the European Data Protection Board and approval from a committee made up of EU member state representatives, personal data will be able to flow freely between the EU and US companies certified under the new framework without additional safeguards needing to be implemented. In theory, the EU-US Data Privacy Framework could be completed during Summer 2023, three years following the invalidation of the EU-US Privacy Shield.

The United Kingdom is expected to seek a similar arrangement for UK-US data transfers.

It is likely that NOYB Chairman Max Schrems will raise a "*Schrems III*" case over any approved adequacy decision. Doubt has already been expressed regarding the draft decision concerning how equivalence has been drawn from the US framework to EU standards.

## Risk Assessments

Controllers and processors who transfer personal data outside of the United Kingdom or EEA under an Article 46 UK/EU GDPR transfer mechanism (for example, SCCs) must carry out a transfer risk assessment (TRA). This rule is derived from the *Schrems II* judgment.

The UK privacy regulator published new guidance on TRAs on November 17, 2022.

The intention behind a TRA is to evidence that the transfer mechanism selected will provide an appropriate safeguard, and effective and enforceable rights for data subjects.

The risks that must be considered in a TRA are

- risks to people's rights arising in the destination country from third parties accessing the information that are bound by the Article 46 transfer mechanism, in particular government and public bodies; and
- risk to people's rights arising from difficulties enforcing the Article 46 transfer mechanism.

EU regulatory guidance suggests that an assessment is carried out whereby the laws and practices of the exporting country are compared to the laws and practices of the importing country. This involves looking at the safeguards in place about third-party access to the information, in particular by governments. The

safeguards in place in the importing country do not need to be identical to the exporting country, but must be sufficiently similar.

As an alternative to the method endorsed by EU regulatory guidance, the UK's privacy regulator has also developed a TRA tool for controllers and processors to use by way of a TRA. This involves a six-question assessment; the template is available on the ICO's website.

It is expected that evidencing compliance with this requirement will become increasingly important in light of certain countries (for example, China) introducing increasingly powerful requirements for data to be transferred to local authorities.

## DATA BREACH DEVELOPMENTS

The latest 2022 UK government figures state that 39% of UK businesses identified a cyberattack in the preceding 12 months, which is the same percentage as last year but slightly less than 2020 (46%). The most common threat vector was phishing attempts (83%). It has been reported that ICO fines have increased threefold between November 2021 and October 2022 (from £4,848,00 in the previous 12 months to £15,249,200).

High-profile data breaches across the EU/UK in 2022 include the following:

- €405 million fine for Instagram in Ireland (second largest fine under the EU GDPR) resulting from Instagram's default account setting for business account users, which allowed email addresses and phone numbers of children to be exposed.
- €225 million fine for WhatsApp/Meta in Ireland (third largest fine under the EU GDPR) upheld by Court of Justice of the European Union following Meta's challenge.
- Potential £27 million fine for TikTok in the UK regarding non-consensual processing of minors' data, unlawful processing of special category data, and insufficient transparency.
- Clearview fined €20 million in France regarding non-compliance with a notice to remedy privacy violations.
- Easylife fined £1.48 million by the ICO for predicting customers' medical conditions using their personal data without their consent and targeting them with health-related products.

The ICO has recently announced a change in approach to publishing reprimands. In the past, companies could typically rely on their dealings with the ICO regarding data breaches being kept confidential. This is no longer necessarily the case. In early December 2022, the ICO published its reprimands from January 2022. Some of the information now publicly available includes details of organizations' data breaches and resulting reprimands.

## ANALYTICAL COOKIES

Interest in the use of analytical cookies has increased over the last year following complaints from None of Your Business (NOYB), an Austrian non-profit organization established with the aim of strengthening individuals' privacy rights. NYOB has issued complaints in all 30 EEA member states against 101 European companies. Many tracking technologies commonly used on websites in the EU are offered by companies based in the United States. Subsequently, use of such tools may involve the transfer of data to a third country (the United States), which means that the requirements in Chapter V of the GDPR must be met. NOYB has claimed that personal data has been transferred to the United States using Google Analytics and Facebook Connect in violation of the GDPR as these requirements are not met.

