Skadden

Privacy & Cybersecurity Update

California Attorney General Releases Proposed Modifications to Draft Regulations Accompanying the California Consumer Privacy Act

On February 7, 2020, the California Office of the Attorney General issued a second draft of the regulations to accompany the California Consumer Privacy Act (CCPA).[1] The updated draft closed for public comment on February 25, 2020. Key changes were made to the following topics: notice requirements, service providers' obligations, opt-out of sale of personal information, and access and deletion rights.

The California Office of the Attorney General had released the initial draft regulations in October 2019, which provided much-needed guidance to companies on how to comply with the CCPA. The updated draft regulations clarify certain points in the initial draft and in some cases take an approach different than that reflected in the initial draft regulations. Certain key clarifications and changes are summarized below.

Notice Requirements

"At-Collection" Notice

The modified draft clarifies the "at-collection" notice requirements as they relate to mobile devices. If a company is collecting personal information via a mobile device for a purpose that the consumer would not reasonably expect, it must provide a "just-in-time" notice summarizing the categories of personal information being collected and a link to the full notice at collection. The updated draft provides an example in the context of a flashlight app. If a flashlight app is collecting geolocation information — which a consumer would not reasonably expect in connection with use of such an app — a just-in-time notification is required. In addition, the revisions suggest that businesses may be required to post at-collection notices on all webpages where personal information is collected. However, whether this is a requirement or a suggestion remains unclear.

The modified draft also eases the at-collection notice requirement by adding a materiality qualifier. Whereas the previous formulation of the regulations forbid businesses from using a consumer's personal information for any purpose other than those disclosed in the notice at collection, the revised draft only prohibits uses that are *materially different*

[1] The modified CCPA draft regulations can be found here.

from those disclosed in the at-collection notice. This may permit companies to streamline their disclosures, as opposed to including a laundry list of potential uses; however, it also requires companies to exercise judgment in determining which uses are materially different from those disclosed.

Opt-Out Notice

The modified draft also eases the burden for opt-out notices on companies that qualify as data brokers and register with the California Office of the Attorney General. Under the first draft of the regulations, a data broker was required to either contact the consumer to provide the opt-out notice before reselling the information or obtain an attestation from the data source with a copy of the collection notice that was displayed to the consumer. The modified draft merely requires a data broker to include a link in its privacy policy allowing consumers to opt out.

Service Providers' Obligations

One of the most significant revisions concerns service providers' use of personal information. The revision allows a service provider to process the personal information it receives from a service recipient for internal purposes to improve the quality of services. However, service providers may not use this information (1) to build consumer profiles; (2) to "clean" personal data; or (3) in combination with data obtained from another source. Under the CCPA, consumers have the right to "request to know" the categories and specific pieces of personal information collected by the company about the consumer, whether the company has sold or disclosed that personal information to third parties and, if so, the categories of third parties to which such information has been sold or disclosed, in each case during the 12 months preceding the request. The revised draft also clarifies that if a service provider receives a request to know or delete the personal information processed by it on behalf of the service recipient, it may respond directly rather than refer the consumer to the service recipient.

Opt-Out of the Sale of Personal Information

The modified draft eliminates a company's obligation to pass along opt-out requests to all parties to which the company had sold a consumer's personal information in the 90 days before the receiving the request. Instead, the revised draft contains a new requirement that companies comply with a consumer's opt-out request within 15 business days. If the company sells personal information to a third party after the consumer submitted their request but before the business complied with it (*i.e.*, within those 15 business days), the company must notify those third parties of the consumer's opt-out request and direct those third parties not to sell the personal information. The updated draft regulations stress that it should be easy for consumers to opt-out of the sale of their personal information and require minimal steps to do so.

In addition, the modified draft eliminates the total ban on the sale of information collected by a company that does not have a "do not sell" notice posted. Instead, the modified draft allows a company to sell such information if it obtains opt-in consent.

Access and Deletion Rights

Under the prior draft of the regulations, companies were required to implement a two-step process for responding to consumer requests to delete personal information, under which the consumer would first submit a request to delete and then separately confirm that the consumer wanted the information deleted. Under the modified draft, companies may, but are no longer required to, provide such two-step request submission process. The modified draft incorporates the amendment that was passed in October 2019 that a toll-free telephone number is not required for businesses operating exclusively online. Such businesses only need to provide an email address for receiving requests. Finally, the draft clarifies that businesses must confirm receipt of requests to know and delete within 10 business days.

