Skadden

Privacy & Cybersecurity Update

Swiss Data Protection Authority Determines the Swiss-US Privacy Shield Does Not Protect Data Sent to US

The Swiss Federal Data Protection and Information Commissioner (FDPIC) recently concluded that the Swiss-U.S. Privacy Shield regime fails to provide an adequate level of protection for data transferred out of Switzerland to the United States.

The FDPIC, which oversees the protection of personal data in Switzerland, maintains a list of countries that satisfy the "adequacy" test for transborder data flows from Switzerland within the context of the Swiss Federal Data Protection Act (FADP).[1] Since 2017, the FDPIC had considered the U.S. as a nation that provided an adequate level of protection under certain circumstances, including, specifically, where companies comply with the Swiss-U.S. Privacy Shield regime. This framework provides a mechanism for U.S. companies to self-certify that they comply with Swiss law requirements when transferring personal data from Switzerland to the U.S.

In its annual review, the FDPIC concluded that the U.S. must be removed from the list of countries providing "an adequate level of protection under certain circumstances," with the agency also noting that it does not have the authority to invalidate the Swiss-U.S. Privacy Shield. The FDPIC assessment is subject to any future rulings by Swiss courts and as long as it is not revoked by the U.S., companies can continue to rely on the Swiss-U.S. Privacy Shield. Such companies are still required to grant special protection rights to individuals in Switzerland, but according to the FDPIC, these rights do not meet the requirements of adequate data protection as defined by FADP.

In determining its ruling, the FDPIC relied on the recent ruling from the Court of Justice of the European Union (CJEU) on July 16, 2020, which struck down the EU-U.S. Privacy Shield as a valid mechanism for transferring personal data from the European Economic Area (EEA) to the U.S. (*Schrems II*).[2] The EU-U.S. Privacy Shield was implemented in 2016 to replace the Safe Harbor framework and to date; over 5,200 companies have self-certified under the agreement. The CJEU's decision was based on the limitations on

[1] Federal Act of 19 June 1992 on Data Protection, SR 235.1.

[2] C-311/18 *Data Protection Commissioner v. Face-book Ireland Ltd and Maximilian Schrems*.

the protection of personal data under U.S. laws, and the disproportionate access and use of EEA personal data by U.S. authorities without effective remedies for EEA data subjects.

In its policy paper, the FDPIC acknowledged that although it is not bound by the CJEU decision, "Switzerland and the EU mutually recognize their data protection legislation as equivalent, and the FDPIC agrees with the [European Data Protection Board (EDPB)] criticisms regarding access of data by U.S. authorities, insofar as these can also be derived from Swiss data protection law." The FDPIC concluded that the lack of transparency in U.S. surveillance laws and lack of enforceable legal remedies for individuals in Switzerland with respect to access to personal data by U.S. authorities is "irreconcilable with" the data subject rights and data protection principles guaranteed by the FADP.[3]

With respect to the use of Standard Contractual Clauses (SCCs), the FDPIC also adopted the CJEU approach in *Schrems II*. In the FDPIC's view, such contractual safeguards "cannot prevent foreign authorities from accessing personal data if the public law of the importing country takes precedence and allows official access to the transferred personal data without sufficient transparency and legal protections of the persons concerned." The FDPIC recommends that each individual case of data transfers be reviewed and additional safeguards be implemented when using SCCs. These safeguards could include risk assessments and additional technical measures that effectively prevent authorities from accessing transferred personal data.

Key Takeaways

While the FDPIC does not have the authority to invalidate the Swiss-U.S. Privacy Shield, in light of the agency's policy paper, companies relying on the regime for data transfers from Switzerland to the U.S. should begin to consider alternative data transfer mechanisms. The EDPB and the European Commission are expected to provide further guidance on cross-border data transfers in light of *Schrems II*, which could have further implications for data transfers between the U.S. and Switzerland going forward.

Return to Table of Contents

[3] The FDPIC's policy paper can be accessed here.

Ninth Circuit Rules NSA's Metadata Collection Program Unlawful and Possibly Unconstitutional

In *United States v. Moalin,* the Ninth Circuit found the National Security Agency's (NSA) bulk phone metadata collection program violated the Foreign Intelligence Surveillance Act (FISA) and may have infringed on Fourth Amendment rights.

