Skadden

Privacy & Cybersecurity Update

1 European Commission's Proposed Digital Services Act Could Enhance Regulatory Reform in EU

4 National Institute of Standards and Technology Releases Draft Guidance on Internet of Things Device Cybersecurity

5 FTC Reaches Settlement With Flo Health, Inc. Regarding Its Misleading Privacy and Data Sharing Practices

6 FTC Settles With Everalbum Over Deceptive Practices Regarding Facial Recognition Technology and Data Deletion Practices

7 Data Protection and Digital Trade Post-Brexit

European Commission's Proposed Digital Services Act Could Enhance Regulatory Reform in EU

The European Commission (EC) has proposed the Digital Services Act (DSA), a significant update to the EU's regulatory framework that would enhance "notice and action" requirements for illegal content, require certain online companies to release moderation transparency reports, create new obligations related to online advertising, and require certain companies to evaluate and address the systems risks posed by their services.

Introduction

The pace at which the digital economy has grown and digital service providers have developed has not been matched by equivalent regulatory changes within Europe. To address the risks and challenges of digital trade, regulatory reforms have been proposed by the EC, central of which is the proposed DSA.[1] With a focus on protecting consumers, enhancing transparency and broadening the accountability of online platforms, along with the potential for fines that exceed those under the General Data Protection Regulation (GDPR), the DSA appears to be a significant update to the regulation of the digital economy in the EU by enhancing "notice and action" mechanisms for illegal content, requiring organizations to release content moderation transparency reports, imposing obligations related to online advertising, and identifying and addressing the systemic risks associated with the use of certain online platforms. However, the DSA will not take effect in the near future as the EC's proposal will now be debated by the European Parliament and member states, who can be expected to make amendments to the proposal before it becomes EU law.

Scope of Application and Governance

Much like the GDPR, the DSA will have extraterritorial effect, applying to organizations established outside of the EU if the recipients of their services are established or have their residence in the EU. However, as with the GDPR, there may be practical and procedural hurdles to actually enforcing the DSA against organizations with no physical presence in the EU.

[1] See here for the full text of the DSA.

Obligations under the DSA are tailored to the role, size and impact of the relevant organization. The first-tier of obligations applies to all providers of intermediary services, with three further tiers providing separate and additional — and incrementally more onerous — obligations for providers of hosting services, online platforms and so-called "very large platforms."

To monitor compliance and facilitate enforcement of the DSA, member states will need to designate an independent authority to take the new role of "digital services coordinator" for that member state. Each digital services coordinator shall together comprise a new European Board for Digital Services (EBDS), which, in conjunction with the EC, will be responsible for providing guidance on the DSA and ensuring it is consistently applied across the EU.

The following discusses each tier as mentioned above:

Tier 1

The first tier of obligations applies to all providers of "intermediary services," such as all organizations that act as a conduit for, or provide temporary or permanent storage of, information provided by third parties. These organizations will include internet access providers, content distribution networks, cloud service providers and social media platforms.

As a first step towards enhancing transparency, the DSA will require intermediary service providers to publish annual transparency reports detailing the content moderation they have carried out. This may, for example, include the number of orders an organization has received from member states to act against illegal content or the internal content moderation it has carried out.

This requirement is accompanied by governance obligations, namely to appoint and make public a point of contact with whom the EC and the newly formed EBDS may interact for matters related to the DSA. For organizations that do not have an establishment in the EU, they must appoint an EU legal representative.

Tier 2

Tier 2 obligations apply to all intermediary services that also provide hosting services that enable the storage of information. These organizations will include file-sharing services, cloud-sharing services and social media platforms.

A key development applicable to all hosting service providers is the DSA's "notice and action" mechanism. To counter illegal content online, hosting service providers will be required to implement a user-friendly mechanism to allow users to flag illegal content, and the organization must act on that notification without undue delay. The DSA's obligation goes further than the EU's existing eCommerce Directive, which only states that hosting services must act expeditiously to remove access to illegal content once given notice.

This requirement to offer a user-friendly complaint procedure can be expected to expand the number of notifications hosting service providers receive and therefore increase the number of complaints that hosting service providers must act upon.

While the DSA does expand on the obligations required under the eCommerce Directive, it does not impose upon intermediary services providers a general obligation to monitor content on their platform.

Tier 3

Tier 3 obligations apply to all online platforms with the exception of micro or small enterprises. Such online platforms that fall under the tier include social networks, content-sharing websites, app stores, online marketplaces, and online travel and accommodation websites.