Other Modifications

- Whether information is considered "personal information" depends on whether the company "maintains the information in a manner that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." For example, if an IP address collected by a company cannot be reasonably linked to a particular consumer or household, it is not considered personal information.
- A company must develop documented procedures to collect consent for the sale of minors' personal information only in cases where the company sells that personal information.
- If a non-account-holding consumer submits a request to know or delete household information, the company must verify (1) that all consumers of the household are jointly requesting access or deletion; (2) the identity of each consumer of the household; and (3) that each member making the request is a current member of the household. If there is a child under the age of 13 in the household, the company must obtain verifiable parental consent before complying with a request.
  - Such verification must be achieved in compliance with both the general rules regarding verification set out in the modified draft as well as the standards for verification for

non-account holders set out in §999.325 of the modified draft. The non-account holder verification standards require companies to verify requests to know categories of personal information with a reasonable degree of certainty, which may include matching at least two data points provided by the consumer with two data points maintained by the company. Such standards also require companies to verify requests to know specific pieces of personal information with a reasonably high degree of certainty, which may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the company, together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Such standards provide that a company's compliance with a request to delete may require either a reasonable degree or reasonably high degree of certainty, depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion (*e.g.*, deletion of family photographs may require a reasonably high degree of certainty, while deletion of browsing history may require only a reasonable degree of certainty).

- Companies that buy, sell or use the personal information of 10 million or more consumers for commercial purposes within a single calendar year are granted greater flexibility under the reporting obligations.
- Companies are prohibited from offering incentives to consumers to waive rights granted under the CCPA unless they can calculate a good-faith estimate of the value of the consumer data or demonstrate the reasonableness of the financial incentive, price or service difference.

Key Takeaways

While many do not expect major revisions to the current regulations before they go into effect, companies should monitor regulatory developments and make sure their CCPA programs comply with the regulations that actually go into effect. Enforcement of the CCPA begins on July 1, 2020.

Return to Table of Contents

New CFIUS Regulations Focus on Data Privacy Risks of Foreign Investments

On February 13, 2020, new U.S. Department of the Treasury regulations implementing the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) went into effect. The Treasury's FIRRMA regulations largely adopted many pre-FIRRMA CFIUS trends, standards and practices, while adding some new features in response to several national security concerns, including privacy-related concerns that foreign actors, particularly China, could use acquisitions of U.S. companies possessing significant amounts of sensitive personal data as an easy, legal form of bulk intelligence collection on U.S. citizens.

Background

FIRRMA was the first legislation in over a decade to reform national security reviews of foreign investments or acquisitions involving U.S. businesses by the Committee on Foreign Investment in the United States (CFIUS or the committee).

Motivated by these concerns, one of FIRRMA's more significant changes was to expand the committee's jurisdiction to cover some non-controlling investments in U.S. businesses. Historically, a transaction had to result in a foreign person gaining "control" of a U.S. business for CFIUS to have jurisdiction, and, although CFIUS interpreted "control" broadly, the definition had limits and permitted some forms of non-passive investment to fall outside the committee's jurisdiction. The new regulations implement expanded jurisdiction over U.S. businesses involved in the collection or maintenance of sensitive data about U.S. citizens (referred to as a Data U.S. Business by the regulations), critical technology or critical infrastructure, when a non-controlling investment in the business is accompanied by certain rights, such as access to material nonpublic technical information, a board observer position or substantive decision-making.

The data privacy concerns also resulted in the regulations including a wide range of U.S. businesses that likely would not have previously considered themselves to be of interest to CFIUS. The regulations accomplish this through broadly defined parameters for what constitutes sensitive personal data, stating:

- Sensitive personal data is "identifiable data," meaning that it "can be used to distinguish or trace an individual's identity, including without limitation through the use of any personal identifier."
- Identifiable data falls into one of several enumerated categories, including:
  - financial data that could be used to analyze or determine an individual's financial distress or hardship (which does not include consumer purchase information);
  - data from a consumer report, subject to certain exceptions;
  - insurance application information;
  - health information;
  - nonpublic electronic communications, such as email or text messaging;
  - biometric enrollment data, including facial, voice, retina/iris and palm/fingerprint templates;
  - data for generating a state or federal government ID card;
  - information about U.S. government security clearances and applications for such clearances;
  - genetic test results (which do not include data derived from databases maintained by the U.S. government and are routinely provided to private entities for research purposes); and
  - geolocation data, regardless of the method of collection (*e.g.*, mobile app, vehicle GPS, wearables).

