Skadden

Privacy & Cybersecurity Update

GoodRx and Evolving Digital Health Privacy Oversight in the US

In February 2023, the Federal Trade Commission (FTC) and digital health care platform GoodRx Holdings, Inc. (GoodRx) entered into a stipulated order to resolve allegations that GoodRx's use and disclosure of health information violated Section 5 of the FTC Act and the FTC's Health Breach Notification Rule (HBNR). The order, which marks the first time the FTC has enforced the HBNR, resolved the FTC's allegations that GoodRx shared its users' sensitive personal health information with advertising platforms such as Facebook and Google without user knowledge or consent.

The HBNR requires "vendors of personal health records" like GoodRx to notify consumers, the FTC and, under some circumstances, certain media outlets following an unauthorized disclosure of personal health information. As the GoodRx enforcement action demonstrates, "unauthorized disclosures" under the HBNR not only may involve data breaches that result from cyberattacks by third parties, but also may include a company's disclosure of sensitive data without proper consent.

Taken together with expanding oversight of health-related cybersecurity and privacy issues by states and the Food and Drug Administration (FDA), the GoodRx enforcement action underscores the heightened regulatory standards to which digital health companies will be held and reflects regulators' increasing commitment to keep their enforcement efforts on pace with an evolving digital health marketplace.

Background and Stipulated Order

GoodRx operates a digital health care platform that allows users to compare prescription drug prices, obtain prescription drug coupons and access telehealth services through an online website and mobile application. Through its platform, GoodRx collects a host of health-related information from users, including information about their prescription medications, the types of medical treatment sought for certain health conditions, contact information and persistent identifiers. According to the FTC, since at least 2017, GoodRx promised its users that it would never share personal health information with advertisers and that, when it did share personal health information with certain third parties, it would do so for limited purposes and restricted uses. The FTC further alleged that GoodRx assured its users that its business practices fully complied with industry principles regarding the secure maintenance of sensitive data.

On February 1, 2023, the FTC filed a complaint in the U.S. District Court for the Northern District of California against GoodRx, alleging that the company repeatedly violated these promises by disseminating users' personal health information to third-party advertising companies and platforms, such as Facebook and Google, without users' knowledge or consent. Specifically, the FTC alleged that GoodRx:

- shared users' health and other information with third-party companies, primarily with tracking pixels, and, in some instances, used that shared information to create targeted, health-related ad campaigns, contrary to the company's privacy policies;
- took no action to limit how third parties could use the personal health information it disclosed to them and entered into agreements that permitted the third parties to use such information for their own business purposes, including research and development and ad optimization, despite GoodRx's promise to users that it would use "contractual and technical protections" to limit third-party use of users' information;
- failed to maintain adequate controls to prevent the unauthorized disclosure of personal health information, such as written standards that governed how all types of health and personal information could be shared, privacy personnel with oversight of the company's privacy and data-sharing practices or a formal process for reviewing and approving data sharing requests or third-party tracking tool integrations;
- falsely claimed to adhere to the Digital Advertising Alliance's (DAA) principles, including the DAA's Self-Regulatory Program for Online Behavior Advertising, which provides that entities should not collect health information from individuals without consent; and
- misleadingly displayed a Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance seal on its platform despite not being a HIPAA-covered entity or business associate; according to GoodRx, the HIPAA seal was used by a telehealth entity it had recently acquired and was removed "a few months after the acquisition" as part of the company's integration efforts.[1]

The FTC alleged that these actions constituted deceptive and unfair practices in violation of Section 5 of the FTC Act and that GoodRx's failure to notify users, the FTC and media about its unauthorized disclosures of personal health information violated the HBNR. As to the HBNR, the FTC determined that GoodRx is a "vendor of personal health records" because its digital platform gathers and stores identifiable health information from various sources into a "personal health record" that is managed primarily for an individual's use. Accordingly, the FTC alleged that GoodRx's transfer of users' identifiable health information to third parties for advertising purposes constituted a "breach" under the HBNR because the company disclosed this information without users' authorization.[2]

The stipulated order, in which GoodRx denied the FTC's allegations and did not admit liability, requires GoodRx to pay $1.5 million in civil penalties. In addition, it imposes novel injunctive relief by permanently restraining and enjoining GoodRx — as well as its officers, agents, employees and attorneys with actual notice of the order — from sharing user health data with third parties for advertising purposes. Among other provisions, the stipulated order also requires GoodRx to retain an independent assessor to conduct biennial reviews of its privacy program and the privacy programs of any company it controls, and to submit annual certifications regarding its compliance with the terms of the order.

Expanding Regulatory Oversight

Although the GoodRx enforcement action is the first of its kind under the HBNR, the FTC previously signaled its intention to crack down on HBNR breaches in 2021, when it issued its Statement of the Commission on Breaches by Health Apps and Other Connected Devices[3] (the FTC Policy Statement). The FTC Policy Statement — which was issued after GoodRx's alleged misconduct concluded — admonished entities offering apps and internet-connected devices that "track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet, and other vital areas" to examine their ongoing obligations with respect to protecting users' health data and take steps to prevent the unauthorized disclosure of health information. The FTC Policy Statement also reminds digital health developers that a breach for purposes of the HBNR "is not limited to cybersecurity intrusions or nefarious behavior" and can also include "sharing of covered information without an individual's authorization."