With respect to illegal content, online platforms will be required to suspend users who frequently provide illegal content and must notify law enforcement where criminal offences are suspected. Additionally, online platforms must ensure that "trusted flaggers" (individuals or entities that have expertise for the purposes of detecting illegal content) are able to notify online platforms of illegal content, and deal with such notifications as a priority.

To enhance consumer protection, online platforms must provide the recipients of their services with an adequate means of redress through an internal complaint-handling system to allow for complaints against decisions to remove content or to terminate an individual's account. For any disputes not settled through this internal complaint procedure, online platforms must permit individuals to bring their claim to an out-of-court dispute settlement system that is certified by the relevant digital services coordinator.

Online platforms also are subject to more onerous transparency reporting obligations. In addition to their Tier 1 requirements, online platforms must disclose in their transparency reports the number of disputes submitted to an out-of-court dispute settlement, the number of suspensions they have been required to make, and details of their use, if any, of automated content moderation.

These obligations are accompanied by enhanced transparency obligations with respect to online advertising. Online platforms will be required to ensure that service recipients are able to identify, for

each specific advertisement displayed to them, that the information is an advertisement, on whose behalf the advertisement is displayed, and the criteria used to decide to show that particular advertisement to the specific recipient. Increased transparency for users in relation to online ads is intended to address concerns about the risks of manipulation, disinformation and political polarization that may be triggered by targeted advertising.

Tier 4

The final tier of obligations will apply to online platforms who, on average, provide their services to more than 45 million EU users per month, so-called "very large online platforms" (VLOPs). This set of organizations would likely include companies such as Facebook, Twitter, Google and Amazon.

In addition to the Tier 1-3 obligations, VLOPs will be required to carry out and publish annual risk assessments analyzing any systemic risks arising from the use of their services, and then implement effective measures to mitigate the risks they have identified. While the full scope of systemic risks to be considered are not prescribed, the DSA requires that VLOPs assess three types of risk in depth: (1) risks associated through the dissemination of illegal content on their service; (2) the impact of the service on the exercise of fundamental rights, such as the freedom of expression, the right to private life and the right to nondiscrimination; and (3) the risks arising from intentional manipulation of the platform's service and its impact on health, civic discourse, electoral processes and public security.

Very large online platforms are used in a way that strongly influences online safety, the shaping of public opinion and discourse, and online trade. The way VLOPs design their services is generally optimized to benefit their often advertising-driven business models, which can cause societal concerns. In the absence of effective regulation and enforcement, VLOPs can set the rules of the game without effectively identifying and mitigating the risks and the societal and economic harm they can cause. Should the regulation pass, VLOPs should therefore assess the systemic risks stemming from the functioning and use of their service, as well as potential misuses by the service's recipients, and take appropriate mitigating measures.

With respect to transparency, VLOPs will be required to (1) disclose the criteria by which their recommender systems operate (*i.e.*, the systems that are used to give content prominence on their platforms), and how users can modify that criteria; and (2) maintain "ad repositories" which show the advertisements that have been shown in certain periods and which groups were targeted. Further, Tier 3 transparency reports must be biannual.

In a further step to heighten the accountability of VLOPs, the companies also will be subject to an annual independent audit to assess compliance with their obligations under the DSA. This resulting audit report must be published publicly. Compliance with the DSA also must be monitored internally and VLOPs will be required to appoint a compliance officer for this role.

Defining Illegal Content

The DSA does not go so far as to define "illegal content." Instead, it defers to the laws of the applicable member state, which puts the organization in the sometimes difficult position of determining which laws apply to them and whether a particular piece of content violates that law. Given that service providers must inform affected parties of their ability to contest a decision to take down alleged illegal content, and available recourse must always include judicial redress, organizations may find themselves involved in frequent disputes regarding the takedown of alleged illegal content if the DSA is enacted.

Liability

Much like the GDPR, to achieve far-reaching regulatory reform, the DSA will need teeth, which will come in the form of fines that surpass those under the GDPR.

For all intermediary services aside from VLOPs, penalties for infringements of the DSA will be prescribed by member state law and can be in amounts up to 6% of the annual income or turnover of the service provider. For VLOPs, fines are imposed by the EC and are capped at 6% of the VLOP's total turnover for the preceding financial year.

