Skadden

Privacy & Cybersecurity Update

Illinois Supreme Court Holds That Workers' Compensation Law Does Not Bar BIPA Claims

The Illinois Supreme Court ruled on February 3, 2022, that the Illinois Workers' Compensation Act (IWCA) does not preempt claims for statutory damages under the Biometric Information Privacy Act (BIPA).

In its decision, the Illinois Supreme Court ruled 7-0 that BIPA violations are not preempted by the IWCA.[1] The IWCA states that it provides the exclusive remedy for workplace injuries and, accordingly, has been cited by certain employers accused of BIPA violations in the workplace as a bar to BIPA claims by employees. The Illinois Supreme Court found that BIPA, which was passed after the IWCA, makes clear that state lawmakers did not intend the IWCA to preempt claims under BIPA, because BIPA specifically states that the written consent required prior to the collection of biometric data may include "a release executed by an employee as a condition of employment." The ruling eliminates a defense frequently invoked by employers in response to claims of BIPA violations in the workplace, which often arise in connection with the use of fingerprint scans for timekeeping purposes.

Background

Under BIPA, companies must obtain written consent before collecting, using or storing Illinois residents' biometric data, such as fingerprints or facial scans.

In *In re: Marquita McDonald v. Symphony Bronzeville Park LLC*, first filed in 2017, a former employee of a Chicago nursing home sued her employer for liquidated damages because it required employees to provide fingerprints for a timekeeping system without obtaining the employees' written consent. In response, the employer argued the BIPA claim was barred by the IWCA, because the latter provides the exclusive remedy for workplace injuries. However, the Illinois Supreme Court affirmed an appellate panel decision that found unlawful collection of the plaintiff's personal information does not constitute a compensable injury under the IWCA. Thus, the justices said, the employee's BIPA claim could proceed.

Ruling

The justices distinguished violations of BIPA, ruling that they are different in nature and scope than other injuries that occur in the workplace. Unlike workplace injuries that are

[1] Please see the decision in *Marquita McDonald, Appellee, V. Symphony Bronzeville Park, LLC, et al*.

compensable under the IWCA, the court said, BIPA violations do not negatively impact an employee's ability to work. As such, the court ruled that the exclusive remedy provision of the IWCA does not bar claims under BIPA.

The court has yet to rule on the extent of damages that will be available to potential plaintiffs. For reference, violations of BIPA can result in liquidated damages of up to $5,000 per violation, plus attorneys' fees. Whether damages will be calculated based on each time a company collects an employee's biometric information without consent, or only the first such violation, remains an open question. If each such BIPA violation were to constitute a separate injury, the amount of associated statutory damages in the context of employee timekeeping may be significant.

Key Takeaways

In this case, the Illinois Supreme Court clarified that employers can be liable under BIPA for the failure to obtain employees' consent prior to collecting biometric data in the workplace. Until the question regarding the extent of damages for which employers may be liable is settled, employers face the possibility of statutory damages assessed on the basis of each instance of collection. Accordingly, to mitigate the risk of liability for BIPA violations, employers that collect, use or store biometric data of Illinois employees should ensure that they have policies and procedures in place to comply with BIPA.

Return to Table of Contents

Three Recent Decisions by Data Protection Authorities Will Impact European Advertising Industry

Three recent decisions of data protection authorities in Europe — Datenschutzbehörde (the Austrian DPA), Commission nationale de l'informatique et des libertés (the French DPA) and Autorité de protection des données (the Belgian DPA) — will impact how the advertising industry operates on the continent. The decisions of the Austrian and French DPAs represent the first two decisions on the 101 model complaints filed against a wide range of data exporters across Europe by the NGO Noyb for their alleged continued transfer of personal data to Facebook or Google in the U.S. in breach of *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II)* and the General Data Protection Regulation (GDPR). The decisions by the Austrian and French DPAs particularly focus on the use of Google Analytics by organizations in Europe, while the decision by the Belgian DPA addresses whether the Transparency and Consent Framework (TCF), which is used by much of the advertising industry in Europe, is GDPR-compliant.