The FDA and Congress also have taken steps to increase oversight and regulation of certain health-related apps and other connected devices. The regulatory concept of software as a medical device (SaMD) covers a range of products, from patient-centric applications on smart phones to clinical decision support software products directed to health care practitioners, and it has evolved considerably over time. The 21st Century Cures Act, enacted in December 2016, set forth important guideposts for the regulation of SaMD by, among other things,

[1] GoodRx Response to FTC Settlement.

[2] "FTC Enforcement Action To Bar GoodRx From Sharing Consumers' Sensitive Health Info for Advertising," Federal Trade Commission, (February 1, 2023).

[3] Federal Trade Commission, "Statement of the Commission On Breaches by Health Apps and other Connected Devices" (September 15, 2021),

excluding a number of categories of software from the definition of a "device" subject to the Federal Food, Drug, and Cosmetic Act (FDCA). The FDA has since issued several guidance documents on the regulation of SaMD, and, on December 29, 2022, President Joe Biden signed into law the Food and Drug Omnibus Reform Act of 2022 (FDORA) as part of the Consolidated Appropriations Act, 2023, Pub. L. No. 117-328 (2022). FDORA amended the FDCA to impose premarket submission requirements and such "other requirements" deemed necessary by the FDA to ensure the safety of "cyber devices," which are medical devices that "(1) include[] software validated, installed, or authorized by the sponsor as a device or in a device; (2) [have] the ability to connect to the internet; and (3) contain[] any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats." Failing to adhere to these new cybersecurity requirements constitutes a prohibited act under the FDCA and subjects the device manufacturer to a range of potential FDA enforcement actions, including criminal liability. State regulators are also pursuing legislative changes and taking enforcement action to address use and disclosure of personal health information.

Key Takeaways

The GoodRx enforcement action highlights the evolving regulatory landscape in which digital health companies must operate. In light of this action, companies that maintain or handle personal health information should review their data-sharing controls to ensure their business practices align with their own internal policies as well as with regulators' expectations. For example, digital health companies should:

- Recognize that HIPAA — which applies to certain personal health information held by a relatively limited universe of covered entities and business associates — is not the only potential source of regulatory scrutiny for personal health data held by companies. Accordingly, entities that are not subject to HIPAA but are nonetheless entrusted with personal health information are expected to have in place a robust privacy program, including personnel with the requisite expertise, to ensure that use of personal health information is limited to legitimate uses and that personal health information is protected from unauthorized disclosure. This is in addition to any privacy compliance obligations that companies may have under general data protection laws, such as the General Data Protection Regulation in the EU or U.K. or the California Consumer Privacy Act.
- Be transparent about the use and subsequent disclosure of personal health information and obtain express affirmative consent prior to using or sharing such information.
- Conduct a review of *current* data-sharing practices to ensure that such practices align with company policies or other promises made to customers about use of their health information.
- Implement cross-functional controls to identify, understand and monitor all data sharing requests and third-party tracking tools, including with respect to business development and other marketing initiatives, and require that all such activities require review by privacy personnel or outside counsel.
- Set contractual limitations on how third parties can use customers' personal health information and harmonize those provision across all contracts.
- When considering transactions, ensure appropriate pre- and post-closing diligence of digital health targets, including an assessment for FTC, HIPAA and FDCA compliance, in addition to compliance with general data privacy laws and regulations.

Return to Table of Contents

European Commission Announces Overhaul of Monitoring of Cross-Border Investigations Under the GDPR

Following an inquiry by the European ombudsman into whether the European Commission (EC) has collected sufficient information to properly monitor the implementation of the General Data Protection Regulation (GDPR) in Ireland, the EC has announced it will request that all national data protection authorities (DPAs) share reports of large-scale cross-border investigations that are under review.

In January 2023, the EC announced that it would be introducing a new procedure for monitoring GDPR investigations by DPAs. This new procedure will require DPAs to share with the EC, on a bimonthly and strictly confidential basis, an overview of large-scale cross-border investigations under their review. The EC's decision followed a complaint by a nonprofit organization, the Irish Council for Civil Liberties (ICCL), alleging the EC had not taken adequate steps to collect sufficient information to monitor the implementation of the GDPR in Ireland, and an inquiry by the European ombudsman, Emily O'Reilly, into the same.

While "cross-border" is not defined in the ICCL complaint or in the decisions from Ms. O'Reilly or the EC, the GDPR defines cross-border processing broadly as processing that (1) takes place in more than one member state of the European Union (EU) or (2) affects data subjects in more than one member state.

The ICCL Complaint

In September 2021, the ICCL wrote to the EC to complain about the enforcement of the GDPR in Ireland. In particular, the organization alerted the EC to a "data deficit," questioning whether the EC had collected sufficient information to properly monitor the enforcement of the GDPR by the Irish Data Protection Commission (DPC), which is the lead supervisory authority for many Big Tech companies in the EU (*e.g.*, Meta, Apple, Microsoft). The ICCL argued that to properly monitor the application of the GDPR in Ireland in cross-border cases, the EC would be required to have the following information: (1) how many cases are transferred to Ireland; (2) how long each case takes to process; and (3) what concrete measures are taken (if any) to (a) provide redress to individual citizens and (b) correct unlawful practices by Big Tech companies. The ICCL stated that this information could not be found in the DPC's annual reports or the EC's first report on the application of the GDPR.[4]

In response, the EC stated that it had taken adequate steps to monitor the application of the GDPR by the DPC and had not found any evidence to date to support the ICCL's concern on the application of the GDPR in Ireland. Dissatisfied with the response from the EC, the ICCL lodged a complaint with Ms. O'Reilly in January 2022.

