March 2022

Skadden

# Privacy & Cybersecurity Update



## US and European Commission Announce Commitment to Create New Trans-Atlantic Data Privacy Framework

**On March 25, 2022, the U.S. and the European Commission announced that they had jointly committed to creating a Trans-Atlantic Data Privacy Framework, an important first step in crafting a data transfer structure to replace the EU-U.S. Privacy Shield, which was invalidated by the Court of Justice of the European Union (CJEU) in 2020. The actual agreement between the EU and the U.S. will need to be built over the coming months, and is likely to face new legal challenges when completed.**

President Joe Biden and European Commission President Ursula von der Leyen announced that the U.S. and EU had reached an agreement in principle on the framework, which represents the third attempt at developing a data transfer mechanism in order to more easily allow for data flows from the EU to the U.S. that is complaint with the General Data Protection Regulation 2016/679 (GDPR). The White House also released a corresponding fact sheet further detailing U.S. commitments to address the prior decisions of the CJEU, which had invalidated both the Safe Harbor Privacy Principles and the EU-U.S. Privacy Shield.

### Background

Under the GDPR, personal data cannot be transferred from the European Economic Area (EEA) to countries outside the EEA that have not been deemed by the European Commission to have an adequate level of privacy protection, which includes the U.S., unless the data controller or processor have taken measures to compensate for the lack of data protection in said country by way of appropriate safeguards for the data subject. The U.S. and the EU had developed two data sharing structures between the EEA and the U.S. that were designed to provide a relatively easy "self-certification" method for U.S. companies to satisfy this safeguard requirement, each of which have been invalidated by the CJEU. In October 2015, the CJEU determined that the first such structure, the Safe Harbor Privacy Principles, were invalid in its ruling in *Schrems v. Data Protection Commissioner (Schrems I)*. In that decision, the CJEU found that the Safe Harbor failed to adequately protect the privacy of EU citizens, mainly due to the U.S. government's ability to access personal data for national security purposes.

In response, the U.S. and EU developed a new Privacy Shield self-certification mechanism. The Privacy Shield was aimed at remedying the perceived inadequacies of the

Safe Harbor by imposing certain restrictions on the collection of EU personal data by the U.S. government and appointing an ombudsman to oversee such collection practices. However, after the Privacy Shield's adoption, many privacy advocates criticized the replacement framework for failing to address the concerns about government surveillance that were raised in *Schrems I*.

On July 16, 2020, the CJEU ruled in *Irish Data Protection Commissioner vs Facebook and Maximillian Schrems (Schrems II)* that the EU-U.S. Privacy Shield also was invalid. In its decision, the CJEU criticized the surveillance programs of the U.S. intelligence authorities for lacking legal protection for EEA/U.K. data subjects, and found the safeguarding mechanisms established in the Privacy Shield to be insufficient. Following the *Schrems II* decision, transfers of personal data from the EEA/U.K. to the U.S. must instead be based on an alternative valid data transfer mechanism. Most organizations have chosen to rely on the European Commission's standard contractual clauses (SCCs) to legitimize their data transfers to the U.S. Though welcomed by many EEA/U.K. data subjects, this decision placed significant limitations on companies undertaking frequent transfers of personal data to the U.S.

### Trans-Atlantic Data Privacy Framework

The new Trans-Atlantic Data Privacy Framework is aimed at balancing the privacy of EU personal data while facilitating the data flows necessary to allow companies to conduct cross-border business operations. Since *Schrems II*, the EU and the U.S. have participated in yearslong negotiations to develop a valid data transfer mechanism that will withstand anticipated legal challenges. While the actual agreement between the EU and the U.S. will need to be crafted over the coming months, the announcement outlined the following principles that will be incorporated into the framework. The framework is expected to:

1. set out rules and safeguards to limit U.S. intelligence agencies' access to EU personal data and require such agencies to adopt procedures to ensure oversight of privacy standards;
2. introduce a two-tier redress system through which EU citizens will be able to seek independent review by an independent and binding authority; and
3. leverage the same principles used under the Privacy Shield by requiring companies to self-certify through the U.S. Department of Commerce that they adhere to the Privacy Shield principles.