The Austrian DPA Decision[2]

In this case, the data subject visited a website hosted by an Austrian company while logged into his Google account. The website used Google Analytics, a tool used to track and measure website use. This resulted in the transfer of personal data (*i.e.*, user identifiers, IP address and browser parameters) from the Austrian company, as a data controller, to Google in the U.S., as a data processor. The Austrian company and Google had entered into controller-to-processor standard contractual clauses (SCCs) as the legal mechanism for the transfer of personal data with regard to Google Analytics. However, the Austrian DPA held that the transfer of personal data was in breach of the GDPR transfer provisions. In particular, the Austrian DPA made the following key points:

- Following the decision of *Schrems II*, the Austrian DPA held that SCCs alone cannot offer an adequate level of protection for transferred personal data without a further and specific assessment of the level of protection in the recipient country. In this case, the Austrian DPA stressed that Google qualifies as an "electronic communication service provider" under 50 U.S. Code Section 1881(b)(4) and is therefore subject to surveillance by U.S. intelligence services. This meant that U.S. intelligence services could, in theory, access the transferred personal data.
- Supplementary measures implemented by the Austrian company and Google to safeguard the transfer of personal data — namely involving encryption, with Google having access to the encryption key — were insufficient. The Austrian DPA held that supplementary measures must precisely address specific deficiencies in the protection of personal data in the recipient country and, in particular, would have to prevent access to the transferred personal data by U.S. intelligence services. Encryption could not be considered to be a sufficient measure in this case given that Google had access to the encryption key and therefore could hand it over along with associated transferred personal data if required by U.S. intelligence services.

This decision is not final and can be appealed, and no penalties or corrective measures have been issued to date.

The French DPA Decision[3]

The French DPA's decision, which has not yet been published in full, involved a similar pattern and followed closely in line with the decision of the Austrian DPA. The French DPA echoed the view that transfers of personal data to the U.S. can only take place if appropriate and specific safeguards are implemented in

[2] An English translation of the Austrian DPA's decision is available here.

[3] The French DPA's official announcement is available here.

light of the nature of the transfer and the recipient country and, in this case, supplementary measures adopted by the unnamed French company involved in the case and Google to protect transferred personal data (*i.e.*, encryption) could not prevent access to the transferred personal data by U.S. intelligence services. The French DPA considered the French company to be in violation of the GDPR transfer provisions and ordered the company to bring its processing activities and associated transfer into compliance with the GDPR within one month, if necessary by ceasing to use Google Analytics (under current conditions) or by using an alternative tool that does not involve the transfer of personal data outside of the European Economic Area (EEA).

The Belgian DPA Decision[4]

In this case, the Belgian DPA fined IAB Europe (a European trade association for the digital marketing and advertising ecosystem) €250,000, ruling that its TCF, used by much of the advertising industry in Europe, is not GDPR-compliant. The TCF was developed by IAB Europe and was designed to ensure that all parties in the digital advertising chain complied with the GDPR and ePrivacy Directive in regards to the processing of personal data, including cookies, advertising identifiers, device identifiers and other tracking technologies. The TCF provides an interface whereby website publishers can inform visitors of which personal data is being processed and how their website and partner advertisers use such data. The Belgian DPA held that IAB Europe acts as a data controller for the registration of data subjects' marketing preferences that are stored on the TCF's "Consent String" (a coded character string that records data subjects' consent and marketing preferences), and held that IAB Europe had:

- failed to establish a legal basis for the processing of personal data on the Consent String, and offered inadequate grounds for subsequent processing by advertisers;
- provided generic and vague information to data subjects via the TCF's user consent management interface;
- failed to implement appropriate technical and organizational measures in accordance with the principle of data protection by design and data protection by default;
- failed to maintain a register of processing activities;
- failed to appoint a data protection officer; and
- failed to conduct a data protection impact assessment.

The Belgian DPA fined IAB Europe for several GDPR violations, and ordered it to bring its activities into compliance with the GDPR within six months. IAB Europe confirmed on February 11, 2022, that it will appeal the Belgian DPA's decision to the Market Court, a special section of the Belgian court system that handles appeals involving regulators.

[4]The Belgian DPA's decision is available here.

Key Takeaways

While the decisions of the Austrian, French and Belgian DPAs are not final and are open to appeal, the rulings nonetheless send a targeted message to the wider advertising industry in Europe. Organizations in Europe should be mindful of these decisions and the impact they may have on marketing practices and related data protection compliance. Organizations, specifically website publishers and advertisers, may need to monitor the development of the Belgian DPA's decision in relation to IAB Europe if they rely on the TCF for their advertising practices.

Return to Table of Contents

UK International Data Transfer Agreement and UK Addendum to EU Standard Contractual Clauses Laid Before UK Parliament

On August 11, 2021, the U.K. Information Commissioner's Office (ICO) initiated a period of public consultation on its International Data Transfer Agreement (IDTA) and U.K. Addendum to the EU SCCs. The consultation closed on October 11, 2021, and on January 28, 2022, the Department for Digital, Culture, Media and Sport laid the IDTA and U.K. Addendum before the U.K. Parliament. If no objections are raised, the IDTA and U.K. Addendum will come into force on March 21, 2022.