Similar to the way that significant fines under GPDR forced a shift in companies' behavior toward data protection, the higher level of fines under the DSA suggests that the potential new regulation may bring about a comparably significant change in approach.

Key Takeaways

- Once implemented, the DSA has the potential to bring about a significant transformation to the digital services landscape. In recognition of the impact that intermediary service providers and, in particular, VLOPs have on society and individuals, the proposal advances robust standards of accountability and transparency to safeguard users.
- Although the DSA is not yet in effect and is subject to additional debate and revision before it becomes EU law, organizations should pay close attention to developments in this field given the far-reaching reform underway.

- While the DSA will not have direct effect in the U.K. now that the nation has left the EU post-Brexit, the extraterritorial effect of the DSA means U.K.-based intermediary service providers should expect the DSA to impact their operations. Separately, the recently signed Trade and Cooperation Agreement between the U.K. and EU signed on December 30, 2020, allows both parties to develop new regulations addressing digital trade and therefore the U.K. is free to forge its own regulatory path with respect to digital services.

Return to Table of Contents

National Institute of Standards and Technology Releases Draft Guidance on Internet of Things Device Cybersecurity

The National Institute of Standards and Technology (NIST) has released a draft set of security guidelines for internet of things (IoT) devices, potentially establishing a benchmark of "reasonableness" for these devices.

On December 4, 2020, the IoT Cybersecurity Improvement Act of 2020 was signed into law by then-President Donald Trump. The act obligates the federal government to follow certain cybersecurity standards when using and managing IoT devices, and requires NIST to develop those standards, as well as to update them over time. NIST has now issued its first drafts of these standards. Although expressly applicable only to the federal government, NIST's guidance may develop into an overall benchmark for reasonable cybersecurity practices in the private sector as well.

NIST's Guidance

On December 15, 2020, NIST released four related publications describing its proposed guidance under the act. Together, the four documents — NIST Special Publication 800-213 (the SP) and NIST Interagency Reports 8259B, 8259C and 8259D (the IRs) — form a cohesive strategy to align the government and IoT device designers and manufacturers with respect to cybersecurity for IoT devices used by federal agencies.[2]

The SP provides overall guidance to federal agencies, extending NIST's risk-based cybersecurity approach to include integration of IoT devices into federal information systems and infrastructure. Specifically, the SP provides guidance on considering system security regarding devices and identifies the standards a federal agency to expect from an IoT device and its manufacturer.

The IRs provide overall guidance for IoT device manufacturers, explaining how manufacturers can implement the system security requirements outlined in the SP. Two documents that were previously published in this series — NISTIR 8259 and NISTIR 8259A — summarize foundational activities to help manufacturers meet their customers' cybersecurity needs. The additional IRs extend the landscape of the previous publications, providing guidance on nontechnical processes, such as documenting updates and informing customers how to implement them. In addition, the IRs provide further detail with regard to specific market sectors and explain how the guidelines were developed.

NIST is accepting public comments to the SP and IRs until February 12, 2021.

Potential Application in the Private Sector

Although the SP and IRs explicitly address guidance for the federal government, the question of appropriate cybersecurity standards for IoT devices applies to the private sector as well. The answer to that question could be critical in helping organizations to establish their own internal procedures, meet insurance requirements and fend off claims from affected data subjects if there is a security breach.

In 2014, NIST released its first version of the Framework for Improving Critical Infrastructure Cybersecurity. Over time, that document became a *de facto* industry standard for evaluating an organization's cybersecurity standards and practices. Unlike that prior framework, NIST's guidance for IoT security was not necessarily developed with the goal of providing general guidance to the private sector, but it is not difficult to imagine courts and others looking to these publications as an appropriate set of standards for the IoT industry overall. Deviations from NIST's guidance could potentially be cited as evidence that an organization did not take the appropriate, reasonable steps to address IoT security challenges.

In addition, given the purchasing power of the federal government, one would expect the IoT device industry to design its products to meet the NIST's guidance, which also will likely translate, to some extent, into the products offered in the private sector.

[2] The SP and IRs are available here.

Key Takeaways

NIST's guidance for IoT cybersecurity will likely have a significant impact on the IoT industry. Companies that use IoT devices in their organizations should evaluate their own IoT policies against NIST's guidance, both for the own internal purposes and to ward off potential claims by data subjects in the event of a data breach.