### Commitments to Address Concerns Addressed in *Schrems II*

The Framework announcement from the White House makes clear that the U.S. intends to make efforts to address the CJEU's concerns in *Schrems II*. The Privacy Shield was intended to address the perceived inadequacy of U.S. privacy laws when viewed under the European Commission's privacy standards, but failed to meet the CJEU's standards for protecting EEA's citizens' data. The CJEU's decision to invalidate the Privacy Shield was based on: (i) the limitations on the protection of personal data under U.S. law, and (ii) the disproportionate access and use of EEA personal data by U.S. authorities with no effective redress mechanism for data subjects. In particular, the CJEU found that access to personal data under U.S. surveillance programs could not be regarded as being limited to what is "strictly necessary," and that the Privacy Shield also did not grant individuals based in the EEA actionable rights before U.S. courts against U.S. authorities. According to the CJEU, the Privacy Shield therefore could not ensure a level of protection "essentially equivalent" to that arising from the GDPR as supplemented by national data protection laws across the EEA, nor could it guarantee individuals' fundamental rights under the EU Charter of Fundamental Rights.

The Biden administration's announcement regarding the new framework states that the U.S. will address the decision in *Schrems II* by:

1. limiting signals intelligence collection to what is necessary to advance legitimate national security objectives;
2. requiring that signals intelligence collection does not disproportionately impact the protection of individual privacy and civil liberties;
3. allowing EU citizens to seek redress from an independent Data Protection Review Court consisting of individuals from outside of the U.S. government; and
4. ensuring that U.S. intelligence agencies implement procedures to effectively oversee new privacy standards.

### Potential Impact of *FBI v. Fazaga*

Privacy experts suggest that a recent U.S. Supreme Court decision — *FBI v. Fazaga*[1] — may make it more difficult for the Trans-Atlantic Data Privacy Framework to survive CJEU review. EU law requires that EU citizens be able to seek redress before an independent authority and raise fundamental legal challenges to unlawful surveillance. On March 4, 2022, the U.S. Supreme Court held that the state secrets privilege, which allows the government to withhold information when disclosing it would compromise national security, is not superseded by the Foreign Intelligence Surveillance Act. By allowing the U.S. government to shield sensitive evidence in litigation, this decision may make it more difficult for individuals challenging the U.S. intelligence agencies' surveillance practices. Unless addressed by Congress or provided for in the forthcoming framework, the *Fazaga* decision could work against U.S. efforts to bridge the gap between

[1] *FBI v. Fazaga*, 142 S.Ct. 1051 (2022).

the U.S. government's surveillance rights and the rights provided to EU data subjects under the GDPR.

### Next Steps

The announcement only confirms that the U.S. and the European Commission have reached an agreement in principle, and now the work begins to draft the text of the framework that will need to be adopted by both jurisdictions. A draft of such agreement is expected as early as next month. President Biden also will issue an executive order to implement U.S. commitments outlined in the framework. The agreement will then be subject to the review of EU data protection regulators and each EU government.

Similar to the Safe Harbor and Privacy Shield, the framework is expected to face legal challenges. Relatedly, the plaintiff behind *Schrems I* and *Schrems II*, privacy lawyer and activist Max Schrems, has already suggested he will take legal action after reviewing the text of the framework in depth.

Return to Table of Contents

## Utah Becomes Fourth State To Adopt Comprehensive Privacy Law

**Utah has become the fourth state — along with California, Virginia and Colorado — to enact a privacy law, continuing the splintered state-level approach regarding how businesses need to address privacy and the rights that individuals have with respect to their personal data.**

On March 24, 2022, Gov. Spencer Cox signed the Utah Consumer Privacy Act (UCPA) into law, slated to become effective on December 31, 2023, which is one year later than when the Virginia and Colorado laws go into effect, and when the California Privacy Rights Act (CPRA) is scheduled to replace the California Consumer Protection Act (CCPA).