Inquiry by the European Ombudsman

Overview of the Inquiry

In February 2022, Ms. O'Reilly opened an inquiry into whether the EC had taken adequate steps to collect sufficient information that would allow it to properly monitor the implementation of the GDPR in Ireland. Ms. O'Reilly noted that the inquiry was necessary as public bodies and civil society organizations had raised concerns that the application of the GDPR in Ireland was inadequate. She asked the EC to provide (1) a detailed and comprehensive account of the information the EC had collected on the implementation of the GDPR in Ireland and (2) an explanation of how and from what sources the EC had gathered such information.

Ms. O'Reilly clarified that the inquiry was focused on "information gathering" and did not concern whether the EC was doing enough generally to ensure that the GDPR was applied. She noted that the EC enjoys "wide discretion" in deciding whether and when to commence an infringement procedure. An infringement procedure is set out in Article 258 of the Treaty on the Functioning of the EU, and allows the EC to take formal action against a member state if the EC considers that that member state has failed to fulfill its obligations under EU law. Ms. O'Reilly emphasized the fact that (1) the infringement procedure is directed at member states and not DPAs, and that (2) DPAs act independently when implementing the GDPR and the EC has no mandate to direct DPAs on implementation, though DPAs are required to cooperate with the EC to ensure consistent application.

Ms. O'Reilly held two meetings with representatives from the EC and received two formal replies from the EC. She then gave the ICCL the opportunity to comment on the meeting reports and the EC's formal replies, before she published her decision.

Findings From the Inquiry

The EC cited the European Data Protection Board (EDPB) as the primary source of its information on the implementation of the GDPR and noted that the EC had gathered information directly from DPAs, including the DPC, when preparing its first report on the application of the GDPR.

Additionally, the EC informed Ms. O'Reilly that the DPC sends the EC an overview of Big Tech cases it is investigating on a bimonthly basis.

Conclusions of the European Ombudsman

Ms. O'Reilly published her decision in December 2022, noting that the bimonthly reports sent by the DPC to the EC were an "encouraging example of a specific targeted monitoring measure." However, she noted that there was room for improvement, recommending that the EC:

- draw up a table with predetermined fields that should be completed by the DPC for each cross-border case; and
- provide an account of the EC's practice of receiving the information stated above from the DPC (including an outline of the specific kinds of information received) in its next report on the application of the GDPR, which is due to be published in 2024.

The EC's Decision

The EC accepted and expanded on Ms. O'Reilly's recommendations to require reports on large-scale cross-border investigations from all DPAs (not just the DPC), on a bimonthly and strictly confidential basis.

Each case report must include the following information: (1) case number, (2) controller or processor involved, (3) investigation type (*ex officio* or complaint-based), (4) summary of investigation scope (including which provisions of the GDPR are at issue), (5) DPAs concerned, (6) key procedural steps taken and their dates and (7) investigatory or any other measures taken and their dates.

[4] The report on the application of the GDPR can be found here.

Additionally, the EC agreed to publish an account of its practice of receiving the above information from the DPAs in its next report on the application of the GDPR and to include an indication of the specific information received.

The threshold for "large-scale cross-border" investigations has not been defined Ms. O'Reilly's decision or the EC's decision, though it is likely to capture a number of ongoing investigations of Big Tech companies in the EU. The EC is expected to implement this new reporting procedure later this year, though no official date has been announced.

Approach in the UK

Although the U.K.'s Information Commissioner Office (ICO) will not be subject to the requirement to provide such reports to the EC, the ICO recently made the decision to publish numerous data sets relating to self-reported personal data breaches, data protection complaints from members of the public and investigations by the ICO for breaches of U.K. data protection laws.[5] This change of policy appears to be inspired by the ICO's "new" approach to enforcement actions, which places a greater emphasis on transparency.

Key Takeaways

ICCL Senior Fellow Johnny Ryan lauded the EC's decision to require DPAs to share reports on cross-border investigations, noting that "we should see an acceleration in investigation and enforcement" by DPAs. While the actual effects of the decision have yet to be seen, the decision by the EC marks a shift towards a more interventionist approach to monitoring the implementation of the GDPR, and complements a recent statement by the EC announcing that the EC and EDPB would be presenting a proposal later this year to harmonize cooperation in cross-border cases amongst DPAs.

Return to Table of Contents

[5] Read our January 2023 *Privacy & Cybersecurity Update* article on the ICO's decision to publish the names of organizations subject to data breaches, complaints and investigations

Network and Information Security 2 Directive Strengthens the European Union's Cybersecurity Regime

Entering into force on January 16, 2023, the Network and Information Security 2 Directive (NIS2) has replaced the original NIS Directive, which was introduced[6] in 2016 as the EU's first cybersecurity regime. The NIS2 builds upon the first regime by requiring a broader range of infrastructure sectors and service providers, known as essential entities and important entities, to implement appropriate technical, operational and organizational measures to manage cyber threats.

The NIS2 aims to harmonize and strengthen the EU's cybersecurity regime, particularly by enlarging the scope of the original NIS Directive, introducing a new notification and reporting mechanism for cybersecurity incidents, imposing direct and personal liability on boards of directors for non-compliance and introducing a robust framework of fines.

