May 2020

Skadden

Privacy & Cybersecurity Update

1 Seventh Circuit Finds Standing for Illinois BIPA Claimant

2 European Data Protection Board Adopts Updated Guidelines on Consent Under the GDPR

4 COVID-19 Pandemic Brings Added Attention to Cyber Insurance

4 Trump Administration Issues Executive Order Prohibiting Acquisition and Installation Power System Electric Equipment From Foreign Adversaries

Seventh Circuit Finds Standing for Illinois BIPA Claimant

On May 5, 2020, the U.S. Court of Appeals for the Seventh Circuit held in *Bryant v. Compass Group USA, Inc.* that an Illinois plaintiff had sufficient standing to sue in federal court for an alleged violation of the Illinois Biometric Information Privacy Act (BIPA), even though she did not allege a harm beyond violation of the act. The case is consistent with a recent standing decision by the Supreme Court of Illinois but deepens the circuit split regarding the level of harm necessary to meet federal standing requirements for claims under the act.

Background

The Illinois Biometric Information Privacy Act[1] regulates the collection, use and retention of a person's biometric identifiers or information, including fingerprints, retina scans and facial geometry scans. BIPA imposes certain requirements on businesses that collect or otherwise obtain biometric information, including, under Section 15(b) of the act, obtaining the informed consent of any person whose data is acquired and, under Section 15(a) of the act, disclosing a retention schedule and guidelines for permanent destruction of such information.

Under BIPA, any individual "aggrieved" by a violation of the informed consent and disclosure obligations can bring a private action. Last year, the Supreme Court of Illinois held that a violation of a private plaintiff's legal rights under BIPA alone (without further harm) was sufficient to bring a suit in Illinois State Court.[2] The decision, *Rosenbach v. Six Flags Entertainment Corp.*, concerned plaintiff Stacy Rosenbach, who brought a class action suit against Six Flags for violating BIPA when it required her son to scan his fingerprint without obtaining informed consent or providing a policy regarding the use or storage of the scans.[3] The Rosenbach ruling held that an individual is "aggrieved" when their BIPA rights are violated, and therefore can bring a claim even if the only harm is a violation of their legal rights.

[1] 740 ILCS 14 (2008). The text of the BIPA can be found here.

[2] The decision can be found here.

[3] See Skadden's January 29, 2019, article "Illinois Supreme Court Holds That Biometric Privacy Law Does Not Require Actual Harm for Private Suits" for further discussion on this decision.

Rosenbach resulted in an uptick in lawsuits arising under BIPA, but it remained unclear afterward whether such cases could meet Article III standing requirements in federal court, in part because there is a circuit split on the question. For example, in 2019, the Ninth Circuit held that a violation of Facebook users' rights under BIPA was a sufficient concrete injury for Article III standing purposes when Facebook used its facial recognition feature without obtaining informed consent from its users. However, this decision was a departure from a Second Circuit decision in 2017, where the court held that a plaintiff who brought a BIPA claim against a video game company that scanned individuals' faces to create custom avatars without informed consent lacked standing under Article III because the procedural violations did not raise a material risk of harm to the plaintiff's interests. The Seventh Circuit had not yet addressed this matter before its decision in *Compass*.

The Decision

In *Compass*, plaintiff Christine Bryant, a call-center employee, voluntarily provided her fingerprint scan to create an account with her cafeteria's vending machine, which was owned and operated by Compass.[4] Bryant alleged that Compass failed to (1) make publicly available a retention schedule and guidelines regarding the biometric identifiers and (2) obtain informed consent from plaintiff to collect, store and use her fingerprint scan in violation of Sections 15(a) and 15(b) of BIPA.

The plaintiff brought a putative class action against Compass in Illinois State Court as an individual "aggrieved" by the violation of the act. Compass then removed the case to federal court under the Class Action Fairness Act. The plaintiff subsequently moved to remand on the grounds that she did not suffer an injury sufficient to support Article III standing in federal court. The district court granted the plaintiff's remand, finding Compass's alleged violations did not cause concrete harm to the plaintiff, after which Compass petitioned the Seventh Circuit to appeal the remand order.

Drawing from the U.S. Supreme Court ruling in *Spokeo, Inc. v. Robins*, the Seventh Circuit distinguished between two types of cases in reaching its decision: cases where a private plaintiff asserts their own rights and injuries, and cases where a private plaintiff seeks vindication of public rights. The Seventh Circuit found that the plaintiff's claim regarding Compass's failure to obtain informed consent before it collected fingerprint scans, in violation of Section 15(b) of BIPA, was an assertion of the plaintiff's own rights. The court held that the lack of opportunity for the plaintiff and others to consider whether the terms of the collection and usage of the scans were acceptable given the attendant risks constituted a concrete and peculiarized injury sufficient for the plaintiff to meet the requirements for Article III standing in the Seventh Circuit.