On September 2, 2020, the U.S. Court of Appeals for the Ninth Circuit found the NSA's telephony metadata collection program violated FISA and was constitutionally suspect, but ultimately concluded that its role in the prosecution of the defendants was too insignificant to overturn the convictions in the case.[4]

Background

The case involves the NSA's telephony metadata program — which was revealed by former NSA contractor Edward Snowden in 2013 — under which the NSA collected bulk telephone records from telecommunications providers. Those records included the time and duration of calls and the phone numbers involved, but not the voice content of the calls.

Following the exposure of the telephony metadata program, government officials made statements indicating that it played a role in an investigation into four Somali immigrants accused of conspiring with a foreign terrorist organization. At trial, the U.S. government principally relied on evidence obtained through a wiretap of defendant Moalin's phone.

On appeal, the defendants argued that the metadata collection violated the Fourth Amendment and the government failed to provide notice of the metadata collection or other surveillance under FISA.

Fourth Amendment Considerations

Writing for a unanimous three-judge panel, Judge Marsha Berzon stopped short of deciding whether the NSA metadata collection violated the Fourth Amendment. However, the court

[4] *United States v. Moalin*, No. 13-50572 (9th Cir. Sep. 2, 2020). A copy of the decision is available here.

rejected the government's reliance on the third-party doctrine established in *Smith v. Maryland*,[5] under which individuals have no reasonable expectation of privacy in information voluntarily conveyed to a telephone company. Instead, the court found the amount and detail of information collected, as well as the government's ability to analyze the data, had distinguished it from the pen registers in *Smith*.

According to the court's opinion, defendant Basaaly Moalin "likely had a reasonable expectation of privacy in his telephony metadata — at the very least, it is a close question." The court declined to resolve that question because it found suppression of the evidence to be unwarranted on the facts of the case. Based on its review of FISA applications, the court determined that the metadata collection program did not taint the evidence in the case.

FISA Considerations

FISA authorizes the government to apply to the FISA court for an order requiring production of tangible things for an investigation. At the relevant time, the law requires that the application state facts demonstrating that the tangible things sought are "relevant to an authorized investigation."

In *Moalin*, the government argued that all metadata is relevant because the program depended on collecting and reviewing large volumes of data — that is, only through bulk collection could the government identify the information relevant to its investigation. The court rejected this after-the-fact determination of relevance, finding that the metadata collection program violated FISA.

As a remedy for the FISA violation, the defendants sought to suppress the "fruits" of the unlawful collection, including the wiretap of Mr. Moalin's phone. The court, upon reviewing the classified record, determined that the metadata was not necessary to support probable cause for the wiretap and that the wiretap was not the fruit of the unlawful metadata collection. Therefore, the court found suppression of the wiretap evidence unwarranted.

Notice of Surveillance Activities

The defendants also challenged the government's failure to provide notice that it had collected Mr. Moalin's metadata.

The Ninth Circuit announced a test that "[a]t a minimum, … the Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from surveillance of that defendant conducted pursuant to the government's foreign intelligence authorities." According to the court, such notice is necessary for defendants to challenge surveillance under FISA.

The court declined to decide whether the government was required to provide notice to the defendants in this case. Instead, it found that any such failure did not prejudice the defendants because they found out about the metadata collection program through news reports in time to challenge the collection.

Key Takeaways

The decision comes long after the NSA metadata program ended, but demonstrates the increasing scrutiny that courts have applied to the executive branch's invocation of national security interests, particularly when significant privacy interests are at stake. The case also could shine a continued spotlight on European Commission concerns regarding adequacy of data privacy protection in the U.S., as recently articulated in the *Schrems II*[6] decision.

Return to Table of Contents

EDPB Issues Guidance Clarifying Classification of Joint Controllers in Light of Recent Case Law

On September 2, 2020, the EDPB released guidance defining the concepts of the "controller," "joint controller" and "processor" roles under the General Data Protection Regulation 2016/679 (GDPR).[7] The guidance provides clarification in identifying joint controllership, which is particularly welcome in light of recent case law involving confusion surrounding this issue from the CJEU, such as the *FashionID* case, which addressed this issue.[8] As an organization's role will affect its obligations under the GDPR, it will be important for those who are unclear to consult the Guidance to ensure that they are accurately classified.

Background

The concepts of "controller," "joint controller" and "processor" are central to the GDPR as they outline the scope of rights and obligations (and associated liability) of parties in relation to data processing. The EDPB's guidance is divided into two sections:

[5] 442 U.S. 735 (1979).

[6] The *Schrems II* decision is discussed in more detail in the July 2020 edition of our *Privacy & Cybersecurity Update*.

[7] The guidance is accessible here.