Background

On November 28, 2022, the Council of the EU formally adopted the NIS2, and on December 27, 2022, the NIS2 was published in the Official Journal of the European Union with enforcement to come 20 days later.

As the NIS2 is a directive and not a regulation, it is not automatically enforceable in all EU member states. Instead, each EU member state must implement the directive into its own national legislation, and they are obligated to do so by October 17, 2024.

The NIS2, like the GDPR, has extraterritorial reach. This means that the NIS2 will apply to all organizations that are: (1) established in the EU or (2) not established in the EU but provide services in the EU. An organization is defined as established in the EU if: (1) decisions related to the organization's cybersecurity risk management measures are predominantly taken in the EU, (2) decisions related to the organization's cybersecurity operations are taken in the EU or (3) the organization's main establishment (*i.e.*, the establishment with the highest number of employees) is in the EU.

Further, digital infrastructure and digital service providers, as well as managed service providers that come under the extraterritorial scope of the NIS2, are required to appoint a representative for the purposes of NIS2 compliance in the jurisdiction where they

[6] Read our 2019 Skadden *Insights* article "European Data Protection and Cybersecurity in 2019."

are established. This representative should act on behalf of the organization and should be empowered to report cybersecurity incidents to competent authorities and the Computer Security Incident Response Team (CSIRT) (further described below).

Rules and Requirements

The NIS2 notes that small and medium-sized enterprises are increasingly becoming the targets of supply chain cybersecurity attacks (*i.e.*, attacks that distribute malware through an organization's IT infrastructure via an outside partner or third-party supplier) due to their often limited cybersecurity resources.

To address these concerns, the NIS2:

- enlarges the scope of the original NIS Directive to capture more service providers;
- introduces a new two-step notification and reporting mechanism for cybersecurity incidents;
- introduces direct and personal liability on boards of directors that do not comply with the NIS2;
- requires regulated entities to incorporate cybersecurity measures into their contractual arrangements with their suppliers; and
- provides for considerable administrative fines for noncompliance.

Enlarging the Scope of the Original NIS Directive

The original NIS Directive applied to two categories of service providers: (1) operators of essential services (OES) (i.e., transportation, energy, banking, health, water and digital infrastructure service providers) and (2) digital service providers (DSP) (*i.e.*, cloud service providers, online stores and search engines).

Under the NIS2, the categorization of an organization as either an OES or DSP has been replaced by two new categories that are much broader than those under the original NIS Directive. The new categories are:

- *Essential entities* (EEs), which include all organizations that are essential for economic and societal activities, *i.e.*, energy, transportation, financial, health, drinking water, wastewater, public administration/electronic communications and digital infrastructure *(e.g.*, data centers, mobile telecommunications infrastructure and broadband infrastructure) as well as business-to-business (B2B) information and communication technology (ICT) management service providers, and ground-based infrastructure for the provision of space-based services (*e.g.*, satellite infrastructure); and
- *Important entities* (IEs), which includes all the service providers that were previously listed as DSPs, as well as providers of: postal and courier services, waste management services, manufacturing services, food distribution services, research services and health care products.

In order to be classified as an EE, the service provider must be an organization that: (1) is essential for economic and societal activities (as described above), (2) has fewer than 250 employees and (3) does not meet the annual turnover/balance sheet threshold of €50 million (*i.e.*, a medium-sized business). All organizations with (1) an annual turnover/balance sheet of less than €10 million and (2) fewer than 50 employees are exempt from the NIS2 (*i.e.*, micro/small businesses).

IEs act as a catch-all designation, capturing all service providers that are not micro/small businesses or EEs.

All EEs and IEs are obliged to implement technical, operational and organizational measures to manage cybersecurity risks to their networks and systems; obtaining industry-recognized cybersecurity certifications (*e.g.*, ISO 27001, ISO 22301) may help an organization to demonstrate the implementation of such measures. Under the NIS2, the minimum cybersecurity management measures that an EE or IE are obliged to implement are:

- risk analysis and information system security policies;
- cybersecurity incident handling procedures;
- business continuity and disaster recovery plans, backup and crisis management;
- supply chain security measures, including measures that concern the relationship between an EE or IE and its direct suppliers;
- security in-network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- policies and procedures to assess the effectiveness of cybersecurity risk management measures;
- cyber hygiene practices and cybersecurity training;
- policies and procedures on the use of cryptography and encryption (where appropriate);
- human resources security, access control policies and asset management; and
- multifactor authentication or continuous authentication solutions; secured voice, video and text communications; and secured emergency communication systems (where appropriate).

Two-Step Notification and Reporting Mechanism for Cybersecurity Incidents

Under the original NIS Directive, OES and DSPs were required to notify a competent authority (such as the National Authority for Cyber-defence and Network and Information Security), or the EU member states' CSIRT, "without undue delay" upon becoming aware of a cybersecurity incident. Such cybersecurity incidents were required to have a significant or substantial impact on the continuity of the OES or DSP's services before they were reportable. CSIRTs are designated and/or established by EU member states and can sit within the EU member states' competent authority.

Under the original NIS Directive, to determine if the impact of a cybersecurity incident was significant or substantial, organizations had to assess:

- the number of users affected;
- the duration of the incident;
- the geographical spread of the incident;
- the extent of the disruption to the underlying services; and
- the impact the cybersecurity incident had on economic and societal activities.