With respect to the plaintiff's claim regarding Compass's failure to disclose a retention schedule and appropriate guidelines in violation of Section 15(a) of BIPA, the court found that the duty to disclose is a duty owed to the public generally and not one to a particular person. Therefore, given the plaintiff did not allege a particularized harm resulting from Compass's failure to comply with Section 15(a), the court found that the plaintiff did not suffer a concrete and particularized injury and thus lacked standing under Article III with respect to the claim under Section 15(a) of BIPA.

Key Takeaways

The *Compass* decision aligns with *Rosenbach* to provide clarity in Illinois state and federal courts regarding standing requirements for violations of BIPA, while also deepening the circuit split on standing. The decision additionally provides defendants an opportunity to remove Section 15(b) claims to federal court, which may provide defendants with a new strategic avenue; however, the decision also may result in an increase in claims under Section 15(b) of BIPA in federal court. Therefore, companies should consider carefully whether they have put proper safeguards in place to ensure BIPA compliance.[5]

Return to Table of Contents

European Data Protection Board Adopts Updated Guidelines on Consent Under the GDPR

On May 4, 2020, the European Data Protection Board (EDPB) adopted guidelines on the use of consent as a legal basis for the processing of personal data under Regulation 2016/679 (GDPR).[6] The guidelines are a slightly updated version of those on consent adopted by the Article 29 Working Party on April 10, 2018,[7] which the EDPB then endorsed in conjunction with the GDPR.[8] The guidelines provide substantive clarification on two topics: (1) the conditionality of consent, in particular, the validity of consent when using "cookie walls" and (2) the unambiguous indication of wishes, in particular, the use of scrolling to indicate consent.

[4] The decision is available here.

[5] Certain BIPA compliance pointers may be found here.

[6] The EDPB guidelines can be found here.

[7] The Article 29 Working Party guidelines can be found here.

[8] The EDPC endorsed the Article 29 guidelines on May 25, 2018.

Background

Consent is one of the six lawful bases that can be used to process personal data, as provided for under Article 6 of the GDPR. Generally, consent can only be secured on an appropriate lawful basis if an individual has control and is offered a genuine choice with regard to accepting or declining the terms offered. Article 4(11) of the GDPR makes clear that consent must be freely given, specific, informed and unambiguous. As a general rule, if consent is bundled up as a nonnegotiable part of the terms and conditions of a contract, or a prerequisite to the provision of some good(s) or service(s), then it is presumed not to have been freely given. Consent also should be a reversible decision so that the data subject retains a degree of control. The guidelines provide a thorough analysis of the notion of consent under the GDPR to allow controllers to ensure that a data subject's consent is valid.

Clarification 1: Cookie Walls

A cookie wall is a form of consent which obliges the visitors of a website to accept the use of cookies in order to access the website itself or certain services on the website. Data protection authorities across the European Economic Area (EEA) have taken different views on the use of cookie walls. The U.K.'s data protection authority, the Information Commissioner's Office (ICO), has previously suggested that cookie walls could be permitted in limited circumstances, including where the use of cookies do not compel website visitors to consent to their personal data being processed. Conversely, data protection authorities in countries like the Netherlands (the Autoriteit Persoonsgegevens) and France (the Commission Nationale de l'Informatique et des Libertés) have opined that cookie walls are not acceptable under any circumstances.

The guidelines confirm the EDPB's position on the use of cookie walls, stating that in order for consent to be freely given "access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls)." Accordingly, the EDPB does not view cookie walls as GDPR-compliant as they fail to present individuals with a genuine choice. Where access to a website or use of a service is conditional upon the acceptance of or consent to cookies, that acceptance/consent is not freely given. The guidelines clarify that cookie walls are unlawful and consent obtained via such mechanisms will not be considered valid as it cannot be seen to be freely given for the purposes of the GDPR.

Clarification 2: Scrolling and Consent

Valid consent under the GDPR requires either a statement from the data subject or a clear affirmative act. In either case, consent must be given through an active motion or declaration (*i.e.*, it must be obvious that the data subject has consented). Article 4(11) of the GDPR states that valid consent requires an unambiguous indication of wishes. The guidelines note that the most literal way to satisfy this requirement would be via a "written statement" where the data subject writes in a letter or types in an email specifically the processing to which he or she agrees. The EDPB recognizes that this is often not realistic and that organizations develop consent flow mechanisms that suit their products and enhance user experience, which may include the use of physical motions (such as swiping a bar on a screen) to indicate clear affirmative action.