[8] More information about this case can be found in the the September 2019 issue of our *Privacy & Cybersecurity Update*.

the first section considers the definitions of "controller," "joint controller" and "processor", and the second section deals with the relationships between these roles. The guidance is significant because, while the roles of controller and processor have previously been the subject of guidance from the EDPB's predecessor, the Article 29 Working Party, guidance in relation to the role of joint controller had thus far been lacking.

Controller

Article 4(7) of the GDPR states that a controller is an entity that "determines the purposes and means of the processing of personal data," meaning the entity responsible for complying and demonstrating compliance with the overarching principles of the GDPR in relation to their data processing activities. The guidance states that:

- Identification of the controller is a question of fact. For each processing activity the controller is the body with the decision-making power over the processing, to be assessed on a case-by-case basis rather than any prior agreement between the parties.
- A controller need not have access to the data to be classified as a controller. An organization that outsources a processing activity but retains a determinative influence over the purpose and means of the processing will be the controller of the data, even in cases where it never accesses the data.
- A controller must decide on both the means and purposes — or the why and how — of the processing. In practice, a processor will often make decisions about the means of the processing. However, the guidance distinguishes between "essential means" and "non-essential means." "Essential means" pertain to central matters, such as what data should be processed, how long it should be processed for and who should have access to it. By contrast, "non-essential means" refer to the practical aspects of implementation, such as security measures or software choices. Therefore, the organization acting as a controller must determine both the purposes and essential means of processing, while non-essential means can be left to the processor.

Joint Controller

Joint controllership exists where two or more parties jointly determine the purpose and means of a specific processing activity. To assess whether a joint controllership has arisen, the guidance employs the same analysis used to determine the existence of a controller, focusing again on the factual, rather than formal, influence of the relevant parties. The predominant criterion for the existence of a joint controllership is the joint participation of two or more entities in the determination of the purposes and means of a processing activity. The guidance suggests that joint participation will typically arise through either a "common decision" where the parties make decisions about the processing together, or "converging decisions," where the parties make decisions about separate aspects of the processing, but not without the decision of both parties, such that the activities could be considered inextricably linked.

For example, assume Company A and Company B organize a promotional event for their co-branded product, pursuant to which they share data about their respective clients and collectively decide on invitees and follow-up marketing actions following the event. In this case, Company A and Company B are joint controllers as they jointly decide — through common decisions — on the purpose and essential means of the processing. However, the guidance stresses that even in cases where several actors are involved in the same processing operation, this does not necessarily mean that they are acting as joint controllers. The exchange of a data set between two parties where the processing purposes and means of processing are not jointly determined is an exchange of data between two separate controllers, rather than joint controllers. For example, if a group of companies uses a shared marketing list, whereby each group member enters the data of its own clients for its own purposes and does not have access to other group companies' data, each group company will be a separate controller.

Processor

The guidance states two essential preconditions for an organization to be considered a processor:

- it must be a separate entity from the controller (though it can belong to the same corporate group as the controller); and
- it processes data on the controller's behalf or for the benefit of the controller.

The processor must only process data on the documented instructions given in relation to each processing activity and will be considered a controller to the extent it exceeds these instructions and determines both the purposes and essential means of the processing (as opposed to the non-essential means). For example, Company A hires payroll provider Company B to provide payroll services. Company A decides the essential means of processing (*e.g.*, who to pay, what amounts, pay date). Company B decides on the payroll platform it uses to provide the services and the detailed security measures in place in relation

to the data, including access controls to the platform. These are non-essential means of processing which will not alter Company B's role as processor. However, if Company B were to decide on the essential means of processing (*e.g.*, who to pay, pay date), it would be considered a controller. Therefore, "non-essential means" are limited to the practicalities of implementation.

Inter-Relationships

Between Controllers and Processors

The guidance states that a controller must use processors that provide sufficient guarantees to implement appropriate technical and organizational measures. These guarantees often will require an exchange of the relevant documentation, such as the processor's privacy policy, records of processing and information security policy. The controller must then assess and document whether the guarantees offered by the processor are sufficient.

Any processing of personal data by a processor must be governed by a data processing agreement reflecting the mandatory requirements of Article 28(3) of the GDPR. For example, the guidance states that where a controller provides a general authorization for the processor's use of subprocessors, the parties could include an annex setting out the criteria for the processor to consider in the appointment of subprocessors.

