Skadden

# Privacy & Cybersecurity Update



## FTC To Continue Enforcing EU-US Privacy Shield Following Invalidation

**The Federal Trade Commission (FTC) has confirmed its intent to continue enforcing the EU-U.S. Privacy Shield Framework in the United States in respect of personal data transferred under the framework prior to its invalidation by the Court of Justice of the European Union (CJEU) last month.**

### Background

The Privacy Shield, which took effect in 2016, allowed companies to transfer personal data from the European Economic Area (EEA) to the U.S. if they self-certified compliance with certain requirements based on the EU's standards for data protection. After taking effect, more than 5,300 companies certified their adherence to the Privacy Shield.

On July 16, 2020, the CJEU invalidated the Privacy Shield as a mechanism to transfer personal data from the EEA to the U.S. while upholding the validity of standard contractual clauses as a transfer mechanism. The European Union's high court found that the Privacy Shield did not adequately protect Europeans' data once it entered the U.S. and did not offer effective redress for EU citizens whose data was transferred. The CJEU struck down the Safe Harbor, which was the Privacy Shield's predecessor, for similar reasons in 2015.[1]

### FTC Enforcement of the Privacy Shield

In testimony before the Senate Committee on Commerce, Science, and Transportation, FTC Chairman Joe Simons expressed the agency's intent to continue holding companies accountable for privacy commitments made under the Privacy Shield prior to its invalidation. Companies that transferred data to the U.S. under the Privacy Shield must continue to handle that data in accordance with the commitments made under the framework, with failure to comply subject to potential FTC enforcement actions. As such, a company's failure to abide by its commitments under the Privacy Shield may be challenged as deceptive by the FTC. The agency has the power to prohibit such misrepresentations through administrative orders or by seeking court orders, and to impose civil penalties for violations of its administrative orders of up to $40,000 per violation or $40,000 per day for continuing violations.

[1] The CJEU's decision is discussed in more detail in the July 2020 edition of our *Privacy & Cybersecurity Update*.

### Key Takeaways

The U.S. and the EU are currently in discussions about a mechanism that will replace the Privacy Shield, but until there is a solution companies are obligated to uphold any commitments to safeguard personal data transferred under the Privacy Shield. In addition, companies that previously relied on the Privacy Shield as a transfer mechanism should ensure that their privacy policies are updated to accurately reflect their current practices regarding international data transfers.

Return to Table of Contents

## Office of Administrative Law Finalizes California Consumer Privacy Act Regulations

**On August 14, 2020, the California Office of Administrative Law approved the regulations issued by the California Department of Justice pursuant to the California Consumer Privacy Act (CCPA), with the regulations taking immediate effect. The final regulations include certain changes to the drafts previously submitted by the California Department of Justice.**

The California Office of Administrative Law approved final regulations issued by the state's Department of Justice that pare back some of the requirements for companies that were originally expected to be included in the law. The final CCPA regulations remove certain previous provisions that addressed consent from and communications with consumers, as well as methods for companies to handle consumer requests submitted pursuant to the CCPA. The removal of these provisions make the final regulations somewhat less stringent in certain respects than previous drafts. California Attorney General Xavier Becerra left open the possibility that these provisions, or variations thereof, may be resubmitted by his office for inclusion in the regulations following further review.

### Changes Compared to Previous Drafts

The finalized regulations included five notable changes from previous versions:

- The requirement that companies obtain consent from consumers before using their personal information for any new business purpose has been deleted from the final regulations. Instead, a company must only provide notice of its intent to use the data for a new business purpose.
- Companies that substantially communicate with their customers offline are not required to provide notice to consumers regarding the right to opt out of data collection through hard copy notices. Instead, a company may provide such notice on its website.
- Language stipulating that a company's methods for handling consumer requests to opt out must be "easy for consumers to execute" and "require minimal steps" has been removed from the final regulations, as has language expressly prohibiting companies from using a method "designed with the purpose or [that] has the substantial effect of subverting or impairing a consumer's decision to opt-out."
- The final regulations do not include a provision that permitted companies to deny a request from a consumer's agent who does not offer proof that the agent has been authorized by that consumer to act on their behalf.
- Companies must label their hyperlinks directing consumers to privacy choices with "Do Not Sell My Personal Information," rather than the shortened version, "Do Not Sell My Info."