The new Utah law draws on concepts from the EU's GDPR (such as the use of "controllers" and "processors") and the legislation passed in California, Virginia, and Colorado (regarding rights of consumers), but is more business-friendly than these privacy regulations. Additionally, despite their similarities, the passing of the UCPA adds to the fragmented approach to privacy law in the U.S. Fortunately, for companies already working to comply with the CPRA and Virginia and Colorado laws, Utah's approach may mean they will not have to do much additional work to comply with this additional state requirement.

### Which Businesses Are Covered?

The UCPA applies to entities that (i) either conduct business in Utah or conduct business outside of the state but produce a product or service that is targeted to consumers who are residents of Utah, and (ii) have an annual revenue of $25 million and satisfy one or more of the following thresholds: (1) during a calendar year, controls or processes personal data of 100,000 or more consumers, or (2) derives over 50% of their gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers. This creates a higher trigger for compliance than California, Virginia and Colorado since it requires that a business meet both a financial threshold as well as a data volume threshold.

### Exemptions

The UCPA includes certain carve-outs, similar to the laws in the other three states. For example, it does not apply to governmental entities, nonprofit corporations, tribes, institutions of higher education, covered entities and business associates governed under the Health Insurance Portability and Accountability Act (HIPAA), and air carriers. It additionally exempts information governed by certain federal laws, including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act, the Family Education Rights and Privacy Act, and HIPAA.

### Which Consumers Are Covered?

A "consumer" is defined under the UCPA as "an individual who is a resident of the state acting in an individual or household context." Echoing the business-to-business and employment carve-out under Virginia and Colorado's regulations, the UCPA excludes from its definition of consumer any "individual acting in an employment or commercial context." Although California's CPRA contains a similar exemption, that carve-out will no longer apply as of January 1, 2023, unless it is extended.

### What Information Is Protected by the UCPA?

The cornerstone of all privacy laws is the definition of "personal data," which is defined under the UCPA as "information that is linked or reasonably linkable to an identified individual or an identifiable individual." This construct is virtually identical to that of Virginia's CDPA and Colorado's CPA, and, as in these two regulations, does not include specific categories of data that are found in California's CCPA and CPRA. In another distinction from the California laws, the definitions of personal data under the Colorado CPA, Virginia's CDPA and Utah's UCPA do not include information linkable to "households."

### Exemptions

As with the laws in California, Virginia and Colorado, the definition of personal data under Utah's law explicitly excludes "de-identified data, aggregated data, or publicly available information." Publicly available information under the UCPA, similar to Virginia and Colorado, is defined as (i) information that is lawfully made available from government records, (ii) "information that a person reasonably believes a consumer or widely distributed media has lawfully made available to the general public," or (iii) "information that a person reasonably believes a consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information."

As with the laws in Virginia and Colorado, certain consumer rights under the UCPA do not apply to "pseudonymous data" (*i.e.*, personal data that is not attributable to a specific individual without the use of additional information) as long as the additional information is "kept separate from the consumer's personal data and subject to appropriate technical and organizational measures to ensure that the personal data are not attributable to an identified individual or an identifiable individual."

### Controllers and Processors

Similar to the regulations in Virginia and Colorado, Utah's UCPA utilizes the categories of "controllers" and "processors" to lay out obligations for businesses, mirroring the approach of the EU's GDPR. A controller is defined as "a person doing business in the state who determines the purposes for which and the means by which personal data are processed, regardless of whether the person makes the determination alone or with others," whereas a processor is any "person that processes personal data on behalf of a controller." The majority of the obligations created by the UCPA are aimed at the controllers rather than the processors.