Between Joint Controllers

Where a joint controllership arises, Article 26(1) of the GDPR states that the parties must set out their respective obligations by means of an "arrangement." The guidance states that, while there is no form or substance requirement for such arrangements, it is recommended that the arrangement be in writing and include, at a minimum, which party is responsible for answering data subject requests, while providing the prior information required under Articles 13 and 14 of the GDPR in the form of a privacy notice.

The allocation of responsibility between parties should take into account which party is best able to comply with those obligations. The parties should further document their internal assessment for accountability purposes. While most obligations can be allocated, the guidance makes clear that certain duties under the GDPR cannot be allocated between the joint controllers and instead requires compliance from both controllers (*e.g.*, the duty to maintain records of processing activities to the detail required by Article 30(1) of the GDPR).

Key Takeaways

While the guidance does not amount to a radical restatement of the controller and processor concepts, it helpfully lays out how these roles can be identified and what responsibilities will flow from the designations. The guidance also expands on joint controllership, providing some examples to illustrate what "common" and "converging" decisions might look like. In particular, organizations should ensure that:

- where they act as a controller, they determine the purposes and essential means of processing;
- where they act a joint controller, the decisions made together with the other controller are either common or converging decisions, and that the "arrangement" they enter into is in writing and allocates the responsibilities of each joint controller; and
- where they act as a processor, they only determine the non-essential means of processing, as controllership could arise should they determine the essential means of processing.

Return to Table of Contents

EDPB Issues Guidance on Targeting Social Media Users

On September 7, 2020, the EDPB released its guidelines on targeting social media users, clarifying the risks, roles and responsibilities that arise, given the presence of the GDPR.[9] The guidance is open for feedback until October 19, 2020.[10]

Background

Targeting services, which have developed over the past decade, make it possible for organizations to communicate specific messages, such as advertisements, to social media users based on defined parameters or criteria (*e.g.*, users' internet browsing history). As targeting techniques become more sophisticated, individuals' data protection rights and freedoms are subject to a number of risks. In light of these risks, the EDPB's guidance seeks to provide clarity on the roles and responsibilities of the social media provider, and the organizations targeting users via social media (targeters).

How Does Targeting Occur?

[9] The guidance is accessible here.

[10] Comments can be submitted here.

Targeting occurs when a targeter defines criteria (*e.g.*, age range, relationship status) and a social media provider identifies a desired audience among its user base. Social media users may be targeted on the basis of provided, observed or inferred data:

- **Provided data.** Individuals actively provide their information to a social media provider or targeter, for example, via creating or updating a social media profile, or through setting up an account with an online shopping targeter.
- **Observed data.** An individual is targeted on the basis of their online activity. For example, this could either be on the social media platform itself, on third-party applications or where a third-party website has a social media plug-in.
- **Inferred data.** A social media provider or targeter uses provided or observed data in order to infer something about the individual. For example, a social media provider may infer that an individual may be interested in a particular product, based on their web browsing behavior and/or social media connections.

The guidance analyzes controllership for each of the above scenarios and concludes that, in most cases, the social media provider and targeter will be joint controllers (*i.e.*, two or more controllers that jointly determine why and how to process personal data). Accordingly, the social media provider and the targeter both exert control over the means of the processing activity and converge around the joint purpose of displaying a specific advertisement to a targeted individual.[11]

What is the Appropriate Legal Basis for Targeting Activities?

The appropriate legal basis for targeting will depend on the how the targeting will occur:

- **Provided data.** The guidance notes that there are two legal bases that could justify targeting: (i) consent or (ii) legitimate interests. However, the guidance emphasizes that legitimate interests would not be an appropriate legal basis for certain processing activities, such as intrusive profiling, which would require collection of users' consent.
- **Observed data.** Such data often will be collected via cookies or similar technologies, to which the ePrivacy Directive and corresponding national legislation will apply. The ePrivacy Directive requires consent to place cookies on an individual's device. Therefore, in practice, consent often will be the most appropriate legal basis for targeting on the basis of observed data.
- **Inferred data.** The guidance notes that the use of inferred data has the potential to produce legal or similarly significant effects on an individual, for example, where an individual is inferred to be impulsive and financially vulnerable from their internet search history, and is therefore targeted by pay-day loan companies. In such circumstances, the guidance clarifies that the targeting only can be justified on the basis of explicit consent, the necessity of the decision-making, or authorization under EU or member state law, as provided for in Article 22 of the GDPR. The guidance notes that profiling can create special categories of data by inference from data that is not itself a special category of personal data (*e.g.*, inferring religious beliefs when an individual regularly checks in as being at a mosque on social media). If this occurs and regardless of whether the inference is correct, the data must be processed on the basis that it is a special category of personal data and also will need to meet one of the conditions set out under Article 9 of the GDPR to be lawful.