Recognizing that virtually every U.S. business possesses at least some personal data of U.S. citizens, CFIUS provides several factors ostensibly designed to narrow the application of the regulations. For example, aggregated or anonymized data is not covered if a party to a transaction lacks the ability to disaggregate or de-anonymize the data. Encrypted data also is excluded if the business does not have the ability to decrypt the data or trace an individual's identity through the data. The regulations also exempt data concerning a business's own employees or publicly available information.

The regulations also include certain data thresholds that apply to all of the above categories, other than genetic test results. For example, the business also must have (1) data maintained or collected on over 1 million individuals over the past year; (2) a demonstrated objective to maintain or collect data on over 1 million individuals, with the data being an integrated part of the business' primary product or service; or (3) any amount of data, if the business targets or tailors products to U.S. national security agencies or their personnel. The regulations also include an exception to the data threshold if the business can demonstrate that it does not and will not have the capability to maintain or collect sensitive information on over 1 million persons as of the closing of a transaction in question. It is important to note, however, that these data counts are not limited to U.S. citizens, which further lowers the bar for companies.

Nevertheless, in practice, the thresholds described above are unlikely to narrow CFIUS' scope significantly or reduce CFIUS risks for many businesses and investors. Possessing or seeking to possess data on 1 million or more persons is no longer a sizable figure for many businesses, especially considering data collection types such as geolocation that are widely used by mobile apps. Examples in the regulations also confirm CFIUS' expansive scope, providing cases where the total sum of different types of data adds up to more than 1 million persons and stating that the time period for demonstrating a business objective to maintain or collect sensitive data from 1 million individuals could extend to at least two years.

Key Takeaways

The new regulations will affect a wide range of companies and transactions that may not have traditionally been considered of interest to U.S. national security. Additionally, CFIUS has shown an interest in all types of data over the past several years, not just identifiable data that meets the definition of a Data U.S. Business. Data sensitivity can provide a hook for CFIUS to assert jurisdiction in any transaction where the committee may have other concerns about a foreign investor. As such, foreign investors will want to expand their diligence regarding how a U.S. business collects, stores and protects its data (particularly U.S. personal data) when considering a new investment. Conversely, sellers should be interested in a potential investor's history of data-related compliance and practices.[2]

Return to Table of Contents

[2] For more detailed analysis of the new regulations, including how this expanded jurisdiction may apply to filings with CFIUS, please see our recent client alert "CFIUS' Final Rules: Broader Reach, Narrow Exceptions and Foretelling Future Change."

SEC's OCIE Releases Cybersecurity Observations and Guidance

The Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE) published observations on cybersecurity and resiliency practices for market participants.

On January 27, 2020, the OCIE released a report[3] highlighting the measures organizations have taken to prevent cybersecurity incidents. As the report notes, this is not a major shift for the SEC, as the agency has focused on cybersecurity with respect to market systems, data protection and compliance for several years.

The January report is one of the most comprehensive cybersecurity reports provided by the SEC to date. Recognizing there is not one approach to cybersecurity that applies to all organizations, the OCIE based its guidance on its overall findings from examinations of a variety of SEC registrants, including broker-dealers, investment advisers, clearing agencies and national securities exchanges.

The report includes observations across seven key areas: governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor management, and training and awareness.

Governance and Risk Management

The OCIE found that incorporating cybersecurity protocols into an organization's governance and risk management program is key for demonstrating an organization's commitment to mitigating cybersecurity risks. The report notes that successful programs in this area generally include cybersecurity risk assessments and enforcement of written policies and procedures to address the identified risks. In practice, the OCIE has observed organizations (1) engaging senior level leadership to set and oversee cybersecurity programs, (2) establishing testing methods to continually evaluate cybersecurity policies and procedures, updating policies where necessary, and (3) implementing communication policies to facilitate effective communication between decision makers, customers, employees and regulators.

Access Rights and Controls

The OCIE notes that access controls generally include understanding the location of data within the organization, restricting access to systems to authorized users, and establishing appropriate controls to prevent and monitor unauthorized access. The OCIE also notes that successful access control strategies often involve developing a clear understanding of user access needs in order to limit access to users with legitimate and authorized purposes. The report also emphasizes effective access management strategies, which include limiting access when appropriate, implementing separation of duties for access approval, requiring strong passwords with periodic changes, utilizing multifactor authentication and promptly terminating former employees' access to data.