Under the NIS2, the notification requirement is divided into two phases as follows:

Two-step notification mechanism. The organization must submit a notification to its CSIRT or competent authority: (1) within 24 hours of becoming aware of a significant cybersecurity incident (as defined above) and (2) 48 hours after the 24-hour notification (*i.e.*, 72 hours after a significant cybersecurity incident).

- The 24-hour notification should indicate whether the significant cybersecurity incident is:
  - suspected of being caused by unlawful or malicious acts; and
  - likely to have a cross-border impact.
- The 72-hour notification should include:
  - an initial assessment of the severity and impact of the significant cybersecurity incident; and
  - any indicators of system compromise.

Report submission. A report must be submitted by the organization no later than one month after the abovementioned 24-hour notification to the CSIRT or competent authority. This final report should include:

- a detailed description of the severity and impact of the cybersecurity incident;
- the type of threat or root cause of the cybersecurity incident;
- relevant mitigation measures taken or being taken; and
- any additional information that has been discovered regarding the cross-border impact of the incident since the original 24-hour notification.

Implementing Cybersecurity Measures in Contracts With Suppliers

Another change under the NIS2 is the establishment of the Cooperation Group. The Cooperation Group is made up of representatives of all EU member states, the EC and the EU Agency for Cybersecurity (ENISA) and is tasked with the following: (1) providing guidance and advice, (2) producing cybersecurity policy initiatives, (3) providing training and awareness of cybersecurity issues, (4) exchanging information on best practices in relation to cybersecurity, (5) defining standards and technical specifications, and (6) maintaining a central register of EEs and IEs in each EU member state.

Due to the global increase in major supply chain cybersecurity attacks, the Cooperation Group is also empowered to carry out coordinated, EU-wide supply chain risk assessments. These persuasive assessments will identify: (1) the main threats and threats actors, (2) the assets most sensitive to cyber threats, (3) the main cybersecurity vulnerabilities (including technical and other types of vulnerabilities), and (4) any strategic risks that are likely to impact critical ICT services, systems and product supply chains.

Under the NIS2, both EEs and IEs are required to consider these persuasive assessments to determine the most appropriate cybersecurity measures to implement with their suppliers.

As such, prior to onboarding and throughout their relationship, organizations classified as EEs or IEs need to perform robust, documented due diligence on their suppliers' cybersecurity vulnerabilities and cybersecurity practices, while ensuring that their suppliers maintain the minimum cybersecurity measures required by the NIS2 (as discussed above).

The obligations on boards of directors of EEs and IEs, and the new fines regime (discussed below) under the NIS2, indicate that the cybersecurity measures implemented by the suppliers of EEs and IEs will be a key issue. In particular, EEs and IEs should perform due diligence on prospective suppliers and review their relationships with their existing suppliers.

Enforcement and Penalties

A key change under the NIS2 is that the boards of directors of an EE or IE (referred to as "management bodies" in the NIS2) can

be held directly and personally liable for noncompliance by the EE or IE. If the board of directors does not take the necessary actions to ensure the EE or IE complies with the NIS2, then the competent authority can request that the relevant bodies, courts or tribunals in the competent authority's EU member state temporarily prohibit the EE's or IE's managers from exercising managerial functions. As such, the NIS2 requires the boards of directors of both EEs and IEs to actively manage and engage with their organization's cybersecurity compliance program.

If an EE or IE fails to implement the minimum cybersecurity management measures (as described above), the competent authority also has the power to:

- issue warnings to an EE or IE detailing its infringements of the NIS2;
- order the EE or IE to adopt the minimum cybersecurity management measures;
- conduct a cybersecurity audit of the EE or IE and order the EE or IE to implement its recommendations within a reasonable deadline; and/or
- temporarily suspend, or request the relevant courts, bodies or tribunals in the competent authority's EU member state to temporarily suspend, the services carried out by the EE or IE.

The NIS2 also introduces the following fines for noncompliance:

- IEs: the greater of €7 million or 1.4% of global annual turnover.
- EEs: the greater of €10 million or 2% of global annual turnover.

However, in instances where a failure to comply with the NIS2 also results in a personal data breach under the GDPR, and a data protection authority decides to impose an administrative fine against that organization for violating the GDPR, the NIS2 authority cannot impose an administrative fine for the same incident as this would constitute double punishment for the same infringement.

Under the NIS2, EU member states must empower their competent authorities to take enforcement actions against non-compliant organizations. These enforcement actions include:

- issuing warnings about an EE's or IE's noncompliance with the NIS2's obligations;
- issuing binding instructions or an order requiring an EE or IE to remedy any deficiencies in their cybersecurity measures that are identified by the competent authority;
- ordering an EE or IE to bring their risk management measures and/or reporting obligations into compliance with the NIS2 within a specified period;
- ordering an EE or IE to make public statements about aspects of their noncompliance with the NIS2;
- ordering an EE or IE to make a public statement that identifies the person or organization responsible for any infringements of the NIS2; and/or
- imposing or requesting the imposition of an administrative fine on an EE or IE by the relevant courts, bodies or tribunals in the competent authority's EU member state.

Parallel Effort in the UK

As the NIS2 is an EU directive, it will not be implemented in the U.K. However, the U.K. government has separately announced its proposal to update the Network and Information Security Regulations 2018 (which implemented the original NIS Directive in the U.K.) (U.K. NISR).[7] The proposal, which remains open for response until April 10, 2023, indicates that, despite the U.K.'s exit from the EU, the U.K. government will continue to closely align its cybersecurity regime with that of the EU.