### Consumer Rights

As with all three of the other states' privacy laws, the UCPA grants consumers a series of data privacy rights, including the rights to access and delete personal data, data portability and the right to opt out. Consumers may exercise such rights by submitting a request to a controller and specifying the right the consumer intends to exercise, to which the controller must respond within 45 days. A controller may extend the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller. The controller must inform the consumer of the extension in the initial 45-day period, including details of the length of the extension and the reasons the extension is reasonably necessary. The 45-day period does not apply if the controller reasonably suspects the consumer's request is fraudulent and the controller is not able to authenticate the request before the 45-day period expires. The UCPA also allows for businesses to charge consumers fees when responding to requests, including allowing controllers to charge a fee if the request is the consumer's second or subsequent request during the same 12-month period.

### Right To Opt Out

Consumers have the right to "opt out of the processing of the consumer's personal data for purposes of: (a) targeted advertising or (b) the sale of personal data." Similar to Virginia's law, the UCPA defines a sale as "the exchange of personal data for monetary consideration by a controller to a third party," which is considered a narrower approach than California, which includes any type of consideration. Under the UCPA, if the controller sells a consumer's personal data to third parties or engages in targeted advertising, the controller must "clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of the: (i) sale of the consumer's personal data or (ii) processing for targeted advertising." This is intended to provide consumers with transparency regarding their right to opt out. Unlike Virginia and Colorado's privacy laws, the UCPA does not allow consumers to opt out from profiling.

### Right of Access

Consumers have the right to "confirm whether a controller is processing the consumer's personal data and access the consumer's personal data."

### Right to Correction

Unlike the other three states' privacy laws, the UCPA does not grant consumers in Utah the right to correct inaccuracies in their personal data.

### Right to Deletion

Consumers have the right to "delete the consumer's personal data that the consumer provided to the controller." This right does not allow consumers the right to delete all personal data that a controller possesses about the consumer, rather only the personal data that was provided by the consumer to the controller. Unlike the Virginia, but similar to California, the consumer's right to deletion is more limited under the UCPA as under the Virginia CDPA, consumers have a right to delete both personal data they have provided to the controller and data that has been obtained by the controller from third parties about the consumer.

### Right to Data Portability

When exercising the aforementioned right to access personal data, under the UCPA consumers have the right to "obtain a copy of the consumer's personal data, that the consumer previously provided to the controller, in a format that: (a) to the extent technically feasible, is portable; (b) to the extent practicable, is readily usable; and (c) allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means."

### Obligations Imposed on Businesses

The UCPA imposes limitations on how businesses can collect and use consumers' personal data, while also requiring businesses to implement specific security and transparency measures regarding personal data.

### Duty of Transparency and Purpose Specification

A controller must provide consumers with "a reasonably accessible and clear" privacy notice that explains the categories of personal data processed by the controller and the purposes for which such data are processed; the types of information the controller shares with third parties and the categories of third parties the controller may share personal data with; and how consumers may exercise their privacy rights.

### Technical Safeguards and Transparency Measures

A controller must establish, implement and maintain reasonable administrative, technical and physical data security practices to protect personal data and reduce foreseeable risks of harm to consumers related to the processing of personal data.

### Duty of Nondiscrimination

A controller may not discriminate against a consumer for exercising a right by denying goods or services to the consumer, charging the consumers different prices for such goods or services, or providing the consumer a different level of quality.

### Duty Regarding Sensitive Data

A controller is not allowed to process a consumer's "sensitive data" without first presenting the consumer with clear notice and an opportunity to opt out of the processing, or, in cases involving a child, processing the data in accordance with the federal Children's Online Privacy Protection Act.

"Sensitive data" under the UCPA is defined as personal data that reveals an individual's racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, or information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional. "Sensitive data" also includes the processing of genetic personal data or biometric data for identifying a specific individual and specific geolocation data.