This has resulted in several regulatory decisions being issued in the EU. This pattern is expected to continue into 2023. The use of analytical cookie tools Google Analytics and similar tracking devices using cookies has faced scrutiny from several European regulators, including those in Austria, France, Italy, Germany, Liechtenstein, Norway, Denmark, and the Netherlands. Some authorities have banned the use of Google Analytics transfers to the United States without supplemental measures additional to those already provided by Google. Guidance has also been issued by those authorities still investigating NOYB complaints such as the Dutch Autoriteit Persoonsgegevens.

The overall effect of the judgments summarized below is the need for EU website operators to give greater consideration to the use of analytical cookie tools that transfer personal data to the United States. Corporations should be analyzing their cookies use—particularly any use of Google Analytics—to mitigate enforcement risks and adapt accordingly while monitoring developments.

## Austria

On December 22, 2021, the Austrian Data Protection Authority found that use of Google Analytics cookies by Austrian website operators violated Chapter V of the GDPR and the *Schrems II* judgement. The Austrian Data Protection Authority found that personal data was collected and transmitted to Google in the United States. The SCCs did not ensure an adequate level of protection within the meaning of the GDPR in light of potential surveillance of electronic communication services by US intelligence agencies.

## European Data Protection Supervisor Decision

The European Data Protection Supervisor (EDPS) decision on January 5, 2022 involved the use of cookies on a European Parliament (EP) website and related transfers of personal data of staff to a company based in the United States using Google Analytics tools. The EDPS issued a reprimand to the EP, as it was found that the EP did not have any evidence concerning the contractual, technical, or organizational measures ensuring an equivalent level of protection for the personal data. The EDPS stated that using SCCs is not a substitute for the individual assessment of each transfer that must be conducted by the data controller in accordance with *Schrems II*.

## France

The French Commission (CNIL) issued a decision on February 10, 2022 finding that personal data transfers using Google Analytics are unlawful. French operators were ordered to cease using Google Analytics if necessary to comply with GDPR requirements and to use alternative tools that do not require the transfer of data out of the European Union. The CNIL also stated their intention to examine other analytical cookie tools and tracking technologies that transfer personal data from the EU to the United States.

## Italy

On June 23, 2022, the Italian Garante ruled against data transfers to the United States using Google Analytics. Companies found in violation have 90 days to rectify issues. The Garante said the decision stems from "a series of complaints and in coordination with other European privacy authorities."

## Denmark

The Danish Datatilsynet held on September 21, 2022 that a website operator's legitimate interests to gain a more in-depth understanding of browsing behavior does not outweigh the legitimate privacy interest of the data subject. The Danish Datatilsynet held that Google did not take sufficient supplemental measures in addition to the SCCs to protect data transfers from the European Union to the United States. The Danish authority noted the shared view of other European regulators representing "a pan-European attitude among the supervisory authorities."

# FUTURE DEVELOPMENTS

## AI Regulation

EU policymakers will continue to seek to address emerging AI technologies. On April 21, 2021, the European Commission proposed new rules and actions in an effort to turn Europe into a global hub for "trustworthy" artificial intelligence (AI Act). This is a wide-reaching standard aimed at both harmonizing the ethical use of AI and strengthening AI's position in the EU. The AI Act consists of the first legal framework on AI and a new coordinated plan specifically aimed at guaranteeing the safety and fundamental rights of people and businesses while simultaneously strengthening AI innovation across the EU. The coordinated plan provides an outline of the necessary policy changes and investment among members states to bolster Europe's position in developing a human-centric, sustainable, trustworthy, and secure AI.

On December 6, 2022, the European Council adopted its position concerning the AI Act, in which various amendments are suggested. The European Council may enter into negotiations with the European Parliament once it has adopted its own position in order to reach an agreement on the proposed AI Act. It is intended for agreement to be reached in early 2023 to allow for implementation during the course of 2024.

## AI Act – Key Points

The definition of AI systems in the AI Act is wide in scope: "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."

Annex I of the AI Act includes machine-learning approaches, logic, as well as knowledge-based and statistical approaches.

The proposed AI Act applies to the following:

- Providers of AI systems in the EU
- Users of AI systems located within the EU
- Providers and users of AI systems that are located outside the EU if the output produced by the system is within the EU

The following AI systems are identified as "high risk":

- Safety components of products (such as toys, machinery, and medical devices)
- Systems used to evaluate creditworthiness, biometric identification, and critical infrastructure

Providers of these systems will be required to register their systems in an EU-wide database before they are marketed or put into service, and will be subject to various other obligations.