The guidelines state that controllers should design consent mechanisms that are clear and unambiguous, and that such mechanisms must ensure that the action by which consent is given can be distinguished from other actions. To that end, merely continuing the ordinary use of a website is not conduct from which unambiguous indication of consent can be inferred. The guidelines confirm that scrolling or swiping through a webpage will not, under any circumstances, satisfy the requirement of a clear and affirmative action. According to the EDPB, such actions may be difficult to distinguish from other user activity and therefore cannot be used to determine unambiguous consent. The guidelines also note that in such cases, it would be difficult for users to withdraw their consent as easily as they gave it.

Key Takeaways

The guidelines clarify that cookie walls and scrolling/swiping through a webpage cannot be used to obtain valid consent for the purposes of the GDPR. This clarification will be welcomed by online service providers, who now must ensure that access to their services is not conditional upon user consent and that individuals are given a genuine choice as to whether they accept or decline the use of cookies. The guidelines come at an interesting time, as the ICO recently stated that it is pausing investigations and enforcement actions into real-time bidding and the advertising technology industry during the pandemic.[9] The EDPB's adoption of the guidelines should encourage a more uniform approach from EEA-based data protection authorities when it comes to cookie walls and affirmative action consent, but as the U.K. is no longer a part of the EU, it remains to be seen whether the ICO will differ in its approach.

Return to Table of Contents

[9] The ICO's recent statements can be found here.

COVID-19 Pandemic Brings Added Attention to Cyber Insurance

The COVID-19 pandemic is exposing companies to increased cyber risks as an unprecedented portion of the workforce continues to work remotely. Cyber insurance is one tool that can be used to help mitigate this increased risk. Whether a company currently maintains cyber insurance, or is considering procuring cyber insurance for the first time, it is important to have a full understanding of what coverage is — and is not — provided by their policies.

What Does Cyber Insurance Cover?

While cyber insurance policies often include a similar array of coverages, the policy forms are not standardized, as each policy will have its own variations based on the insurer and the needs of a particular company. Companies should note these variations when reviewing policies they currently have or are debating procuring. Nonetheless, while the scope of coverage can vary widely, cyber insurance policies often include coverage for network security and privacy liability, business interruption, media liability, and regulatory defense and penalties.

Network Security and Privacy Liability Coverage

Network security and privacy liability provides coverage for first-party losses incurred as a result of a cyber incident. First-party losses often include costs for forensic services, notification to affected consumers, data restoration, public relations response and management, establishing a call center for affected persons, credit monitoring services and ransom payments. This coverage also typically protects a company for liability arising out of third-party claims resulting from a security breach of the company's computer system, including unauthorized access or use, viruses or denial of service attacks. Moreover, it often provides coverage for third-party claims alleging that a company failed to protect personally identifiable information stored on the company's computer system.

Business Interruption Coverage

Business interruption often provides coverage for lost profits and certain expenses resulting from a network security or system failure. Business interruption coverage provided under a traditional property insurance policy may not cover cyber-related business interruption losses.

Media Liability Coverage

Media liability typically provides coverage for the display or production of media content resulting in, among other things, claims alleging defamation, invasion of the right to privacy, copyright and/or trademark infringement, and plagiarism.

Regulatory Defense and Penalties Coverage

Regulatory defense and penalties policies often include coverage for regulatory fines and penalties incurred in privacy-related regulatory proceedings and investigations brought by federal, state or local governmental agencies. They also typically cover associated defense costs.

Illustrative Policy Exclusions

As with most insurance policies, cyber insurance policies usually include a variety of exclusions that bar or limit the scope of coverage. For example, among other things, some cyber insurance policies exclude or limit coverage for losses arising from infrastructure that is not owned or leased by the insured; unencrypted devices; failure to maintain adequate security standards; bodily injury and property damage; prior acts; and war and terrorism.

Key Takeaways

Cyber insurance policies are not standardized and come in many shapes and sizes. In light of the COVID-19 pandemic, perhaps now more than ever it is important that companies have a thorough understanding of the terms, conditions and exclusions in the policies that they have or are considering. For companies that do not currently maintain cyber insurance, now may be a good time to reevaluate the possible addition of this coverage line to their insurance policies.

Return to Table of Contents

Trump Administration Issues Executive Order Prohibiting Acquisition and Installation Power System Electric Equipment From Foreign Adversaries

On May 1, 2020, President Donald Trump issued an executive order prohibiting the acquisition and installation of "bulk-power system electric equipment" (such as generators, circuit breakers, metering equipment, generation turbines and industrial control systems) supplied by foreign adversaries and persons subject to their control, and establishing the creation of a task force to monitor threats to the U.S. power system from foreign adversaries.