Data Loss Prevention

The OCIE observed organizations protecting against the loss or misuse of sensitive data by (1) establishing vulnerability management programs, (2) monitoring incoming and outgoing network traffic (*i.e.*, using firewalls, web proxy systems and intrusion detection systems), (3) implementing endpoint threat detection capabilities, (4) establishing patch management programs for software and hardware, (5) maintaining an inventory of hardware and software, including how such systems are protected, (6) encrypting data and implementing network segmentation, (7) monitoring insider threats through testing business systems and conducting penetration tests, and (8) securing legacy systems and equipment to ensure that any disposal of hardware and software programs does not lead to vulnerabilities.

Mobile Security

The report states that organizations can mitigate the cybersecurity risks associated with the use of mobile devices and applications by implementing policies and procedures for use; using mobile device management applications; requiring multifactor authentication for all users; preventing printing, copying and saving to personally owned devices; maintaining the ability to remotely wipe content from a lost device; and providing employee training.

Incident Response and Resiliency

In order to ensure business continuity, the OCIE observed that many organizations' incident response plans are risk-assessed plans that consider a wide array of scenarios and contemplate compliance with applicable federal and state reporting requirements for breaches or cyber events, designate employees to address cyber incidents, and include tests of the response plan (such as tabletop exercises). The OCIE noted the use of the following to address resiliency: identifying and maintaining an inventory of core business operations and systems, conducting risk assessments, prioritizing business operations, and maintaining additional safeguards, including back-up capabilities on different networks as well as offline.

[3] The OCIE's report is available here.

Vendor Management

The OCIE has observed vendor management practices to include programs aimed at ensuring vendor compliance with security requirements and safeguards, showing a clear understanding of all vendor contract terms to ensure alignment on risk and security protocols, and ongoing monitoring of the vendor relationship.

Training and Awareness

The report highlights several training and awareness practices, including fostering a culture of cybersecurity preparedness, providing specific cybersecurity training (*i.e.*, phishing exercises) and monitoring the effectiveness of such trainings.

Key Takeaways

The measures set out in the report may be viewed as an indication of the OCIE's expectations in cybersecurity examinations moving forward. Companies regulated by the SEC should consider this guidance when evaluating their current cybersecurity practices.

Return to Table of Contents

Federal Court Holds That Losses From Ransomware Attack are Covered Under Businessowners Policy

A federal court in Maryland recently held that the loss of data, software and functionality of a computer system suffered as a result of a ransomware attack were covered under a businessowners policy, finding that such losses constituted "direct physical loss of or damage to" covered property.

On January 25, 2020, the U.S. District Court for the District of Maryland issued a decision holding that insurer State Auto Property and Casualty Insurance Company (State Auto) owed coverage under a businessowners policy issued to its insured, National Ink & Stitch, LLC (National Ink), for losses sustained as a result of a ransomware attack.[4]

The Ransomware Attack

National Ink, an embroidery and screenprinting company, stored art, logos and designs on its computer server, which also held various types of software. In December 2016, National Ink suffered a ransomware attack that prohibited the company from accessing that software and data. After National Ink complied with the attacker's initial bitcoin demand, the attacker refused to release the software and data absent additional payment. In response, National Ink hired a security company to replace and reinstall its software and install protective software. However, the protective software caused the computers to operate at a very slow pace and National Ink was unable to access a significant portion of the software and data. As well, dormant remnants of the ransomware continued to threaten the system.

National Ink's Insurance Claim

National Ink submitted a claim under its businessowners policy to replace the entire system. The policy covered "direct physical loss of or damage to Covered Property ... caused by or resulting from any Covered Cause of Loss." "Covered Property" encompassed "Electronic Media and Record (Including Software)," which included "(a) Electronic data processing, recording or storage media such as files, tapes, discs, drums or cells; [and] (b) data stored on such media." State Auto denied coverage, contending that National Ink only lost an intangible asset — the data — and could still use the computer system to operate its business. State Auto therefore claimed that the company not experience "direct physical loss" as necessary to trigger coverage. National Ink then filed suit.

The Court's Decision

On cross-motions for summary judgment, the court ruled in National Ink's favor, holding that it "can recover based on either (1) the loss of data and software in its computer system, or (2) the loss of functionality to the computer system itself."