Certain AI systems are prohibited under the AI Act because of the "unacceptable risk" they create, including those that

- deploy subliminal techniques beyond a person's consciousness to materially distort the person's behavior and cause harm;
- exploit any of the vulnerabilities of a specific group of persons to materially distort the person's behavior and cause harm;

- evaluate/classify the trustworthiness of natural persons, i.e., social scoring; and
- use "real-time" remote biometric identification systems in publicly accessible spaces for law enforcement.

Other AI systems may be characterized as presenting "limited risk," and such systems will be subject to a limited set of transparency obligations.

It is proposed that fines of up to €30 million or 6% of total worldwide annual turnover (whichever is higher) will apply to providers contravening the AI Act.

## Regulation of AI in the UK

The AI Act will not apply directly in the United Kingdom, yet it is still relevant to UK businesses as a result of its extraterritorial reach. The UK has announced a 10-year plan to make the UK an "AI Superpower" in its National AI Strategy. From a privacy perspective, the UK needs to maintain data protection equivalence with the UK to maintain its adequacy status, which can be revoked at any time by the European Commission, but which is otherwise expected to last until June 2025 and be up for renewal at that time. The UK government's white paper on proposals to regulate AI is expected shortly, as is the House of Commons' inquiry into the governance of AI.

## Information Commissioner's Office Guidance on AI

In July 2020, the ICO issued a framework for auditing the impact of AI, comprising the following:

- Auditing tools and procedures that the ICO will use in audits and investigations
- The ICO detailed guidance on AI and data protection
- A toolkit designed to provide further practical support to organizations auditing the compliance of their own AI systems.

In 2022, the ICO issued its toolkit, which acts as a practical checklist of the key data protection issues that need to be considered by organizations from the outset of any project that they are planning. The ICO acknowledges that the toolkit is not "a pathway to absolute compliance with data protection law"—but is a strong starting point.

The ICO published a paper in August 2021 in which it provides its support to the Commission's proposals on artificial intelligence and the AI Act. It also published guidance on AI and data protection.

In conjunction with the Alan Turing Institute, it also published guidance on explaining AI decisions.

## ePrivacy Regulation

The ePrivacy Regulation regulates the use of electronic communications services within the European Union. The intent of this regulation is to replace the Directive on Privacy and Electronic Communications (Directive 2002/58/EC) and specify additional requirements that companies operating in the digital economy need to satisfy in relation to the processing of personal data.

Although intended to apply from May 2018 alongside the GDPR, EU member states have yet to agree on draft legislation. In 2017, the EU Commission presented a first draft, and the EU Parliament adopted an amended draft. This was followed by drafts from European Council presidencies in Estonia, Bulgaria, Austria, Romania, Finland, Croatia, and Germany. In 2021, a new draft of the ePrivacy Regulation was approved, and the trilogue negotiations (between the European Parliament, Council, and Commission) officially began.

Negotiations are still ongoing. A potential transitional period of 24 months means that any new regulations would not come into effect before 2025, if the ePrivacy Regulation comes into force in 2023 as expected.

## Cookie Consents

### Summary of Current Requirements for Use of Cookies

Website operators must

- communicate to users if they have set cookies;
- clearly explain what the cookies do and why; and
- obtain actively and clearly given consent from the user to allow the storing of non-essential cookies on their device.

### Recent Proposals for Future UK Privacy Reform

On June 23, 2022, the UK government responded to the September 10, 2021 consultation from the Department for Digital, Culture, Media and Sport titled, "Data: a new direction."

The initial consultation included proposals to reduce burdens on businesses by (among other things) limiting cookie banners by altering the Privacy and Electronic Communications Regulations (PECR) rules and removing consent requirements in relation to audience measurement cookies. The majority of respondents to the initial consultation agreed that organizations should be able to use cookies (and similar technologies) without consent for a wider range of non-intrusive purposes, including cookies allowing organizations to measure webpage traffic and improve offerings to users. Most respondents disagreed with removing the consent requirement for cookies completely and argued that users should be given clearer information on intrusive varieties that collect personal data for the purposes of real-time bidding and micro-targeting of advertisements.