The U.K. government's proposal indicates that some updates that are similar to the NIS2 will be implemented, including:

- the expansion of the scope of the U.K. NISR's definition of a DSP to include managed service providers, which are B2B providers of services such as managed network services;
- amending the incident reporting requirements under the U.K. NISR to include incidents that pose a significant risk to the security and resilience of service providers and the essential services they provide; and
- providing for a two-step supervisory regime for DSPs, which will require proactive notification of cybersecurity incidents for critical digital services.

Key Takeaways

- The NIS2 and the U.K. NISR present an opportunity for organizations to review and strengthen their cybersecurity readiness. Organizations falling under the remit of the NIS2 or the U.K. NISR should ensure that they have implemented appropriate technical, operational and organizational measures and have performed robust due diligence on their suppliers to ensure they also have implemented such measures.
- Due to their extraterritorial reach, the NIS2 and the proposed updates to the U.K. NISR will increase the cyber resilience of EEs and IEs throughout the world, not only in the EU and U.K.
- Organizations that implement adequate risk analysis, information system security policies, incident handling protocols,

[7] The U.K. government's proposal to expand the scope of the U.K. NISR can be found here.

business continuity and disaster recovery plans, cybersecurity penetration testing, adequate training and encryption, and that monitor the cybersecurity measures implemented by their suppliers through comprehensive due diligence and regular audits, will be in a good position to demonstrate their compliance with the NIS2 and the U.K. NISR. Such measures also will ensure that organizations can reduce their risk of a cybersecurity attack.

Return to Table of Contents

Illinois Supreme Court Holds That BIPA Claims Accrue Each Time Biometric Data Is Scanned or Transmitted

The Illinois Supreme Court ruled on February 17, 2023, that claims accrue under Sections 15(b) and 15(d) of the Illinois Biometric Information Privacy Act (BIPA) every time — not just the first time — biometric data is scanned or transmitted without prior consent.

In *Cothron v. White Castle System, Inc.*, the Illinois Supreme Court determined that a separate claim accrues under Sections 15(b) and 15(d) of BIPA "each time a private entity scans or transmits an individual's biometric identifier or information in violation of section 15(b) or 15(d)."[8] Per the ruling, plaintiffs can bring a claim under Sections 15(b) and 15(d) every time, rather than just the first time, their biometric data is collected or disclosed in violation of such sections.

The court also clarified that the Illinois General Assembly "chose to make damages discretionary rather than mandatory under" BIPA. Relatedly, the court noted that the equitable nature of the class action mechanism permits judges to fashion awards that compensate plaintiffs and deter future violations without significantly impacting the defendant's business.

Background

BIPA Section 15(b) states that private entities may not "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data without that person's prior consent and also may not "disclose, redisclose, or disseminate" that data under BIPA Section 15(d).

Plaintiff Latrina Cothron, a longtime employee of the fast food chain, alleged that her employer violated BIPA Sections 15(a),[9] 15(b) and 15(d) by requiring her to scan her finger to access the company's computer system. Her fingerprint scans were then allegedly transmitted to third-party vendors.

On a motion to dismiss, the Northern District of Illinois rejected the plaintiff's Section 15(a) claim for lack of standing. However, her 15(b) and (d) claims were permitted to proceed.

The company later filed a motion for judgment on the pleadings and argued that the plaintiff's claims were untimely. According to the company, the plaintiff's only BIPA claims would have accrued, if at all, in 2008, right after the passage of BIPA. The district court denied the restaurant's motion and held that BIPA claims accrue with *each* scan or transmission of biometric data, meaning the "first" scan is not the beginning and end of a private entity's BIPA liability. The company then appealed to the Seventh Circuit.

The Seventh Circuit, however, found itself "genuinely uncertain" of the correct interpretation under BIPA and certified the following question to the Supreme Court of Illinois: Do Sections 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?[10]

Ruling

The Illinois Supreme Court agreed with the district court, ruling that a violation accrues each time biometric information is scanned or transmitted without consent. The court, at the outset, pointed to the language of the statute, stating "[w]here the language is clear and unambiguous, we must apply the statute without resort to further aids of statutory construction."[11]

The court concluded that Section 15(b), which prohibits a private entity's collection of biometric identifiers "unless it first" receives consent, covers both the first and each subsequent collection or transmission of data. The court determined that the phrase "unless it first" refers not to the first collection of information, but to an entity's continuing obligation to obtain consent.[12]

[8] Please see the decision in *Cothron v. White Castle System, Inc.*, 2023 IL 128004, ¶ 1 (Ill. 2023).

[9] 740 ILCS 14/15(a) ("A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first….").

[10] *Cothron v. White Castle System, Inc.*, 20 F.4th 1156, 1166-67 (7th Cir. 2021)

[11] *Cothron v. White Castle System, Inc.*, 2023 IL 128004, ¶ 20 (Ill. 2023).

[12] *Id.* at ¶¶ 23-25.