With respect to National Ink's loss of data and software, the court reasoned that "the Policy expressly lists 'data' as an example of Covered Property under its definition of 'Electronic Media and Records (Including Software)." The court was not moved by the fact that the term "data" is qualified with the phrase "stored on such media." Rather, "if the Policy intended to require physical loss or damage to the media itself, as opposed to just the data, it could have stopped at subsection (a), which describes the covered media" but instead goes on to "include 'data stored on such media' as a separate subcategory of Covered Property in subsection (b)." The court further observed that the policy "also contains the phrase 'Including Software' in its heading describing covered property." In reaching its conclusion, the court distinguished the authorities cited by State Auto, including a matter where, unlike in the National Ink case, the policy limited coverage to "tangible property."

[4] *Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co.*, No. CV SAG-18-2138, 2020 WL 374460 (D. Md. January 23, 2020).

Turning to the damage to the computer system itself, the court rejected State Auto's argument that the system must be completely inoperable in order to constitute "physical loss or damage." Rather, after evaluating the policy language and case law, the court was persuaded that "loss of use, loss of reliability, or impaired functionality demonstrate the required damage to a computer system, consistent with the 'physical loss *or damage to*' language in the Policy." Specifically, the court explained that National Ink was left with a slower system, which appears to be plagued by a dormant virus, and a significant portion of software and data remained inaccessible.

Key Takeaways

The *National Ink* decision illustrates that insurance coverage for cyber-related losses is not necessarily limited to specialized cyber policies. In this case, the court determined that losses arising out of a ransomware attack were covered by the plain language of a businessowners policy. The decision also serves as an important reminder for insurers and policyholders to closely review and fully understand a policy's terms and conditions.

Return to Table of Contents

ICO Publishes Age-Appropriate Design Code

On January 21, 2020, the U.K.'s data protection supervisory authority, the Information Commissioner's Office (ICO), published a code of practice for online services likely to be accessed by children, titled "Age Appropriate Design: A Code of Practice for Online Services" (the code)[5] outlining how to ensure that services are appropriate for use by children. The ICO anticipates that the code will not be fully effective until fall 2021 as it needs to be laid before Parliament, after which there will be a 12-month transition period. Therefore, online service providers that are covered by the code have time to ensure that they comply

Background and Legal Effect

The code is a statutory code of practice that the ICO is required to prepare under the Data Protection Act 2018 (DPA). The DPA makes clear that the code is not law as liability does not arise simply from a failure to act in accordance with the code. However, the DPA requires the ICO to take the code into account when considering whether an online service has complied with its obligations under the General Data Protection Regulation (EU) 2016/679 (GDPR) or the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Consequently, failure to conform to the code could cause the ICO to take action.

Online Services Covered by the Code

The code applies to online services that are (1) "relevant information society services" (RISS) and (2) "likely to be accessed by children."

An RISS is defined under the GDPR as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." This effectively means that most online services qualify as an RISS, including online games, news websites, search engines and social media platforms. Funding through advertising, as opposed to payment by the end user, fulfils the remuneration requirement.

For the purposes of the code, a person under 18 years of age is a child. This is in contrast with the GDPR's approach to consent, which allows for European Economic Area (EEA) member states to establish an age between 13 and 16-years-old at which a child's consent alone is a lawful basis for processing.

For an RISS to be determined to be likely accessed by children, the possibility of this happening needs to be more probable than not. If user data shows that children form a substantial group of users, the requirement will be fulfilled. Otherwise this will be assessed on (1) the nature and content of the RISS; and (2) the way in which the RISS is accessed and the measures put in place to prevent access by children. For example, a website containing adult material should not be applying the code, even if a substantial group of users are under 18, as such a provider should be focused on preventing access rather than making it child-friendly. If the decision is made that an RISS is not going to be regularly accessed by children, this should be documented and reviewed on an ongoing basis.

The geographical scope of the code is equivalent to that of the DPA. Consequently, it applies to online services (1) established in the U.K.; and (2) with no establishment in the U.K. or the EEA, but offering services to, or monitoring the behavior of, users in the U.K. Currently, the code does not apply to an online service that does not have a U.K. establishment but does have an EEA establishment. However, following the end of the Brexit transition period (currently December 31, 2020), the code will apply to an online service established in the EEA that targets U.K. users.

[5] The code is available here.