What are the Obligations for Controllers Engaged in Targeting?

The following obligations are imposed upon controllers where they are engaged in targeting:

- **Transparency.** Data subjects should be informed if a profile will be built based on their online behavior on the social media platform or on the targeter's website. The word "advertising" alone is insufficient to inform users that their behavior is being monitored for targeted advertising purposes. The transparency information should be available through a "Why am I seeing this ad?" link and in the website's privacy notice. Although joint controllers will both be subject to this duty to inform, it can be mutually agreed upon that just one will undertake the provision of handling this initial information.
- **Data subject rights.** Data controllers must enable users to easily and fully exercise their individual rights. The individual is entitled to learn the targeter's identity and controllers must allow access to information about the targeting (*e.g.*, what targeting criteria was used). Joint controllers are free to decide who is responsible for responding to data subject requests, but they cannot exclude the possibility of the data subject exercising their rights against each of them.
- **Data Protection Impact Assessments (DPIAs).** Controllers are required to assess whether a DPIA should be conducted and, if one is necessary, both joint controllers are responsible for complying with this obligation. Any joint arrangement between the controllers must address this requirement and ensure that the exchange of knowledge required to complete the DPIA

[11] For more information on how to identify joint controllership, see our above article in this mailing on this topic.

takes place. This is because one joint controller may be in a better position than the other to assess the risks posed by certain processing operations.

- **Joint Controller Arrangements.** Pursuant to Article 26(1) of the GDPR, joint controllers must set out their respective responsibilities by way of an arrangement that encompasses all processing operations for which they are responsible. The guidance emphasizes the need for joint controllers to clarify the stages of processing for which each joint controller is responsible. For example, in the *FashionID* case, the website operator was considered a controller for the collection and transmission of the personal data via the social media plug-in on its website, but the social media provider was the controller for any subsequent processing.

Key Takeaways

- **Social media providers and targeters are likely to be joint controllers where they perform targeting activities.** Following the *FashionID* case, this is not a new concept. However, the guidance provides further support for the proposition that joint controllership relationships are becoming more common.
- **Targeting is not always automated decision-making under Article 22 of the GDPR.** The guidance states that targeted advertising will often not produce "legal effects concerning him or her or similarly significantly affects him or her," and therefore will not always constitute automated decision-making. However, the intrusiveness of the profiling and the individual's vulnerabilities can lead to automated decision-making (*e.g.*, targeting financially vulnerable persons interested in online betting with advertisements for pay-day loan services). Controllers should therefore be mindful that where targeting allows for automated decision-making, data subjects' explicit consent will be required.
- **Article 9 of the GDPR's additional condition for lawful processing is needed where controllers infer special categories of personal data.** To the extent that the controller infers a special category of personal data in relation to an individual, they will need to ensure that they have established the appropriate condition under Article 9 of the GDPR in addition to the appropriate legal basis under Article 6 of the GDPR, even if the inference is incorrect. The guidance does not comment on how the processing of incorrectly inferred special categories of personal data can be consistent with the data accuracy principle of the GDPR.

Return to Table of Contents

BIPA Class Action Suit Against Topgolf Will Go Forward

A district court judge denied golf entertainment company Topgolf's motion to dismiss a suit brought by former employees alleging that the company violated the Illinois Biometric Privacy Act (BIPA).

Background

Former Topgolf employees Thomas Burlinski and Matthew Miller are alleging that the company violated the BIPA through its use of a biometric fingerprint-scan system to track hourly employees' time. The plaintiffs claim that Topgolf violated the BIPA by (1) failing to maintain a public retention and destruction schedule before collecting biometric data, (2) failing to obtain written consent before collecting biometric data and (3) disclosing such data to a third-party timekeeping vendor without obtaining employees' prior written consent. The plaintiffs seek to represent a class of more than 40 employees who were required to use the fingerprint system. Mr. Burlinski and Mr. Miller filed suit in state court in September 2019, but Topgolf removed the case to federal court and filed a motion to dismiss in October 2019, with the plaintiffs then filing a motion to remand the case to state court.