The regulations became effective immediately as of August 14, 2020.

### Key Takeaways

Companies that are subject to the CCPA may now finalize their compliance programs with some degree of certainty based on the issuance of the final regulations. However, it remains to be seen whether other changes to the California privacy landscape may be made in the months to come, either through passage of the California Privacy Rights Act (Proposition 24), which Californians will vote on in November, or otherwise. Given the immediate effect of the final CCPA regulations, companies should quickly review their compliance programs to ensure that they are in compliance with the final regulations, including the changes summarized above.

Return to Table of Contents

## NIST Proposes Four Principles of 'Explainability' for Artificial Intelligence

**The National Institute of Standards and Technology (NIST) has proposed four principles to assist companies in determining how well the decisions made by artificial intelligence (AI) systems can be explained. The proposed principles are subject to public comment through October 15, 2020.**

### Background

AI systems are based on algorithms that learn from large amounts of data. Once these algorithms have learned from past experience by identifying patterns in the training data, an AI system can be queried with new data, with the result of such queries being the AI system's output.

Given the complexity of AI systems, the ways in which these systems generate outputs are generally not intuitive and often hard to explain. In addition, AI systems are increasingly used by companies to make decisions that may have a material impact on consumers, such as whether a particular consumer is creditworthy. Accordingly, regulators are increasingly requiring companies that use AI in certain types of decision-making to be able to explain how the AI system arrived at a particular decision. The extent to which a decision made by an AI system can be explained is referred to as the system's "explainability."

NIST's proposed principles are designed to assist companies in evaluating the extent to which the AI systems that they use are explainable, which may in turn assist companies in determining whether they are likely to meet the explainability requirements imposed by certain regulators. NIST also noted that explainability, along with resiliency, reliability, bias and accountability, helps to determine how trustworthy an AI system is perceived to be. Additionally, NIST noted that the draft publication introducing these principles (Draft NISTIR 8213)[2] is meant to serve as a conversation starter on these issues. These draft principles are part of a broader NIST project designed to build trust in AI systems by understanding their theoretical capabilities and limitations and by improving their accuracy, reliability, security and robustness, in addition to their explainability.

### Proposed Principles of Explainability

In its draft document NIST proposed the following four principles for explainability:

- **Explanation:** The AI system should deliver accompanying evidence or reasons for all of its outputs. This principle does not examine whether the explanation is itself correct, only whether there is evidence that the system is capable of providing an explanation.
- **Meaningful:** An explanation is deemed to be meaningful if a user can understand the explanation. NIST noted here that different groups of users for a system may require different explanations.
- **Accuracy:** In the context of AI explainability, this means that explanation correctly reflects the system's process for generating the output. Just as the meaningful principle acknowledges that different groups of users may find different explanations meaningful, NIST notes that this principle allows for different accuracy metrics for different users. Thus, explanations with varying levels of detail can all be accurate, depending on the users to which the explanations are directed. It is important to note here that this requirement does not mean that the system's output itself must be correct.
- **Knowledge Limit:** Systems should identify the cases for which they were not designed or approved to operate, or for which their answers are not reliable. The other three principles assume that the AI system only operates under conditions for which it was designed or when the system reaches a sufficient confidence in its output. If the system is operating outside of its knowledge limits, such that it produces inaccurate or even dangerous results, then it is untrustworthy.

### Key Takeaways

As organizations increasingly use AI technology to drive high-impact decision-making, various stakeholders — including consumers and regulators — are focused on the explainability and transparency of such systems. Companies that use AI systems should familiarize themselves with the principles of explainability and consider whether their systems would satisfy NIST's proposed principles. In addition, companies with strong views on the ways in which the proposed principles may impact their use of AI systems should consider submitting comments to NIST prior to October 15, 2020.