While both Colorado's CPA and Virginia's CDPA require controllers to obtain consumers' affirmative consent to collect or process their sensitive data, the UCPA aligns closer to California's law, imposing only an obligation to provide an opt-out mechanism (unless the sensitive data belongs to a child).

### Data Protection Assessments

Notably, unlike the other three state privacy laws, the UCPA does not require data controllers to conduct and document data protection impact assessments of its processing activities, highlighting the UCPA's more business-friendly approach.

### Data Processors

Under the UCPA, data processors are required to adhere to the instructions of the controller and assist the controller to meet its obligations under the law. The UCPA requires controllers and processors to enter into a contract that establishes their relationship and respective obligations, including clearly setting forth instructions for processing personal data. Processors are obligated to take "appropriate" technical and organizational measures to assist controllers in meeting their obligations, including those related to the security of processing personal data and notification of a breach of a security system. The UCPA takes a more limited approach to the contract requirements than the other state privacy regulations, including not requiring contracts with processors to include provisions mandating that processors allow for or contribute to reasonable audits, or requiring processors to make information necessary to demonstrate compliance available to the controller.

### Enforcement

As with Virginia's CDPA and Colorado's CPA, but unlike California's CCPA and CPRA, the UCPA does not create any private right of action for consumers. Instead, the UCPA allows the Division of Consumer Protection (DCP) to accept and investigate consumer complaints regarding the processing of personal data. If the DCP identifies substantial evidence, it will refer the matter to the state attorney general, who has exclusive authority to enforce Utah's law. Similar to Virginia and Colorado, Utah's law does not allow consumers to sue for alleged failures to adequately protect consumers' personal data, which is indeed permitted under California's law.

Prior to taking any enforcement action to address noncompliance, the Utah attorney general must issue a written notice of violation

to the controller or processor. Upon receiving such notice, the controller or processor has 30 days to cure the alleged violation, which is the same length as the California and Virginia laws, but divergent from Colorado's law, which has a cure period of 60 days (however, this cure period expires on January 1, 2025).

If a controller or processor fails to cure a violation after receiving notice, the attorney general may recover (i) actual damages to the consumer and (ii) an amount not to exceed $7,500 per violation. Similarly, the Virginia law imposes civil penalties of up to $7,500 for each violation, while the California laws impose a civil penalty of $2,500 for each violation or $7,500 for each intentional violation. The CPRA also imposes a $7,500 penalty for each violation involving a minor. Distinctly, the Colorado law does not specify the penalty amounts, and civil penalties could be up to $20,000 for each violation with a maximum penalty of $500,000 for any related series of violations.

### Key Takeaways

Despite similarities to California's CCPA and CPRA, Colorado's CPA and Virginia's CDPA, the rights and obligations created by Utah's new privacy law take a lighter, more business-friendly touch than the other regulations, particularly with respect to not requiring data protection impact assessments. Consumer advocates have expressed concern that this will spark a "race to the bottom," with states seeking to be seen as more business-friendly when crafting their own privacy laws. While it remains to be seen whether these concerns come to fruition, the different approaches utilized by the four states discussed above offers those states that have yet to create their own privacy legislation with a variety of frameworks to go off of if they choose to enact similar laws.

Return to Table of Contents

## California Attorney General Clarifies Status of 'Inferences' Under CCPA

**The Office of the Attorney General of the State of California clarified that internally generated inferences about a consumer must be provided in response to a request to access such consumer's personal information. However, inferences are not required to be provided if a business can establish that doing so would disclose the company's trade secrets.**

### Background

The CCPA, which was signed into law in June 2018 and became effective as of 2020, gives California consumers the rights to know about businesses' collection of their personal information, to request that it be deleted, and to opt out of its sale. On March 10, 2022, the state attorney general's office released its first-ever opinion[2] interpreting the CCPA. In the release, the attorney general explained that internally generated "inferences" — defined as "the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data" — about a consumer are required to be provided in response to the consumer's request for access to such consumer's personal information, where such inferences are used to create a profile about a consumer.