Standards of Age-Appropriate Design

The code sets out 15 standards of age-appropriate design.[6] Below is a summary of some of the standards.

The first standard establishes that the best interests of each child that is likely to access an online service should be a primary design and development consideration for such service. This is in line with the commitments under the United Nations Convention of the Rights of Children (UNCRC), to which the U.K. is a signatory. The code makes clear that the commercial interests of an organization are unlikely to ever outweigh a child's right to privacy.

The third standard requires age-appropriate application of the code. While it is ultimately for the online service provider to establish how to meet this standard, the code suggests that children be banded into five developmental age ranges: 0-5, 6-9, 10-12, 13-15 and 16-17. Online service providers should then establish whether a given user falls into any of those bands and tailor the safeguards appropriately on a risk-based approach: for low-risk services, self-declaration (where a user simply states that they are of a certain age while providing no further evidence) may be appropriate, while very high-risk services may require formal identity documents, such as a passport, although the code does recommend not going to such lengths as children may not have access to such documents.

The fourth standard relates to the lawfulness, fairness and transparency principle set out under the GDPR and requires information about how the personal data of users is handled to be tailored to that user's age-group. For example, the privacy notice to be provided should be tailored for parents if the user is 0-12 years old, while the privacy notice should be tailored to the child if the child is also tailored if the user is 13-17 years old. It also is recommended that "just-in-time" notices ensure that children are provided with an explanation at the point at which the use of the personal data is activated (*e.g.* if a child were to try to change a privacy setting).

The seventh standard requires that the privacy settings for a child user should be set to "high" by default. The code makes clear that a privacy setting is not required for any personal data that has to be processed to provide the core service. However, anything superfluous to the core service, such as to personalize the service, should have to be activated by the user. Tied to this are the 10th and 12th standards, which require geolocation and profiling options to be set to "off" by default unless they are core to the service. The 13th standard also is tied to the seventh in that it requires online services to not use nudge techniques to encourage children to provide personal data that is not needed or to alter privacy settings (*e.g.*, by pre-filling options in a way that would lead to more personal data being collected). Pro-privacy nudge techniques are, however, encouraged.

The ninth standard prevents the sharing of children's personal data unless there is a "compelling reason" to do so, such as to prevent or detect crimes against children. It is made clear that the sale of children's personal data for commercial use is unlikely to constitute a compelling reason.

The 11th standard requires children to be made aware when any parental monitoring and tracking is ongoing. While parents can be expected to have their children's best interests at heart, monitoring of a child's online activities is still considered an intrusion into that child's privacy. The code also suggests that parents should be provided with information about the rights of children regarding privacy and resources to discuss privacy with their children.

Proving Compliance

In accordance with the GDPR's accountability principle, the code expects online service providers to be able to prove their compliance. This will, to some extent, be achieved simply by following the code. For instance, the second standard requires a data protection impact assessment to be carried out whenever an online service is likely to be accessed by a child. In addition, paper trails such as training records and policies should be kept.

Key Takeaways

The code's transition through Parliament is not expected to lead to significant amendments. Given the importance of the code to proving compliance with the GDPR, companies subject to the code should therefore begin to consider how they will comply. This will put them in a strong position once the code's transition through Parliament is complete and the 12-month transition period begins.

Return to Table of Contents

[6] The full 15 standards of age appropriate design are: (1) Best Interests of the Child, (2) Data Protection Impact Assessments, (3) Age Appropriate Application, (4) Transparency, (5) Detrimental Use of Data, (6) Policies and Community Standards, (7) Default Settings, (8) Data Minimisation, (9) Data Sharing, (10) Geolocation, (11) Parental Controls, (12) Profiling, (13) Nudge Techniques, (14) Connected Toys and Devices, and (15) Online Tools.

Federal District Court Holds Bare Procedural Violations of Illinois Biometric Privacy Act Fail to Establish Article III Standing

In *Hunter v. Automated Health Systems, Inc.*, the U.S. District Court for the Northern District of Illinois held that the defendant's alleged violations of the notice, consent, and data retention and destruction provisions in the Illinois Biometric Information Privacy Act (BIPA) failed to constitute a "concrete injury" for purposes of Article III standing. Notwithstanding the alleged lack of notice and consent, the court ruled the plaintiff was aware that the defendant collected and stored her fingerprints in connection with an employee time clock system. The court also ruled the plaintiff failed to show an increased risk of harm from her fingerprints being allegedly provided to a third-party payroll vendor.