Return to Table of Contents

## New Federal Guidance Around Anti-Drone Technologies

**On August 17, 2020, the Federal Aviation Administration (FAA), Department of Justice (DOJ), Federal Communications Commission (FCC) and Department of Homeland Security (DHS) issued advisory guidance for nonfederal public and private entities considering using technical tools, systems and capabilities to detect and mitigate unarmed aircraft systems (UAS), often referred to as "drones." The guidance, which is the first of its kind with respect to detection and mitigation technologies for these systems, highlights the potential legal ramifications for adopting such anti-UAS technologies.**

### Background

In recent years, the increased use of UAS has raised significant concerns regarding privacy and security. In response, some companies and individuals alike have adopted "anti-UAS" technologies to either deter unwanted UAS from entering a particular area or disable these aircraft from operating entirely. A handful of states have adopted laws addressing UAS technologies; however, there is little legal guidance on anti-UAS technologies, particularly under federal law. The advisory, while issued for informational purposes only, serves as a comprehensive guide to the federal laws that may be implicated by these anti-UAS technologies.

[2] NIST's document setting forth the four proposed principles can be found here.

### Overview of the Advisory

The advisory[3] is split into two categories of federal laws that may be implicated by anti-UAS technologies: federal criminal laws, and federal laws and regulations administered by the FAA, DHS and FCC. The advisory generally discusses two different types of anti-UAS technologies — those technologies that "detect" UAS and those that "mitigate" UAS.

Technologies that detect UAS generally rely on radio-frequency, radar, electro-optical, infrared or acoustic capabilities, or any combination of these methods. Technologies that mitigate UAS generally rely on solutions that use either nonphysical measures, including radio-frequency, Wi-Fi or GPS capabilities, or physical measures, including nets, projectiles and lasers, to disrupt or disable UAS.

According to the advisory, technologies that detect UAS systems may implicate existing federal surveillance laws, such as the Penn/Trap Statute (18 USC Section 3121-3127) or the Wiretap Act (18 USC Section 2510). Whether an anti-UAS detection technology will implicate such laws may depend on whether the technology captures, records, decodes or intercepts the electronic communications transmitted from a UAS to the individual or entity controlling the device. For example, detection systems that emit electromagnetic waves or pulses of sound or light are less likely to present concerns with respect to federal criminal surveillance statutes than systems that use radio-frequency capabilities to detect and track UAS, according to the advisory.

The advisory also cautions that technologies that mitigate UAS either through physical or nonphysical solutions also may implicate existing federal criminal laws. For example, jamming technologies that restrict radio-frequency signals from being used by a UAS or that prevent GPS units from receiving positioning signals, or the use of spoofing technologies, which can replicate, replace or modify signals to interfere with the UAS's link to its controller, may run afoul of several statutes, according to the advisory. These include the Computer Fraud and Abuse Act (18 U.S.C. Section 1030); Interference with the Operation of a Satellite (18 U.S.C. Section 1367); and Communication Lines, Stations or Systems (18 U.S.C. Section 1362). Physical destruction, seizure or control of the UAS may implicate the Aircraft Sabotage Act (18 U.S.C. Section 32(a)) or the Aircraft Privacy Act (49 U.S.C. Section 46502).

The advisory also notes that UAS detection or mitigation technologies also may implicate laws and regulations administered by the FAA, the FCC and the TSA. For example, anti-UAS detection technologies may implicate laws relating to aviation safety and efficiency, as regulated by the FAA; laws relating to transport and airport security, as regulated by the TSA; and, given anti-UAS technologies may involve radio-frequency-enabled solutions, laws that relate to the authorization of use of the radio frequency spectrum, as regulated by the FCC.

### Open Issues

While the advisory provides an overview of the federal laws that may be implicated by anti-UAS technologies, it does not propose solutions for avoiding violations of the laws (although it does provide some exceptions that could apply to the use of anti-UAS technologies). Further, the advisory does not address how courts will interpret these laws in the context of anti-UAS technologies. To date, there has been limited case law on this issue.