Return to Table of Contents

FTC Reaches Settlement With Flo Health, Inc. Regarding Its Misleading Privacy and Data Sharing Practices

The Federal Trade Commission (FTC) has settled with Flo Health, Inc., a women's health and fertility tracking app with over 100 million users, over allegations the company shared sensitive health data with third parties in violation of the company's privacy policies and stated privacy practices.

On January 13, 2021, the FTC announced that it settled with Flo Health, Inc. over allegations that it misled users about the disclosure of their sensitive health information. Under the proposed settlement, Flo Health would be prohibited from, among other things, misrepresenting the purposes and nature of its disclosure of personal information to third parties and misrepresenting its compliance with privacy, security or compliance programs. The proposed settlement also would impose notification and deletion requirements on Flo Health.

Background and FTC Complaint

Flo Health is a mobile application that uses artificial intelligence to allow women to track periods, create ovulation calendars and use pregnancy guides. The application, which has over 100 million users, encouraged users to provide sensitive information regarding their reproductive health.

According to the FTC's original complaint, the company's privacy policy between August 2017 and February 2019 stated, among other things, that information shared with third parties "excluded information regarding [users] marked cycles, pregnancy, symptoms, notes and other information that is entered by [the user] and that [the user] [does] not elect to share." The complaint also alleged that the company's privacy policies listed specific third parties with which it stated it would only share nonidentifiable information (and in certain instances, personal data identifiers).

However, the FTC alleged that, in violation of these policies, the company disclosed health information to various third parties between 2016 and 2018. According to the complaint, these third parties were then permitted to use the information for a variety of purposes, including for their own internal purposes in certain instances. In many cases, the company's disclosure of the sensitive health information to these third parties violated the third parties' terms of service, which often prohibited the sharing of such information, though at least some of the third parties stated they were unaware of the company's disclosures.

The complaint also alleged that the company misled its users in stating that it was compliant with the EU-U.S. Privacy Shield (EU Privacy Shield) and the Swiss-U.S. Privacy Shield Framework (Swiss Privacy Shield). Although the EU Privacy Shield and Swiss Privacy Shield have since been invalidated, both frameworks required companies to comply with certain principles regarding the transfer of personal information from the EU and Switzerland to the U.S. through a self-certification process with the U.S. Department of Commerce and in compliance with European and Swiss data protection law. The complaint alleged that Flo Health failed to provide the users with adequate notice of the disclosures of their health information and the choice to opt out of the disclosures as required under both frameworks.

The FTC also alleged that Flo Health's practices deceived consumers in violation of the prohibition on unfair or deceptive acts and practices under Section 5(a) of the Federal Trade Commission Act.

FTC Consent Order

The proposed terms of the FTC's consent order would prohibit Flo Health from misrepresenting:

- the purposes for which it or the entities to whom it discloses data collect, maintain, use or disclose the data;
- the degree of control its users have over the company's data uses;
- the company's compliance with any privacy, security or compliance program; and
- how the company collects, maintains, uses, discloses, deletes or protects users' personal information.

In addition, Flo Health also would be required to notify affected users about the unauthorized disclosure of their health information and to obtain express consent from its users before sharing health information with any third party. Flo Health also would be required to instruct any third party that received users' health information to destroy such data within 30 days after the order is filed.

The order now awaits 30 days of public comment following its publication in the Federal Register before it is finalized by the FTC. The FTC also has issued guidance to consumers related to health applications, including information on how to choose and use health applications in a way that reduces privacy risks.

Key Takeaways

The proposed order emphasizes the importance of companies' compliance with their privacy policies and statements they make regarding privacy matters. Further, the proposed order demonstrates that even though the EU Privacy Shield and the Swiss Privacy Shield have been invalidated, the FTC will still hold companies accountable for the promises that they made by certifying to it.

Return to Table of Contents

FTC Settles With Everalbum Over Deceptive Practices Regarding Facial Recognition Technology and Data Deletion Practices

The FTC has settled with California-based photo application company Everalbum, Inc. over allegations that the company misled its users regarding its facial recognition technology and data retention practices.

On January 11, 2021, the FTC announced that Everalbum, Inc. settled with the agency over allegations that the company deceived its users about the its use of facial recognition technology and improper retention of users' photos and videos after they had deactivated their accounts. Under the proposed settlement, the company would be required to delete certain models and algorithms, and obtain affirmative consent from users before collecting data for facial recognition technology purposes, highlighting the FTC's focus on companies' practices regarding facial recognition technology.