The court next concluded that Section 15(d), which prohibits the disclosure, redisclosure and dissemination of biometric data without informed consent, covers repeated transmissions of the same data to the same third party, not only transmissions of new data. The court further held that it need not decide whether the word "redisclose" refers to transmission of the same data to the same party or, instead, transmission to downstream parties (other words in the statute (*i.e.*, "disseminate") contemplate repeated transmissions of the same data to the same party).[13]

The court next addressed the company's "nontextual arguments," rejecting the claim that injury under BIPA is the loss of control over privacy of biometric data. Rather, the court read its precedent, *Rosenbach*,[14] to hold that the violation of the statute constitutes an injury. The court acknowledged the company's concerns about the potential liability that businesses would face as a result of the holding, but reiterated that where statutory language is clear, it must be given effect, even though the consequences may be harsh, unjust, absurd or unwise. The court also clarified that damages under BIPA are discretionary and not mandatory.

Finally, the court "respectfully suggest[ed]" that the Illinois state legislature address the policy concerns raised and clarify how damages should be assessed under BIPA.

Key Takeaways

While the practical effects of this decision have yet to be seen, the *Cothron* decision made clear that claims Sections 15(b) and 15(d) of BIPA accrue at every collection or dissemination of biometric information. The court also clarified that the Illinois General Assembly chose to make "damages discretionary rather than mandatory under BIPA" — however, the ruling did not provide clear guidance to lower courts as to how to exercise this discretion. The court emphasized its belief that policy concerns regarding damages are better assessed by the legislature and not the court system, and invited the Illinois state legislature to revisit BIPA and clarify how damages should be calculated under the statute.

Return to Table of Contents

[13] *Id.* at *5-6

[14] *Rosenbach v. Six Flags Entertainment Corp.*, 129 N.E.3d 1197 (Ill. 2019).

District Court Holds That CGL InsurerHas Duty To Defend BIPA Suit

The U.S. District Court for the Northern District of Illinois recently held that Mitsui Sumitomo Insurance USA, Inc. (Mitsui) has a duty to defend its insured Thermoflex Waukegan, LLC (Thermoflex), in a lawsuit alleging violations of Illinois' BIPA, but only after Thermoflex exhausts the limits of an underlying primary insurance policy issued by another carrier, Citizens Insurance Company of America (Citizens).[15]

The Underlying BIPA Lawsuit

In July 2020, employees of TempsNow, a temporary employment and staffing agency, filed a putative class action in Illinois state court against Thermoflex and TempsNow, alleging that the companies violated BIPA. The plaintiffs alleged that: (1) data from their handprints, which were used to clock in and out of work, was disclosed or disseminated to third parties without the plaintiffs' consent; a retention schedule and guidelines for permanently destroying the plaintiffs' handprint data was not provided; and a written release was not obtained from the plaintiffs to collect, store or use their handprint data.

The Insurance Coverage Dispute

Thermoflex sought coverage for the BIPA lawsuit from Mitsui, which issued a series of primary and umbrella/excess general liability insurance policies to Thermoflex during the relevant period, but Mitsui denied coverage. As a result, Thermoflex filed a suit against Mitsui in the U.S. District Court for the Northern District of Illinois seeking coverage for the BIPA lawsuit. Separately, Thermoflex filed a suit in the same court against Citizens, another Thermoflex primary insurer that denied coverage, and the court found that Citizens had a duty to defend the BIPA lawsuit.

In Thermoflex's suit against Mitsui, the parties subsequently cross-moved for summary judgment as to whether Mitsui had a duty to defend and indemnify under its policies. In granting Mitsui's motion and denying Thermoflex's motion, the court concluded that, while the BIPA lawsuit triggered the Mitsui primary policies' "Personal and Advertising Injury" coverage, the policies' "Access or Disclosure of Confidential or Personal Information" exclusion barred coverage. The court did not address whether the umbrella/excess policies provided coverage but set a briefing schedule on the issue.

[15] The order is *Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc.*, No. 21-cv-00788 (N.D. Ill. Jan. 19, 2023) (ECF No. 70).

In the subsequent briefing, Mitsui argued that, although the BIPA lawsuit fell within its umbrella/excess policies' "Personal and Advertising Injury" coverage, three exclusions — the "Data Breach," "Statutory Violation" and "Employment-Related Practices" exclusions — barred coverage for the BIPA lawsuit and that, alternatively, Mitsui had no duty to defend because the Citizens primary policy was not exhausted. In its decision on the umbrella/excess policies, the court first addressed the exclusions, noting at the outset that, under Illinois law, unambiguous policy language must be afforded its "plain and ordinary meaning." However, if exclusionary language is "reasonably susceptible to more than one meaning, [it is] considered ambiguous and will be construed strictly against the insurer who drafted the policy." After analyzing precedent from the Illinois Supreme Court and other courts in the Northern District of Illinois, and applying these canons of construction to the umbrella/excess policies' exclusions, the court concluded that each exclusion was ambiguous. As a result, the court construed the exclusions in favor of coverage and found that Mitsui had a duty to defend the BIPA lawsuit under the umbrella/excess policies.

The court then addressed Mitsui's alternate argument: that it had no present duty to defend under the umbrella/excess policies because Thermoflex's other primary insurer, Citizens, presently owed a duty to defend the BIPA lawsuit under its primary policy. Citing Illinois law requiring an insured to exhaust all available primary limits before invoking excess coverage, the court held that while Mitsui owes a duty to defend Thermoflex in the BIPA lawsuit under the umbrella/excess policies, that duty does not arise until Thermoflex exhausts the Citizens primary policy.