Background

Following *Schrems II*, whereby the E.U.-U.S. Privacy Shield was invalidated as a data transfer mechanism and enhanced due diligence requirements were imposed on companies seeking to rely on SCCs to transfer personal data to third countries, the European Commission published a new set of SCCs in June 2021. The new SCCs apply only to data transfers outside of the EEA and, following the U.K.'s withdrawal from the E.U., not the U.K. itself. Going forward there will be two options for restricted transfers of personal data under U.K. data protection laws:

- **The IDTA:** This will serve as the U.K. equivalent of the SCCs and function as a contractual mechanism to enable companies to transfer personal data outside of the U.K. to a country which has not received an adequacy decision.
- **U.K. Addendum**: The U.K. Addendum will attach to the new set of SCCs and will enable companies to utilize them for transfers of personal data outside of both the U.K. and EEA. The U.K. Addendum will be useful to companies with multinational operations because such companies can avoid having to enter into both the IDTA and a new set of SCCs for transfers outside of the EEA and U.K.

According to the ICO, the IDTA and U.K. Addendum can be used immediately by companies transferring personal data outside of the U.K., subject to the caveat that they come into force on March 21, 2022, and are awaiting approval from the U.K. Parliament.[5]

Timeline

Companies should be aware of the following key dates in relation to the implementation of the IDTA and U.K. Addendum:

- **March 21, 2022:** The IDTA or U.K. Addendum can lawfully be used as a data transfer mechanism for transfers of personal data from the U.K. to third countries.
- **September 21, 2022:** The old set of SCCs can no longer be used as a data transfer mechanism for transfers of personal data from the U.K. to third countries under new contracts.
- **March 21, 2024:** All contracts must incorporate either the IDTA or U.K. Addendum to legitimize personal data transfers from the U.K.

Key Takeaways

Companies should continue to update their template data transfer agreements to reflect the introduction of the IDTA and U.K. Addendum and ensure that a lawful data transfer mechanism is relied upon for international transfers of personal data in line with the U.K. GDPR. The ICO is expected to publish its responses to the consultation, as well as further guidance on the IDTA and U.K. Addendum, in due course.

Return to Table of Contents

Digital Advertising Watchdog Issues Compliance Warning for 'Fingerprinting'

The Digital Advertising Accountability Program (DAAP), a self-regulatory initiative that enforces industry principles for privacy in online advertising, warned that it will treat the use of "fingerprinting" for targeted advertising purposes as equivalent to cross-app data, which in turn may require companies to provide notice, enhanced notice or a consent right to data subjects.

On February 8, 2022, the DAAP issued a compliance warning regarding the practice of "fingerprinting" users or devices to generate targeted ads (the Compliance Warning).[6] This Compliance Warning was issued in the context of recent industry programs aimed at scaling back targeted advertising, such as Apple's implementation of the AppTrackingTransparency Framework, which requires that users be notified and given the ability to opt out when apps seek to track them across other apps or websites, and Google's decision to remove third-party cookies from its Chrome web browser.

DAAP, a division of the Better Business Bureau's National Programs that enforces industry self-regulation principles for data privacy in web and mobile advertising, was developed to support the Digital Advertising Alliance (DAA), a nonprofit industry trade association, and holds companies accountable to the DAA's Self-Regulatory Principles for Online Interest-Based Advertising (principles).[7] The principles are a set of best practices for the online and mobile interest-based advertising industry.

Under the principles, data collected from a particular device regarding application use over time and across non-affiliate applications constitutes "Cross-App Data." An entity that collects Cross-App Data and uses it for interest-based advertising (IBA) — or allows another entity to do so — may need to provide notice, enhanced notice or a consent right to users, depending on the entity's relationship to its users and the details of collection. In the Compliance Warning, DAAP clarified that Cross-App Data can include "fingerprinting," which occurs when different information gathered by an app is combined and used for IBA purposes. According to DAAP, such information may include, but is not limited to, the device IP address, platform, brand, model, carrier, OS version, screen resolution, processor or language settings, whether collected at once or over multiple sessions.

Key Takeaways

The Compliance Warning underscores the increased scrutiny of targeted advertising practices currently being undertaken by a number of regulatory bodies. DAAP itself noted that, while fingerprinting techniques are not new, they are becoming more widely used as access to other identifiers is curtailed. DAAP's renewed focus on fingerprinting recognizes that companies continue to seek alternate means of engaging in targeted advertising and reminds companies that the same principles apply to the use of a persistent identifier, regardless of the technology employed.