### 'Inferences' Broadly Defined

The CCPA specifically identifies "inferences drawn … to create a profile about a consumer" as one category of personal information. The opinion clarified that the term "inference" applies even in instances where the information from which said inference was derived is itself exempt from the scope of the CCPA (*i.e.*, where the basis of the inference does not qualify as "personal information" under the statute) or was obtained from sources other than the consumer. Since the CCPA gives consumers the right to receive all information *collected about* the consumer — not just information *collected from* the consumer — the opinion reasoned that it is irrelevant if the inference was generated internally (*i.e.*, "collected" in the broader sense) by the responding business using internal or external information sources.

### No Obligation To Disclose Trade Secrets

With respect to the concern that an obligation to disclose internally generated inferences may expose a company's trade secrets, the opinion clarified that the CCPA does *not* require disclosure of trade secrets. While not clearly stated in the statute, the opinion identifies the disclosure of trade secrets as one potential exception to responding to a request for personal information under the CCPA. However, any business that chooses to withhold any inferences on the basis that such inferences constitute the company's trade secrets "bears the ultimate burden of demonstrating that such inferences are indeed trade secrets under the applicable law."

### Key Takeaways

Businesses subject to the CCPA should review their policies and practices to confirm that inferences used to create profiles about consumers are included within the definition of "personal information" for purposes of CCPA compliance. Any business that is concerned about the disclosure of internally generated inferences resulting in the disclosure of trade secrets should consider taking steps to mitigate such risks. For example, if such inferences are

[2] The attorney general's opinion can be viewed here.

generated and then anonymized or aggregated, then the inferences would no longer constitute "personal information" and would therefore be exempt from verifiable consumer requests to access personal information of consumers.

Return to Table of Contents

## SEC Proposes Heightened Cybersecurity Disclosure Requirements

**The Securities and Exchange Commission (SEC) is proposing new rules relating to public company cybersecurity incident reporting requirements.**

On March 9, 2022, the SEC introduced a cyocused proposal, setting forth new rules that aim to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies."[3] If adopted, public companies will face increasingly comprehensive oversight from the SEC with respect to cybersecurity events and management of such occurrences.

### Overview of Proposed Changes

The SEC's proposal requires that public companies report cybersecurity incidents within four days of their determination that such incident is material through Form 8-K filings. Companies would be tasked with reporting information relevant to investors, including impacts on the business such as business interruptions, extortion, expenses and legal risks, but not technical information regarding the incident (so as to not tip off hackers).

The proposal also contemplates that companies update information provided regarding previously disclosed cyber incidents and disclose, if known by management, when prior cybersecurity breaches previously considered immaterial have amounted to material incidents in the aggregate. The SEC also has introduced a number of disclosure requirements pertaining to a company's internal strategy and governance with respect to cybersecurity risk management.

### Key Takeaways

If the proposed rules are adopted, public companies could expect to be subject to far more granular reporting requirements than previously existed, as part of the SEC's efforts to step up its involvement in the cybersecurity space. In such event, companies may be prudent to adopt protocols or prompt escalation and assessment of cybersecurity incidents in order to comply with these more stringent obligations, especially in the face of increasingly prevalent data breaches and cybersecurity incidents.

Please see the full version of this March 11, 2022, mailing here for more detailed analysis.