In its response, the UK government stated an intention to legislate to remove the need for websites to display cookie banners to UK residents. Cookies (and similar technologies) used for non-intrusive purposes will be permitted to be placed on a user's device without explicit consent in the immediate term. In the future, the government plans to move to an opt-out method of consent for cookies. This would mean that cookies could be set without seeking consent as long as the website provided clear information on how to opt out. The opt-out model would not apply to websites likely to be accessed by children.

The new Data Protection and Digital Information Bill has now been approved in the United Kingdom. The headline points are as follows:

*Definition of Scientific Research Updated*

There will be a new definition of scientific research: allowing processing that "could reasonably be described as scientific" and could include activities such as innovative research into technological development.

The government states that this is because current data laws are unclear on how scientists can process personal data for research purposes. It would mean that commercial organizations could now benefit from the same freedoms as academics to carry out innovative scientific research (this might include reusing data for research purposes).

*Paperwork Will Supposedly Be Reduced*

The bill removes the requirement for all businesses to keep data processing records. Only organizations whose processing activities are "likely to pose high risks to individual's rights and freedoms" will need to keep processing records—including, for example, personal health data.

*AI Technologies*

The United Kingdom's current data protection laws lack clarity in this area. The bill ensures greater clarity about when safeguards apply in relation to AI. Under the new bill, people will be made aware when decisions are made using AI, and they can challenge these decisions and seek human review if the decisions are inaccurate or harmful.

*Data Sharing*

The government states that the bill is compatible with the GDPR and any other data regimes, and that businesses can continue to "trade freely with global partners."

Businesses are meant to continue to use their "existing international data transfer mechanisms to share personal data overseas if they are already compliant with current UK data laws." In reality, this means that British businesses are not subject to further fees or required to carry out further checks to demonstrate that they are compliant with the updated rules.

*Information Commissioner's Office*

The ICO will be strengthened by creating a statutory board with a chair and chief executive. This will allow it to better support organizations to comply with data regulation.

*Consent*

Some have suggested that the government is keen to provide companies with "greater confidence" about when they can process user data without consent—for example, for "certain public interest activities" in relation to law enforcement and protecting vulnerable people. This is likely to have a large impact on technology companies, marketing, and the use of cookies, with an expanded range of exemptions to consent for cookies and reducing the number of consent pop ups people encounter online.

In addition to the Data Protection and Digital Information Bill, the UK Parliament is currently debating a draft bill called the "Defamation, Privacy, Freedom of Expression, Data Protection, Legal Services and Private Investigators Bill." The draft includes proposals regarding the application of privacy rights and freedom of expression in civil cases on matters of public interest, regulations of lawyers and proposals to reduce the use of lawsuits for strategic purposes (known as "lawfare").

# UNITED ARAB EMIRATES

Authors: Ksenia Andreeva, Jessica Christensen

## BACKGROUND (SCOPE/APPLICABILITY/PURPOSE)

The United Arab Emirates' comprehensive data protection legislation—Federal Decree Law No. 45 of 2021—made its debut on November 27, 2021 and came into effect on January 2, 2022. This decree, otherwise known as the Personal Data Protection Law (PDPL), marks the first time that the UAE has begun to regulate data privacy on a federal level. The Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM) each have their own set of data privacy rules which will continue to govern the entities operating within their respective jurisdictions.

While the PDPL contains the basic framework for how the data privacy regime will operate, the UAE government has yet to release the Executive Regulations—a set of rules governing the specific application and enforcement of the law. The Executive Regulations are expected to be published in 2023.

Even though the Executive Regulations have not been released, it is imperative that corporations with connections to the UAE are familiar with the general parameters of the law as it stands. Once the Executive Regulations are released, all companies that are subject to its regulation will only have a six-month grace period to become compliant before the actual implementation and enforcement of the law.

The PDPL has broad application for the processing of personal data. Its provisions apply to the processing of personal data, whether in full or part through electronic systems, inside or outside the UAE. In particular, the law applies to (1) any data subject who resides or has a place of business in UAE, (2) any data controller or processor located in the UAE that processes personal data, and (3) any data controller or processor located outside the UAE that processes personal data of data subjects who are inside the UAE.

## LEGAL BASIS FOR DATA PROCESSING

The universally sufficient legal ground for processing personal data under the PDPL is a data subject's consent. The law generally prohibits the processing of personal data without consent, except for some limited instances in which the processing is necessary to protect a public interest or to carry out any of the legal procedures and rights. The PDPL also allows processing personal data without consent, when it is necessary to protect the interests of the data subject, or for the performance of a contract to which the data subject is party.