Return to Table of Contents

[5] Additional information about the IDTA and U.K. Addendum is available in our August 2021 *Privacy and Cybersecurity Update*.

[6] See DAAP release, "Compliance Warning Regarding Fingerprinting of Users or Devices."

[7] See here for the DAA's Self-Regulatory Principles.

NIST Publishes Recommended Criteria for Cybersecurity Labeling of Consumer Internet-of-Things Products

On February 4, 2022, the National Institute of Standards and Technology (NIST) published a cybersecurity white paper titled "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products" (the Recommended Labeling Criteria).[8] The paper identified critical elements for the creation of a labeling scheme applicable to consumer IoT products — internet-connected devices intended for personal, family or household use. Its release advances the goal of creating "product-focused outcomes that enable consumers to make informed decisions about purchasing and maintaining IoT products" and intend to serve as guidance toward the creation of national cybersecurity consumer IoT device labeling requirements.

NIST's Cybersecurity Labeling Directive and Purposes

President Joe Biden's May 2021 Executive Order on Improving the Nation's Cybersecurity[9] tasked NIST with developing cybersecurity labeling initiatives for consumer products, including "pilot product labeling programs to educate the public on the security capabilities of [IoT] devices." The Recommended Labeling Criteria was published in furtherance of this directive, outlining material considerations for the development of a cybersecurity labeling scheme for consumer IoT devices that a "scheme owner" — a public or private sector organization other than NIST — could devise.

The Recommended Labeling Criteria provide "minimum requirements and desirable attributes" for a labeling scheme, which aim to permit IoT device developers to adopt labeling practices with respect to a variety of IoT devices. The criteria apply to each component of an IoT device, including gateway hardware, companion app software and back ends, and address three main topics: (1) baseline product criteria, (2) labeling and (3) conformity assessments. High-level recommendations for each topic are set forth below.

Baseline Product Criteria

The following baseline product criteria recommendations set forth the cybersecurity expected of IoT devices and device developers as part of a labeling scheme.

1. **Asset Identification:** An IoT device should be uniquely identifiable by consumers and developers, and it should inventory all the device's components. Such identification would support asset management for updates, data protection and incident response capabilities.
2. **Product Configuration:** An IoT device's configuration should be modifiable so that consumers can tailor a device's functionality as needed, including to avoid specific cybersecurity threats.
3. **Data Protection:** An IoT device should protect the data it stores and transmits from unauthorized access, disclosure and modification.
4. **Interface Access Control:** An IoT device should restrict access to all internal and external interfaces to authorized individuals, services and components.
5. **Software Updates:** IoT devices should include secure, authorized software updates of all device components to address vulnerabilities.
6. **Cybersecurity State Awareness:** An IoT device should support cybersecurity incident detection. A device should alert the consumer of abnormal behavior (*e.g.*, detected botnet presence, malware or unauthorized access attempts) that was not caused by the consumer or planned by the developer.
7. **Documentation:** An IoT device developer should compile information relevant to a device's cybersecurity and make such documentation available both prior to consumer purchase and throughout the product lifecycle.
8. **Information and Query Reception:** An IoT device consumer should be able to contact the device developer for information related to the device's cybersecurity, as well as to ask questions and report issues that might improve the device's cybersecurity status.
9. **Information Dissemination:** An IoT device developer should communicate information relevant to cybersecurity, both publicly and directly to device consumers or others in the IoT product ecosystem.
10. **Product Education and Awareness:** An IoT device developer should continuously educate consumers on relevant cybersecurity information, including on how to change configuration settings and the cybersecurity implications of such changes; the importance of software updates; and vulnerability management, all in order to support safe, secure use of IoT devices and informed consumer decision making in the IoT marketplace.

[8] See here for the Recommended Labeling Criteria.

[9] Executive Order 14028 of May 12, 2021. Per the Executive Order, NIST was directed to develop criteria that "shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products."

Labeling Considerations

While NIST does not display a sample label design, the Recommended Labeling Criteria provide general design and functionality considerations, including the following:

- IoT device developers should employ a single binary label — a "seal of approval"-type indication that a product has met certain basic standards.
- A label should be "layered," directing consumers to additional device details online through a URL or scannable QR code.
- IoT device developers should be flexible in supporting digital and physical label formats and should test consumer reactions to usability, modulating formats accordingly.
- Labels should be available to consumers prior to, during and after purchase.
- Any labeling program should be accompanied by a "robust consumer education campaign."