Background and FTC Complaint

Everalbum was the operator of since-shutdown service Ever, a photo storage and organization application that allowed consumers to upload photos and videos from various sources to cloud servers, and included automated features where users could organize photos and videos into albums by location and date. According to the FTC's initial complaint in February 2017, Everalbum launched a "friends" feature that used facial recognition technology to group users' photos by the faces of the people who appear in those photos. Although Everalbum implied on its website that it would not use facial recognition technology unless the feature was turned on, the complaint alleged that the technology was automatically active for most users and could not be disabled for a certain period of time, unless the user was in certain jurisdictions (Illinois, Texas, Washington state or the EU).

The complaint also alleged that, between 2017 and 2018, Everalbum combined millions of facial images it extracted from Ever users' photos with facial images that the company obtained from publicly available datasets in order to create new datasets to develop the company's facial recognition technology. The technology was used both for Ever's "friends" feature and also to build face recognition services offered by its enterprise brand, Paravision, to customers for various purposes, including security, access control and facilitating payments (according to the complaint, the company did not provide the customers direct access to Ever user data).

The complaint also alleged that Everalbum did not delete deactivated users' photos and videos from 2017 to 2019, in violation of its own public privacy policies.

As such, the FTC alleged that Everalbum's practices deceived consumers in violation of the prohibition on unfair or deceptive acts and practices under Section 5(a) of the Federal Trade Commission Act.

FTC Consent Order

The proposed terms of the FTC's consent order would require Everalbum to:

- delete all photos and videos that it collected from users who requested to deactivate their account on or before the issuance date of the order;
- delete all data derived from images of individuals' faces where users did not affirmatively consent to the use of facial recognition technology; and
- delete all models or algorithms developed by the company using any biometric information that the company collected from its Ever users.

The proposed order also would require Everalbum to clearly and conspicuously state the details of the collection, use, disclosure, maintenance or deletion of personal information, including face

embeddings, created with the use of facial recognition technology. Further, if the company markets software to consumers for personal use, it would be required to obtain express consent before using biometric information to create face embeddings or develop facial recognition technology.

In a statement made on January 8, 2021, FTC Commissioner Rohit Chopra noted that the proposed order is an "important course correction" from past data protection law violators who have been permitted to retain algorithms and technologies that derive value from "ill-gotten" data. Mr. Chopra also noted that while the proposed order does not require Everalbum to pay a penalty, the FTC "needs to take further steps to trigger penalties, damages, and other relief for facial recognition and data protection abuses."

The order now awaits 30 days of public comment following its publication in the Federal Register on January 25, 2021, before it is finalized by the FTC.

Key Takeaways

The proposed order is notable as it highlights the importance for companies to not only properly document their data collection and data retention practices in publicly facing policies and disclosures, but also ensure such policies align with how their business is conducted. The failure to do so may result not just in violations of state or federal privacy laws, but also risk penalties from the FTC.

Return to Table of Contents

Data Protection and Digital Trade Post-Brexit

The EU-U.K. Trade and Cooperation Agreement (TCA) addresses many of the questions left open regarding the post-Brexit relationship of the U.K. and EU with respect to data protection and digital trade.

Introduction

The U.K.'s withdrawal from the EU has raised much uncertainty regarding the future of data protection and digital trade between the two regions. While the U.K.'s incorporation of the GDPR into domestic law in January 2021 eased some uncertainty, there remain unanswered questions, particularly involving the status of data transfers from the European Economic Area (EEA) to the U.K. Given the importance of digital trade to the economic future of both the EU and the U.K., it was crucial that the TCA, signed on December 30, 2020, facilitated frictionless digital trade post-Brexit. That the TCA reaches a pro-business position on data protection and digital trade should be welcomed by organizations navigating the new relationship between the U.K. and EU in these important areas.

Data Protection: Certainty, for Now

The TCA provides a temporary solution to the issue of data transfers from the EEA to the U.K. Absent the agreement, beginning January 1, 2021, the U.K. would have been considered a third country for the purposes of data transfers from the EEA. Additionally, all organizations would have therefore been required to implement a valid data transfer mechanism to legitimize such transfers under the GDPR, such as the EC's Standard Contractual Clauses. Organizations also would have had to undertake Transfer Impact Assessments to determine whether the U.K. provides "essentially equivalent" protection of personal data to that which is guaranteed under EU law and, if not, would have had to implement supplementary technical, contractual and/or organizational measures to safeguard their data transfers. Such obligations can be onerous, even for the most well-resourced businesses.