Return to Table of Contents

## Ninth Circuit Holds That Insured is Entitled to Coverage Under Commercial Crime Policy for Fraudulent Bank Transfers

**The U.S. Court of Appeals for the Ninth Circuit recently held that property management company Ernst & Haas Mgmt. Co.'s (Ernst & Haas) loss stemming from fraudulent bank transfers was covered under its commercial crime policy issued by insurer Hiscox, Inc. (Hiscox).[4]**

### The Fraudulent Transfers and Ernst & Haas' Insurance Claim

In March 2019, an Ernst & Haas accounts payable clerk received a series of emails from someone the clerk believed to be the company's managing broker directing the clerk to pay several hundred thousand dollars in invoices to a third party via wire transfer. Unbeknownst to the clerk, the emails had been sent by a fraudster who duped the clerk into complying with the first two directives and was sent a wire transfer of $200,000. However, after receiving a third invoice, the clerk became suspicious and contacted the company's actual managing broker to confirm the authenticity of the request, only to discover that she had been duped.

After a failed attempt to retrieve the lost funds, Ernst & Haas submitted a claim under its commercial crime insurance policy that had been issued by Hiscox. As relevant here, the policy provided the following coverages:

- Computer Fraud coverage "for loss of or damage to Money, Securities and/or Other Property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the Premises or Banking Premises: (i) to a person . . . outside those Premises or Banking Premises; or (ii) to a place outside those Premises or Banking Premises"; and

[3] Please view the SEC's "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" here.

[4] *Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc.*, 23 F.4th 1195 (9th Cir. 2022).

- Funds Transfer Fraud coverage "for loss of Money and Securities resulting directly from a Fraudulent Instruction directing a financial institution to transfer, pay or deliver Money and Securities from Your Transfer Account."

Hiscox denied Ernst & Haas' claim. Thereafter, Ernst & Haas filed suit against the insurer in the U.S. District Court for the Central District of California, seeking coverage for the fraudulent transfers. Hiscox moved to dismiss, and the district court granted the motion, reasoning that the loss did not directly result from the fraudulent emails, as required to trigger coverage.[5]

### The Ninth Circuit Reverses the District Court

On appeal, the Ninth Circuit reversed the district court's decision, disagreeing with the narrow reading of the contract language and reliance on what the circuit court found to be an off-point decision with distinguishable facts.

In concluding that the Computer Fraud coverage applied to Ernst & Haas' loss, the Ninth Circuit found that the company suffered a loss resulting "directly" from the fraudulent emails, reasoning that Ernst & Haas "immediately lost its funds when those funds were transferred to [the fraudster] as directed by the fraudulent email[s]," and that "[t]here was no intervening event — [the clerk] acting pursuant to the fraudulent instruction 'directly' caused the loss of the funds." The circuit court found the district court's interpretation of the policy language — which was limited to situations of unauthorized computer use or hacking — to be overly restrictive, noting that it improperly "eliminates the possibility of coverage *whenever* an employee is defrauded into taking an action."

The Ninth Circuit also held that the Funds Transfer Fraud coverage applied to the loss, rejecting the district court's conclusion that the coverage was inapplicable because the fraudster instructed the clerk — rather than the bank — to transfer the money. The court concluded that "the sole purpose of [the fraudulent email] was to instruct [the clerk] to initiate a wire," and thus the email should be considered a direct instruction to the bank.

### Key Takeaways

The Ninth Circuit's ruling serves as an example of the differing approaches taken by courts in analyzing coverage for "cyber"-type losses under traditional crime insurance policies. While some courts have adopted a narrower interpretation of what it means for a loss directly resulting from the use of a computer or a fraudulent instruction, the *Ernst & Haas* court employed a broader interpretation in concluding that the fraudulent transfer loss in this case resulted directly from the use of a computer and directly from a fraudulent instruction. Given the increased frequency and severity of cyberattacks, this decision also serves as an important reminder to insurers and insureds alike to clearly set forth in insurance policies the terms and conditions of coverage for fraudulent transfers and other cyber events.