NIST emphasized that the labels should be developed with the intent to "support non-expert, home users of IoT products," not a technically advanced audience.

Conformity Assessment Considerations

The Recommended Labeling Criteria sets forth options for conformity assessment mechanisms, which a scheme owner would tailor and implement to show a device's level of compliance with certain standards, including the recommended baseline criteria. NIST's recommended conformity assessment approaches include (1) self-attestation, where an IoT device supplier declares conformity against defined criteria; (2) third-party testing or inspection; and (3) third-party certification of a device. NIST recommends a variable approach to conformity assessment instead of one standard approach, given that consumer IoT devices have similarly variable risk profiles and exist in a space without clear international standards.

Key Takeaways

With the Recommended Labeling Criteria, NIST has identified central elements of a labeling scheme that would help consumers make informed decisions about the purchase and maintenance of IoT devices and their respective cybersecurity risk profiles. Implementation of a labeling scheme will depend on a scheme owner's management, program structure determination and oversight, informed by NIST's recommendations. While the details of any particular labeling scheme will vary, NIST's recommendations provide guidance to companies that offer consumer IoT products regarding baseline product and labeling requirements that may ultimately be imposed by a scheme owner.

Return to Table of Contents

Federal Trade Commission Settles COPPA Case

The Federal Trade Commission (FTC) reached a settlement with WW International Inc. (WW, formerly known as Weight Watchers) and Kurbo, Inc., a WW subsidiary that offers a weight management and tracking service designed for users between the ages of eight and 18 and their families, regarding alleged violations of the Children's Online Privacy Protection Act of 1998 (COPPA) and the FTC's Children's Online Privacy Protection Rule (COPPA Rule). The settlement offers guidance regarding the processes for obtaining parental consent as required by COPPA and the COPPA Rule.

Background

COPPA regulates the collection, use and retention of personal data of children under the age of 13 by website and online service providers. Operators of commercial websites that are directed toward children or that knowingly collect, use or disclose children's personal information must, among other requirements, obtain verifiable parental consent prior to collecting, using or disclosing such information, and securely dispose of the children's information when no longer useful for its intended purpose. The FTC may impose a civil penalty of up to $46,517 per violation.

Enforcement

Kurbo Inc., (Kurbo) offers a weight management and tracking service directed to users between the ages of eight and 18, as well as their families. It was acquired by WW in 2018 and provides its services through a mobile app and website, as well as various platforms designed for use in corporate employee benefit offerings. Among the personal data collected are children's names, gender, phone number, birthdate, height and weight, as well as logs of nutritional and activity habits and various persistent and unique identifiers. The FTC asserted that WW and Kurbo failed to meet a number of COPPA requirements.[10] In an attempt to comply with the parental consent requirement, Kurbo notified users that children under 13 seeking to use the service must request that a parent create an account on their behalf. However, the FTC stated that Kurbo should have employed a "neutral age screen" (*i.e.*, one that requires entry of a user's actual birthdate without indicating what an "acceptable" birthdate would be) to avoid encouraging children to falsify their age. This marks the first time that the FTC has enforced the neutral age screen requirement. Further, the FTC stated that

[10] The case is *United States of America v. Kurbo Inc. et al.*, No. 22-CV0946 (N.D. Cal. 2022).

Kurbo had not clearly and completely explained its information collection practices to parents, and objected to the privacy notice being included in a series of hyperlinks, where parents may not notice it. Finally, Kurbo allegedly maintained user data indefinitely, deleting information only in response to users' requests.

In a stipulated order submitted to the District Court for the Northern District of California in February 2022, WW and Kurbo agreed to pay $1.5 million to settle the FTC claims and to undertake certain corrective actions to bring their practices in line with COPPA and the COPPA Rule, including providing direct notice to parents of Kurbo's collection practices and obtaining consent to continue using their children's data, or, in the absence of such consent, delete the children's' data and any models or algorithms developed using the data. This remedy is notable in that it extends not only to the children's data, but to associated models and algorithms as well, which has the potential to have wider effects on these types of business models.

Key Takeaways

This action against WW and Kurbo highlights the FTC's willingness to strictly enforce each prong of COPPA and the COPPA Rule. Companies operating online platforms either directed toward children or through which they knowingly collect data from children under 13 should ensure, among other things, that their gating mechanism is age-neutral, and that they delete such information once it is no longer necessary for the purposes for which it was collected.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000