Unlike the EU's GDPR, there is no legitimate business interest concept for data collection and processing. That said, processing necessary for a data controller to carry out legal obligations in the fields of recruitment, social security, or social protection or otherwise in compliance with the UAE laws does not require data subject's consent.

The PDPL requires the data controllers and data processors to stop any data processing if the individual's consent is withdrawn; however, such withdrawal shall not affect the legality and lawfulness of the processing made based on the consent given prior to the withdrawal.

## COMPLIANCE PROCEDURES

Under the PDPL, any data processing activity should comply with the key principles that are generally similar to the GDPR. Notably, the PDPL does not explicitly list the principles; instead, they are embedded in the requirements and set the foundation for compliance. These principles include the following:

- Lawfulness, fairness, and transparency of data processing
- Purpose limitation in all cases, when the law allows processing data
- Data minimization to ensure that in no case is any excessive data processed
- Accuracy in processing to ensure that the data is up to date
- Storage limitation to avoid accumulation of data that is no longer needed or allowed for processing
- Integrity and confidentiality as fundamental principles for building security measures to protect processed data
- Accountability for compliance for all parties involved (both data controllers or data processors)

The PDPL requires data processors and data controllers to work together to prevent the unauthorized disclosure of personal data. This is achieved through a set of organizational and security measures to be taken to protect the privacy of processed data.

Organizational measures include adoption of policies (such as record of processing activities) and procedures aimed at compliance with data minimization and purpose limitation principles, including internal awareness trainings. Security or technical measures can include, but are not limited to, things such as data disposal mechanisms, anonymization of information, encryption, passwords and two step authentication, and system and physical security.

## DATA PROTECTION OFFICER

Article 10 of the PDPL introduces the role of the data protection officer (DPO)—an individual appointed by data controllers and processors to manage a company's internal compliance with the law. The appointed individual can be either an existing employee of, or may be otherwise authorized by, the data controller or data processor. Notably, the PDPL expressly allows the DPO to work from outside the UAE, if need be, and requires this individual to have "sufficient skills and expert knowledge in personal data protection."

The PDPL requires the appointment of a DPO for entities that (1) process a high volume of sensitive personal data, (2) process sensitive personal data in a comprehensive and systematic way, or (3) if the processing would cause a high-level risk to the confidentiality and privacy of the personal data of the data subject as a result of adopting technologies that are new or associated with the amount of data. All the details of these requirements are to be further explained in the Executive Regulations. From a practical standpoint, the appointment of the DPO is recommended in all cases when a data controller or data processor resides in UAE.

Generally, the DPO is responsible for ensuring compliance with the PDPL, the Executive Regulations, and any other instructions regarding data privacy as issued by the Data Protection Authority. More specifically, the DPO is expected to act as a liaison between the data controller and processors, ensure that the policies and procedures they have established are valid and effective, and oversee the implementation of the PDPL. Additionally, the DPO should provide technical advice, including risk assessments and advice related to the periodic examination of their data privacy policies. Additional duties or powers of the DPO may be included in the Executive Regulations.

## CROSS-BORDER DATA TRANSFERS

In addition to a general requirement of the PDPL for any data controller to ensure that the third-party recipients of personal data implement appropriate safeguards to satisfy the requirements of the PDPL and to ensure ongoing compliance with it, Articles 22 and 23 of the PDPL specifically govern cross-border data

transfers. Article 22 authorizes international data transfers to either (1) countries that have an "adequate level of protection" for personal data in their own legislation or (2) countries that have made an international agreement with the UAE regarding personal data protection between the two countries. Article 23 provides a list of exceptions to Article 22, including the option for corporations to enter into data-transfer contracts that would provide the requisite level of personal data protection. The Executive Regulations are supposed to provide the list of countries that have an "adequate level of protection."

Because the PDPL was largely modeled after the GDPR, some speculate that most, if not all, countries within the EU will be considered to have met the PDPL's adequacy threshold as well.

Notably, the United States and United Arab Emirates have, earlier in 2023, released a Joint Statement on Cross Border Privacy Rules, which indicates only that the US and UAE "intend to promote adoption and implementation of policies and rules in our bilateral and multilateral economic relationships" to protect data that is transferred internationally. The Joint Statement does not reveal whether the UAE will consider the current US data privacy laws to be "adequate"—it is unclear whether the piecemeal data privacy law currently employed by the US will meet this requirement.