Overview of the Executive Order

The Trump administration's executive order outlines a threat to U.S. national security and national emergency arising from the

acquisition, importation, transfer or installation of bulk-power system electric equipment supplied by foreign adversaries.[10] To address this concern, the president authorized the prohibition of any acquisition, importation, transfer or installation of any bulk-power system electric equipment by any person, any of which is defined as a "transaction" if:

- the transaction involves bulk-power system electric equipment designed, developed, manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and
- the transaction:
  - poses an undue risk of sabotage to, or subversion of, the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of the "bulk-power system" in the U.S.;
  - poses an undue risk of catastrophic effects on the security or resiliency of the U.S.'s critical infrastructure or the economy of the U.S.; or
  - otherwise poses an unacceptable risk to the national security of the U.S. or the security and safety of U.S. persons.

The new executive order's geographic limitation on the source of the bulk-power system electric equipment does not apply only to companies formed or organized in the adversarial nation or operating within the adversarial nation. Rather, in the case of a country like China — which is surely the principal focus of the executive order — bulk-power system electric equipment produced by a Chinese company both inside and outside China, as well as bulk-power system electric equipment produced by non-Chinese companies — such as U.S. or European companies with facilities in China — that manufacture bulk-power system electric equipment in China, would all be subject to the executive order.

The U.S. Department of Energy — in consultation with the departments of Defense and Homeland Security and the Office of the Director of National Intelligence (as well as other agencies, as appropriate) — is responsible for implementing the executive order, including issuing regulations within 150 days (by September 28, 2020).

The executive order expressly details the following areas as likely topics for the Department of Energy's regulatory implementation:

- identification of specific countries or persons to be considered foreign adversaries for the purposes of the executive order;
- identification of persons owned by, controlled by or subject to the jurisdiction or direction of a foreign adversary for the purposes of the executive order;
- identification of specific equipment or countries warranting particular scrutiny under the provisions of the executive order;
- establishment of procedures to license transactions otherwise prohibited pursuant to the executive order; and
- identification of a mechanism and relevant factors for the negotiation of agreements to mitigate concerns relating to U.S. acquisition and use of bulk-power system electric equipment provided by foreign adversaries.

General Motivating Concerns

The executive order closely tracks broad Trump administration trade and national security concerns regarding China, as well as more specific concerns regarding energy infrastructure security. The increasing focus on inbound transactions in the information and communication technology and energy sectors mirrors the more aggressive actions the U.S. has taken with respect to preventing countries it views as a concern, most notably China, from obtaining U.S.-origin technology.

Furthermore, the executive order to protect U.S. energy infrastructure follows years of warnings from the departments of Homeland Security and Energy about the potentially disastrous impacts successful attacks on the power grid could have on the country as well as the increasing amount of nation-state cybersecurity threats facing U.S. energy infrastructure. For example, in 2018, the Department of Energy established the Office of Cybersecurity, Energy Security and Emergency Response specifically to prepare for and respond to cybersecurity threats to energy infrastructure and issued its "Multiyear Plan for Energy Security Cybersecurity," which noted dramatic increases in nation-state-level targeting of U.S. energy infrastructure. The president's National Infrastructure Advisory Council followed with its 2018 report, "Surviving a Catastrophic Power Outage: How To Strengthen the Capabilities of the Nation," which discussed the profound risk a catastrophic power outage would pose to national and economic security and highlighted the role cybersecurity and physical attacks by sophisticated actors could play in such an outage. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency also has issued numerous alerts about potential cybersecurity attacks on the energy infrastructure sector generally, as well as specific aspects of the infrastructure, such as industrial control systems. Additionally, in June 2019, the Federal Energy Regulatory Commission issued an order directing the North American Electric Reliability Corporation to bolster the cybersecurity of the bulk-power system

[10] A copy of the executive order may be found here.

through expanded reporting requirements for incidents involving attempts to compromise bulk-power system operation.[11]

Key Takeaways

The federal government continues to take steps designed to protect the U.S. energy infrastructure from nation-state cybersecurity threats. Given the widespread use of Chinese equipment in electric industry infrastructure, the executive order will add a material layer of new regulatory oversight of many transactions. The details of the approval procedures obviously are not yet known, but it seems relatively certain that those procedures will force many industry participants to seek alternative equipment choices, which means the executive order could complicate transactions, particularly during the interim period before regulations are issued.

Return to Table of Contents

[11] Skadden's original client mailing on the topic, "Trump Administration Limits Acquisitions and Use of Bulk-Power System Electric Equipment From Foreign Adversaries," discusses the executive order in more detail.

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