Organizations can therefore be reassured that the TCA provides a "specified period" in which transfers of personal data transfers from the EEA to the U.K. will not be considered transfers to a third country. This specified period will continue until the earlier of (1) a maximum of six months from the date the TCA enters into force or (2) the date on which the EC adopts an adequacy decision regarding whether the U.K. maintains an adequate level of data protection. This arrangement is further contingent on the U.K. not changing its data protection framework, unless otherwise agreed to by the EU.

While this specified period is welcome news for many organizations, they must be prepared for the EC's adequacy decision. The six-month period tentatively suggests that an adequacy decision can be expected within this timeframe, however, the timing of the decision ultimately will be swayed by political factors. Although the U.K. should, absent any significant regulatory change, be in a strong position to be deemed adequate, the future relationship between the EU and U.K. is a politically charged area that is difficult to predict with confidence. Organizations should therefore carefully consider their data flows over the coming months in preparation for the EC's eventual decision or the expiration of the specified period.

Data transfers from the U.K. to the EEA are more straightforward. While the TCA does not address such transfers, Schedule 21 of the U.K.'s Data Protection Act 2018 recognizes the EEA as adequate unless and until the U.K. performs an adequacy assessment. Data transfers from the U.K. to the EEA can therefore continue without further restrictions unless a decision to the contrary is reached, with the U.K. government indicating only that this is "under review."

Looking to the future of the U.K. and the EU's future relationship with respect to data protection, the TCA requires collaboration on data protection matters through dialogue, the exchange of expertise, and cooperation on data protection-related enforcement. Therefore, while the U.K. Information Commissioner's Office (ICO) will no longer have voting rights on the European Data Protection Board (EDPB), the TCA opens the door for a deeper relationship among the ICO, the EDPB and any EEA supervisory authorities.

Digital Trade: A Positive Result for Business

As a testament to the importance of digital trade, the TCA contains an entire chapter dedicated to the U.K. and EU's relationship with respect to trade conducted via electronic means.

The TCA prohibits data localization, meaning that neither the EU nor the U.K. can require or prohibit the storage or processing of data in a particular jurisdiction, subject to limited exceptions (*e.g.*, on the grounds of security interests). Many organizations had been concerned that various jurisdictions would require data to be stored locally, so the rejection of this burdensome practice should be good news for them.

A commitment to maintaining the status quo with respect to digital trade is also evidenced by (1) a prohibition on customs duties on electronic transmissions; (2) a requirement that services can be provided electronically by default (*i.e.*, a prohibition on prior authorization); and (3) a requirement to recognize contracts concluded electronically, such as via electronic signatures.

Unimpeded digital trade also relies on commitments of the parties in the regulatory sphere. The TCA requires that the EU and U.K. continue to prohibit unsolicited direct marketing communications (*i.e.*, marketing campaigns that users have not opted in to receive) and adopt or maintain measures to protect consumers engaging in digital transactions. These requirements will mean that while the U.K. can develop its own approach to the regulation of digital trade, existing U.K. laws providing for a minimum level of consumer protection must be maintained.

The chapter on digital trade also imposes an obligation on the U.K. and EU to cooperate on the regulation of digital trade (including consumer protection) and the development of emerging technologies. While the forum for the discussion of such matters is unclear, much like with data protection, the TCA creates the potential for cross-fertilization of ideas and integration between the U.K. and EU regulatory bodies in the years to come.

Key Takeaways

- Data transfers from the EEA to the U.K. can continue as before until June 30, 2021, at the latest. During this period, organizations should both pay close attention to any decision of the EC on the U.K.'s adequacy and carefully consider their data flows, in preparation for either the U.K. to not be found adequate or the expiry of the specified period.
- Organizations should be aware that the TCA does not change their obligations to (1) appoint a representative in the EU or U.K., if they do not have a company established in either jurisdiction; and (2) update their privacy notices to reflect the reality of current data transfers.
- With respect to digital trade, the message is business as usual. Therefore, what will shape the future of digital trade between the EU and U.K. are their respective approaches to the regulation of digital trade and whether the parties diverge or coalesce on regulatory reform. Reform in the EU, in the form of the Digital Services Act, is imminent, but it remains to be seen whether the U.K. will follow suit.

Return to Table of Contents

Contacts

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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