On September 3, 2020, U.S. District Judge Edmond E. Chang determined that the former employee's BIPA suit against Topgolf could proceed, denying the company's motion to dismiss and granting the plaintiffs' motion to remand in part.[12]

Topgolf's Motion to Dismiss

Topgolf argued that the Illinois Workers' Compensation Act preempts the plaintiff's BIPA claims. However, Chang held that the BIPA is not preempted by the workers' compensation act by pointing to nine Illinois state court decisions as persuasive precedent. The judge also agreed with the plaintiffs' argument that the recovery scheme under the Illinois Workers' Compensation Act does not include purely statutory violations related to biometric privacy. From a common sense standpoint, Chang stated that biometric privacy violations are a "bad fit" for the types of injuries contemplated by the Workers' Compensation Act. Chang further stated that Topgolf failed to explain why Illinois lawmakers would have provided for a cause of action under BIPA in the employment context if the Workers' Compensation Act was intended to serve as the exclusive remedy for accidental workplace injuries in this context.

[12] *Burlinski v. Top Golf USA Inc.*, No. 19-cv-06700, 2020 WL 5253150 (N.D. Ill. Sept. 3, 2020).

Topgolf also had argued that the plaintiff's claims are time-barred. However, the court determined that the former employees' claims were not barred by either the one-year statute of limitations for privacy claims or the two-year statute of limitations for personal injury and statutory penalty claims. Chang noted that while the BIPA does not specify a limitations period, the one-year limitations period for privacy claims is limited to slander, libel or publication of matter violating the right of privacy, none of which are at issue in this case. The court also rejected Topgolf's contention that the two-year limitations period applied given that the company failed to explain how the BIPA violation constitutes an injury to person. Judge Chang determined that the catch-all five-year statute of limitation applies and that the claims at issue were brought within the appropriate time period.

Plaintiffs' Motion to Remand

Chang remanded the claim that Topgolf failed to maintain a retention schedule to state court based on the Seventh Circuit's ruling in *Bryant v. Compass Group U.S.A. Inc.*,[13] which determined that the plaintiffs do not have standing to pursue this claim in federal court.

Return to Table of Contents

Trump Administration Releases Memorandum on Space Policy Directive Regarding Cybersecurity Principles for Space Systems

On September 4, 2020, the Trump administration released its fifth Memorandum on Space Policy Directive regarding cybersecurity principles for space systems. The memorandum, which sets forth policies and principles regarding best cybersecurity practices for commercial and government space systems, is the first of the space policy directives to address cybersecurity.

Background

The "Memorandum on Space Policy Directive-5 – Cybersecurity Principles For Space Systems" (SPD-5) is the fifth in a series of space policy directives (SPDs) signed by President Donald Trump. The previous four, which include SPD-4, signed February 2019; SPD-3, signed June 18, 2018; SPD-2, May 24, 2018; and SPD-1, signed December 11, 2017, addressed various administration priorities in space (*e.g.*, establishing a U.S. Space Force, setting forth standards for space travel management, streamlining regulations on the commercial use of space and calling for human expansion across the solar system). SPD-5 is the first of the SPDs to directly address cybersecurity practices with respect to space systems.

SPD-5

SPD-5 directly addresses "space systems," which are defined as a combination of systems that include ground systems, sensor networks and one or more space vehicles that provide space-based systems. The definition of "space systems" is broad enough and intended to capture a wide range of technologies that could be found in space (*e.g.*, GPS satellites and weather satellites) and is not intended to refer to spacecrafts. The SPD-5 directly addresses how companies and the government can avoid malicious cyber activities that could deny, degrade or destroy these systems by establishing clear cybersecurity principles that take a "cybersecurity-by-design" approach. Specifically, the SPD-5 recommends, among other things, that (1) space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering; (2) space operators and owners should develop and implement cybersecurity plans to protect against unauthorized access to space systems, reduce vulnerabilities of command and control systems, and protect against communications jamming and spoofing by unauthorized third parties; (3) space system owners and operators consider appropriate risks specific to their space systems; and (4) implement physical protection measures to reduce vulnerabilities of a space system's command and receiver systems.

SPD-5 also states that the U.S. government will direct agencies to collaborate and work with the commercial space industry and other nongovernment space operators, consistent with applicable laws, to further define best practices, establish cybersecurity-informed norms and promote improved cybersecurity behaviors.

Key Takeaways

SPD-5 is an important first step in addressing the vulnerabilities presented by a growing commercial space economy. Companies that are considering implementing space systems or whose businesses depend on technology from space systems should ensure that they are in compliance with SPD-5 or, at the very least, consider its principles and guidelines when making decisions regarding cybersecurity.

Return to Table of Contents

[13] *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 624-26 (7th Cir. 2020)

Contacts

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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