### Key Takeaways

Companies considering implementing anti-UAS disabling or mitigating technologies for corporate security purposes should evaluate whether their methods run afoul of certain of the laws highlighted in the advisory, in addition to analyzing whether such technologies implicate any relevant state or local laws. However, in the absence of federal law that directly addresses anti-UAS technologies or clear guidance from the court system, companies considering implementing such UAS disabling or mitigating technologies should be prepared to balance privacy and security considerations with ensuring compliance with federal, state and local laws.

Return to Table of Contents

## UK Information Commissioner's Office Publishes Finalized Artificial Intelligence Guidance

**With artificial intelligence increasingly becoming a part of everyday life, the U.K. Information Commissioner's Office (ICO) has released a guidance framework for which companies can look to when utilizing these technologies. The office's guidance will be particularly relevant for organizations who will make use of AI systems to process personal data, as it covers the ICO's best practices to ensure compliance with data protection laws.**

The ICO has published its final guidance on artificial intelligence following an open consultation period that concluded in April 2020.[4] The guidance aims to help organizations mitigate the data protection risks that may arise in relation to AI projects, and provides a framework for ensuring that AI solutions comply with the General Data Protection Regulation 2016/679 (GDPR) and the U.K. Data Protection Act 2018.

[3] The advisory is available here.

[4] The guidance can be found here.

### Summary of the Guidance

The guidance is divided into four main sections, the key takeaways of which are described in more detail below.

#### Accountability and Governance

This section deals with the GDPR's accountability principle and how organizations can demonstrate that AI systems comply with data protection laws.

- **Data Protection Impact Assessments (DPIAs) are key.** The ICO considers that, in the vast majority of cases, the use of AI will trigger the need for a DPIA. AI systems can involve high-risk processing operations, such as the use of new technology or the novel use of existing technology, both of which may require a DPIA to be performed. The ICO warns against organizations taking a box-ticking approach to DPIAs, saying "they can effectively act as roadmaps for you to identify and control the risks to rights and freedoms that using AI can pose." A DPIA should include a systematic description of the processing activity and any error margin in the performance of the AI system (*e.g.*, where the use of AI may produce effects on individuals). The ICO acknowledges that the processing activity may be difficult to describe and suggests producing two DPIAs: one for a specialist technical audience and one for a generalist audience.
- **Organizations must identify and mitigate risks.** The identification of risks will be aided by the DPIA process, with the ICO recommending assigning a score to each identified risk, factoring in the likelihood of occurrence and the severity of the impact. Organizations can mitigate risks through data minimization and by providing opportunities for individuals to opt-out of the processing. The ICO does not expect organizations to mitigate every risk identified, but if an organization is unable to sufficiently reduce a high-risk instance, it must consult with the ICO before proceeding with the processing.
- **The role of every organization involved should be clearly mapped out.** Given that many different organizations are often involved in developing AI systems that process personal data, the ICO encourages parties to identify in which capacity they are acting (controllers, joint controllers or processors). The ICO plans to consult with stakeholders in order to offer further guidance.
- **Where AI systems involve balancing competing interests, organizations should document their balancing exercise.** For example, a balancing exercise should be performed where there is a clash of interests between training a sufficiently accurate AI system and reducing the quantity of personal data processed to train the system. The ICO notes that such a trade-off will be a case-specific matter of judgment, but stresses the need for organizations to properly document their decision-making process.

#### Lawfulness, Fairness and Transparency

This section explains the application of the lawfulness, fairness and transparency of GDPR principles in the AI context.