Background

Under the BIPA, a private entity desiring to collect biometric information must (1) provide notice to persons that their biometric information is being collected or stored; (2) inform those persons in writing of the "specific purpose and length of term" for which their biometrics are being collected, stored and used; and (3) obtain a written release. Private entities also must develop and comply with a written retention schedule, as well as guidelines for permanently destroying biometric data when certain conditions are met. In enacting the notice, consent, and data retention and destruction provisions, the Illinois General Assembly found that "[b]iometrics … are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at a heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."

The BIPA provides a private right of action to persons "aggrieved" by violations, with negligent violations carrying statutory damages of $1,000 per violation and intentional or reckless violations carrying statutory damages of $5,000 per violation. In either case, a plaintiff may recover actual damages if they are greater than the recoverable statutory damages.

The plaintiff, Evelyn Hunter, sued her employer, Automated Health Systems, Inc., on the ground that it was collecting her fingerprints through a time-tracking system, in violation of the BIPA. Specifically, the plaintiff alleged that the company failed to provide the required notice, obtain the required consent, and provide and comply with the required retention schedule and destruction guidelines.

To satisfy itself that federal jurisdiction existed, the court *sua sponte* asked the parties to brief whether the plaintiff had alleged an injury-in-fact sufficient to establish Article III standing.

The Order

The court held that the plaintiff failed to allege an injury-in-fact and remanded the case to state court.[7] Quoting the U.S. Supreme Court in *Spokeo, Inc. v. Robbins*, 136 S. Ct. 1540 (2016), the court stated that a "bare procedural violation [of a statute] divorced from any concrete" injury does not qualify as an injury-in-fact. Concrete injury exists if the statutory violation presents an "appreciable risk of harm to the underlying interest the [legislature] sought to protect by enacting the statute."

Although the plaintiff alleged that the defendant failed to comply with the BIPA's notice and consent provisions, those procedural violations caused the plaintiff no "concrete injury." Not surprisingly, the plaintiff failed to allege that the defendant "collected her biometric data without her knowledge." As stated in a similar case on which the court relied, *Aguilar v. Rexnord, LLC*, the plaintiff in that case could not assert such allegations because he "knew his fingerprints were being collected" despite not receiving notice or giving consent required by the BIPA, with the court also stating "[h]e scanned them each time he clocked in and out at work, and it was clear that the fingerprints were stored since they were used for authentication purposes."[8]

The court also concluded that the plaintiff failed to allege that the defendant "created a risk that [her] data would fall into the hands of an unauthorized third party." The plaintiff admitted that in her original complaint she was not alleging any disclosure of biometric data to a third party, such as a payroll company, and that she was not presently aware of any "data breach, identity theft, or similar loss." As such, the plaintiff had merely alleged the retention of biometric data, in violation of the BIPA. But, mere retention of biometric information "absent allegations of dissemination, or at least an appreciate risk of dissemination" does not suffice to support Article III standing, the court reasoned. Even an amended complaint alleging dissemination of her biometric data to the defendant's payroll vendor would fail, the court reasoned, because the plaintiff admitted that she could

[7] 2020 WL 833180 (N.D. Ill. February 20, 2020).
[8] 2018 WL 3239715, at*3 (N.D. Ill. July 3, 2018).

not allege that the vendor lacked "any data security controls." Disclosure to the payroll vendor therefore did not "create[] an increased risk of harm that the BIPA was designed to protect, such as identity theft."

The court also distinguished between an injury-in-fact for Article III standing purposes and sufficient injury to sue under the BIPA. Although the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp.* held that a party is "aggrieved" under the BIPA (*i.e.*, has statutory standing to sue) without having to allege any "actual injury or damage beyond infringement of the rights afforded under the law," Article III's standing requirement is distinct and requires more, the court reasoned,[9] stating it requires a "concrete and particularized" injury that is "actual and imminent and not conjectural or hypothetical."

[9] 2019 IL 123186.

Key Takeaways

Federal district courts addressing lawsuits under the BIPA continue to hold that bare violations of the act's procedural provisions fail to establish an injury-in-fact for Article III standing purposes. A plaintiff must allege "concrete" harm from a defendant's failure to provide the required notice or obtain the required consent. A plaintiff also must allege an increased risk of harm, such as identify theft, from the failure to comply with the BIPA's data retention and destruction provisions.

Return to Table of Contents

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

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

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@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

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@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