However, the Joint Statement should provide some optimism that a resolution or agreement between the US and UAE is in the works, which would presumably mean that companies would be able to follow some future guideline rather than attempting to regulate their data processors' behavior on a contract-by-contract basis.

## DATA PROTECTION AUTHORITY

With a separate federal decree (Law No. 44/2021), a dedicated state authority on a federal level to deal with privacy matters (the Authority) is supposed to be established. To date, the Authority has not yet been established. Interestingly, under Article 3 of the PDPL, the Authority has the right to exempt certain companies from the scope of the PDPL at its own discretion provided that these companies do not process a large amount of personal data. It remains to be seen how the Authority will use this discretion , when established.

## DATA BREACH

Under the PDPL, data controllers must immediately notify the Authority in the event of any data breach. If the data breach impacts individuals' personal data, the data controller must also notify the individuals whose data has been affected. The PDPL provides for detailed rules on who and when the Authority should be notified and what the notification should contain. Upon receipt of the notification from the data controller, the Authority is to conduct its own internal investigation and then impose administrative penalties (to be defined in the Executive Regulations) on either the data controller or data processor.

## THINGS TO LOOK FOR IN 2023 IN THE PRIVACY SPACE

The year ahead will bring a number of developments in the privacy space that Morgan Lewis will continue to report on, including the following:

- The China SCC and Standard Contract Provision will become effective on June 1, 2023.
- New US state consumer privacy laws will take effect in January (California Privacy Rights Act and Virginia Consumer Data Protection Act), July (Colorado Privacy Act and Connecticut Data Privacy Act), and December (Utah Consumer Privacy Act).
- Guidance from the UK ICO on the new International Data Transfer Agreement is expected in the first half of 2023.
- The EU's ePrivacy Regulation is expected to come into force in 2023.
- The UAE's comprehensive data protection legislation regulations are expected to be published in 2023.

Morgan Lewis

## CONTACTS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:


**Philadelphia**

| | | |
|---|---|---|
| Tess Blair | +1.215.963.5161 | tess.blair@morganlewis.com |
| Ezra D. Church | +1.215.963.5710 | ezra.church@morganlewis.com |
| Gregory T. Parks | +1.215.963.5170 | gregory.parks@morganlewis.com |
| Kristin M. Hadgis | +1.215.963.5563 | kristin.hadgis@morganlewis.com |
| Kathryn E. Deal | +1.215.963.5548 | kathryn.deal@morganlewis.com |
| Terese M. Schireson | +1.215.963.4830 | terese.schireson@morganlewis.com |
| William Childress | +1.215.963.4999 | william.childress@morganlewis.com |

**London**

| | | |
|---|---|---|
| Pulina Whitaker | +44.20.3201.5550 | pulina.whitaker@morganlewis.com |
| William Mallin | +44.20.3201.5374 | william.mallin@morganlewis.com |

**Chicago**

| | | |
|---|---|---|
| Elizabeth B. Herrington | +1.312.324.1445 | beth.herrington@morganlewis.com |
| Benjamin Kabe | +1.312.324.1707 | benjamin.kabe@morganlewis.com |

**San Francisco**

| | | |
|---|---|---|
| W. Reece Hirsch | +1.415.442.1422 | reece.hirsch@morganlewis.com |
| Carla B. Oakley | +1.415.442.1301 | carla.oakley@morganlewis.com |
| Kevin M. Benedicto | +1.415.442.1340 | kevin.benedicto@morganlewis.com |

**Paris**

| | | |
|---|---|---|
| Charles Dauthier | +33.1.53.30.44.74 | charles.dauthier@morganlewis.com |

**Silicon Valley**

| | | |
|---|---|---|
| Mark L. Krotoski | +1.650.843.7212 | mark.krotoski@morganlewis.com |

**Washington, DC**

| | | |
|---|---|---|
| Ronald W. Del Sesto, Jr. | +1.202.373.6023 | ronald.delsesto@morganlewis.com |
| Dr. Axel Spies | +1.202.373.6145 | axel.spies@morganlewis.com |

**Dubai**

| | | |
|---|---|---|
| Ksenia Andreeva | +971.4.312.1865 | ksenia.andreeva@morganlewis.com |


## ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.