- **Distinguish between AI development and deployment when determining the legal basis for processing.** The guidance notes that the purpose of developing an AI system (including the conceptualization, design and training of the AI system) may be different from the purpose for which the AI system is deployed. For example, a facial recognition AI system may be trained to recognize faces at the development stage, but at the deployment stage it could be used for other purposes (*e.g.*, crime prevention, authenticating employees entering a building). Organizations should be clear on the legal basis they are relying on at each of the development and the deployment stages.
- **Consent can be used as a legal basis, but individuals must be properly informed.** The guidance states that consent may be an appropriate legal basis, provided that it meets the GDPR standard (*i.e.*, it is freely given, specific, informed and unambiguous). Consent also could lead to increased trust in AI systems by giving more control to individuals over their data. However, individuals must be properly informed as to how organizations are using their personal data. The challenge for organizations will be to explain complex AI systems to individuals in an easily understandable and accessible way.
- **The statistical accuracy of AI is essential for organizations to comply with the fairness principle.** Recital 71 of the GDPR states that organizations should put in place appropriate mathematical and statistical procedures for the profiling of individuals. However, the guidance states that this does not mean that every inference made by an AI system has to be correct. Accordingly, whether such inferences are considered fair will depend on the impact on the individual and the statistical accuracy of the inference. Organizations should monitor statistical accuracy on an ongoing basis in order to ensure compliance with the fairness principle.

#### Data Minimization

AI presents a challenge for the data minimization principle due to the large quantities of data required to train AI systems. This section considers data minimization techniques.

- **Organizations should ensure that their compliance function is involved in AI development.** Data scientists may want to collect as much data as possible to train AI systems. Organizations' compliance functions will need to be joined with AI system developers from an early stage to ensure that the development of AI systems uses personal data in a way that is limited to what is strictly necessary in relation to the envisaged purpose.

- **Privacy Enhancing Techniques (PETs) should be used to minimize the amount of personal data used in the training phase.** PETs involve modifying datasets that contain personal data to avoid the tracing back to individuals, or to make such tracing more difficult. An example of a PET is differential privacy, which is essentially where random data is included as part of a dataset preventing individuals from being singled out. Data protection laws, however, will not apply to datasets that have been truly and functionally anonymized.

### Individuals' Rights

This section covers dealing with data subject rights' requests, both in the development and deployment phases of AI systems, and the protection of individual rights generally by ensuring there is human oversight of decisions made by AI systems.

- **Ensure data subject rights' requests can be respected.** Responding to data subject rights' requests may be more challenging in the context of AI systems. However, data subject rights are still relevant, and organizations should ensure that they can respond to them effectively and efficiently. Given the number of parties involved in the development of an AI system, organizations need to ensure that their agreements with co-parties contain cooperation and assistance obligations in responding to data subject rights' requests.
- **Personal data already processed within a training dataset can still be subject to the right to erasure.** Although the right to erasure is not absolute, an individual has a right to seek the deletion of his or her personal data within a training dataset. The guidance further notes that erasing an individual's personal data from a training dataset is unlikely to materially impact the output of the AI system. The ICO therefore considers it unlikely that organizations will be able to justify not respecting an individual's right to erasure, and, when requested, must remove such data from their training datasets.
- **Human oversight of AI decisions must be meaningful.** Individuals may object to automated decision-making under the GDPR where it is *solely* based on automated processing that produces legal effects that concern them or similarly significantly affect them, unless such decision-making has been subject to some level of human input. The degree and quality of human intervention is central and the guidance is clear that merely having a human "rubber-stamp" an automated decision-making process resulting from AI is inadequate. Organizations should ensure that AI systems are designed to facilitate effective human oversight and train staff accordingly so that they can critically assess the output of the AI system. Practically, this means that staff should have the appropriate internal authority to override the outcome of the AI system.

### Key Takeaways

The ICO acknowledges that AI is an area of "fast moving innovation and evolution" and will continue to consult with relevant stakeholders to ensure that the guidance remains relevant. The ICO also is developing an accountability toolkit that is not specific to AI but provides a baseline for demonstrating accountability. Once released, this toolkit will provide further support for organizations auditing the compliance of their AI systems. We will be watching this space for further developments.

Return to Table of Contents

# Privacy & Cybersecurity Update

## Contacts


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

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

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

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

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

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

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

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

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

**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