Key Takeaways

As the *Thermoflex* decision illustrates, coverage for claims under BIPA and other privacy laws under general liability (and sometimes other) policies often is not clear cut. Indeed, while the outcome in any particular scenario will turn on the facts and policy language, and sometimes on applicable law, courts have reached different conclusions even when construing the same or similar policy language and in comparable circumstances. This decision, coupled with the continued enactment of more robust privacy laws, including in the biometrics space, also underscores the importance of ensuring that insurance policy language is clear and unambiguous with respect to the intended scope of coverage for these matters.

Return to Table of Contents

Final CPRA Regulations Anticipated To Take Effect in April 2023

February comes with some much-anticipated greater certainty with respect to the regulations implementing the California Privacy Rights Act (CPRA). On February 3, 2022, the California Privacy Protection Agency (CPPA) Board voted to adopt the proposed regulations, as modified, of the California Privacy Rights Act (CPRA). On February 14, 2022, the CPPA submitted the rulemaking package to the Office of Administrative Law (OAL) for final review. The OAL has 30 business days to approve or disapprove the regulations from the date of submission. If approved, the draft regulations will become final and would take effect late March/early April 2023 at the earliest.

Status of the Regulations

The CPPA board held a public meeting on February 3, 2023, to discuss the status of its rulemaking process for the CPRA. The CPPA board indicated during the meeting that the earliest that the regulations could take effect would be in late March or early April. On February 14, 2023, the CPPA submitted the rulemaking package to the OAL for final review, which started the 30-business day review period and set a timeline that many are hopeful will, in fact, result in final regulations that will be enforceable in late March or early April 2023.

Civil and administrative enforcement of the CPRA was originally set to commence on July 1, 2023. However, the CPPA board had previously discussed the need to act as a "reasonable enforcer" and provide leniency to businesses that have made good-faith efforts to comply with the regulations given the uncertainty regarding when the regulations will be finalized and the limited time remaining for businesses to adjust their compliance posture. Furthermore, the most recent proposed CPRA regulations indicate that enforcement may be further delayed on a case-by-case basis. Specifically, the proposed regulations stated that the CPPA "may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements."

On February 21, 2023, the CPPA announced that the agency will hold a board meeting on March 3, 2023. Among the agenda items are various "updates" from members of the CPPA board. Due to the timing of this announcement, it is highly likely that this meeting will contain updates regarding the status of the CPRA regulations.

Several Regulations Remain Outstanding

As described in greater detail in our November 2022 and January 2023 *Privacy & Cybersecurity Updates*, several outstanding topics required to be addressed through regulations pursuant to the CPRA — cybersecurity audits, risk assessments and automated decision-making — have yet to be addressed by the current regulations. On February 10, 2023, the CPPA issued an Invitation for Preliminary Comments on Proposed Rulemaking on each of these three topics. The public may provide preliminary written comments regarding these topics to the CPPA through March 27, 2023. Rulemaking is still in its infancy for each of these three topics, and any regulations concerning these topics will not take effect or be enforced by the CPPA until adopted by the CPPA board in compliance with the Administrative Procedures Act and approved by the OAL.

Key Takeaways

Companies and other stakeholders are hopeful that the recently submitted final rulemaking package will be approved by the OAL, such that the CPRA regulations can take effect and create greater regulatory certainty by as soon as the end of March 2023. Enforcement of the CPRA regulations is set to commence on July 1, 2023. Any companies that may have been putting off updating their privacy policies, notices, practices and contractual provisions to comply with the CCPA, as amended by the CPRA, should consider focusing on these tasks now.

Return to Table of Contents

California Attorney General Conducts CCPA Investigative Sweep

In observance of Data Privacy Day, the California attorney general (AG) once again sent letters to various businesses alleged to have violated the CCPA — this time, focusing on companies with mobile applications in the retail, travel and food services industries.

On January 27, 2023, California AG Rob Bonta announced an investigative sweep, sending letters to businesses with mobile applications that allegedly fail to comply with the CCPA.[16] Given the timing of the announcement and the specific reference to "Data Privacy Day"— which is observed annually on January 28 — announcements regarding the enforcement of privacy laws and regulations may become a tradition in observance of that day. This follows the AG's similar announcement last year on Data Privacy Day regarding an investigative sweep of a number of businesses operating loyalty programs in violation of CCPA.[17]

This year, the AG sent letters to businesses with mobile applications, specifically in the retail, travel, and food services industries. The recipients of these letters allegedly violated the CCPA by failing to comply with consumer opt-out requests or by not offering any mechanism for consumers who want to stop the sale of their data. According to the AG's announcement, the sweep also focuses on businesses that failed to process consumer requests submitted via an authorized agent — which is required by the CCPA upon verification of certain information.

Key Takeaways

Companies should expect annual announcements regarding CCPA enforcement. Although the CPPA will take over enforcement of the CCPA starting July 1, 2023, it seems likely that the annual "tradition" in observance of Data Privacy Day will continue, in order to galvanize companies to remain vigilant and conscientious regarding their privacy compliance programs year-round.

[16] See "Ahead of Data Privacy Day, Attorney General Bonta Focuses on Mobile Applications' Compliance with the California Consumer Privacy Act," January, 27, 2023.

[17] See "On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act," January 28, 2023.

Privacy & Cybersecurity Update

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

Avia M. Dunn
Partner / Washington, D.C.
202.371.7174
avia.dunn@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

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@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

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@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

Nicole L. Grimm
Counsel / Washington, D.C.
202.371.7834
nicole.grimm@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