Return to Table of Contents

## Minnesota District Court Holds That Insurers Owe Coverage Under General Liability Insurance Policies Following 2013 Target Data Breach

**On March 22, 2022, the U.S. District Court for the District of Minnesota held that Target Corp. (Target) is entitled to coverage under commercial general liability insurance policies issued by two Chubb insurers, Ace American Insurance Co. and Ace Property & Casualty Insurance Co. (ACE), for bank settlements reached in connection with a 2013 data breach suffered by Target.[6]**

### The Data Breach and Target's Insurance Claim

In December 2013, Target discovered that a hacker breached the company's computer network and stole the payment card data and personal information of customers with Target payment cards. Since the data breach compromised the payment cards, the banks that issued the had to cancel and issue new cards, incurring costs in doing so. The banks then sued Target to recover those costs and the company resolved the banks' claims through settlements.

Target sought indemnification for the bank settlements from ACE under commercial general liability insurance policies that ACE issued to Target (collectively, the policies). As relevant in this matter, the policies provided coverage for losses resulting from "property damage," which was defined to include "the loss of use of tangible property that is not physically injured." After ACE denied coverage under the policies for the bank settlements, Target filed suit against ACE in the District of Minnesota for breach of contract and declaratory relief.

### The District Court's Initial Decision in Favor of ACE

On February 8, 2021, the district court granted ACE's motion for summary judgment and denied Target's motion for partial summary judgment, holding that Target failed to establish that

[5] *Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc*, No. CV-20-04062-AB (PVCx), 2020 WL 6789095 (C.D. Cal. Nov. 5, 2020).

[6] *Target Corp. v. ACE Am. Ins. Co. et al.*, No. 0:19-cv-02916 (WMW/DTS), 2022 WL 848095 (D. Minn. Mar. 22, 2022).

the bank settlements were due to a "loss of use of tangible property" as required under the policies.[7] The court reasoned that Target failed to introduce evidence as to the value of the use of the payment cards. Without this evidence, "Target has not established a connection between the damages incurred for settling claims related to replacing the payment cards and the value of the use of those cards," the court found.

### The District Court's Subsequent Decision in Favor of Target

Target subsequently moved to alter or amend the court's judgment pursuant to Federal Rule of Civil Procedure 59(e), contending that the court erred as a matter of law in its February 8, 2021, ruling. In considering Target's motion, the court noted that "[n]either party has presented controlling legal authority squarely addressing whether loss of use includes the inoperability of payment cards following a data breach." However, the court ultimately concluded that the data breach caused a "loss of use" because the compromised cards were inoperable after the banks canceled them. Additionally, "[t]he expense that Target incurred to settle claims brought by the Issuing Banks for the costs of replacing the compromised payment cards was a cost incurred due to the loss of use of the payment cards," the court reasoned. The court therefore vacated its earlier decision, denied ACE's motion for summary judgment and granted Target's motion for partial summary judgment.

### Key Takeaways

It is expected that other courts and litigants may look to this decision as precedent for interpreting the meaning of "loss of use" in the context of coverage for loss resulting from the inoperability of payment cards following a data breach. However, given the contractual nature of the relationship between the policyholder and insurer, as well as the varying and unpredictable case law concerning coverage for data breaches, it also is important for policyholders and insurers to review their insurance policy language when evaluating coverage and potential liability for cyber events.

Return to Table of Contents

[7] *Target Corp. v. ACE Am. Ins. Co. et al.*, No. 0:19-cv-02916, 517 F. Supp. 3d 798 (D. Minn. Feb. 8, 2021).

## European Commission Publishes Proposed Data Act, Potentially Allowing for Enhanced Access and Use of Data Generated by Connected Products

**On February 23, 2022, the European Commission (EC) published its Proposal for a Regulation on harmonized rules on fair access to and use of data (the Data Act or act). While the Data Act is still in the initial stages of the EU legislative process, as drafted it would grant enhanced rights to business and consumer "users" in relation to data generated by connected devices, defined as physical products that can connect with (i) other physical devices, and (ii) other systems, via the internet. This act represents the second deliverable in the European Strategy for Data and aims to promote a freer and fairer market for data sharing by businesses, with a particular focus on market access for small- and medium-sized enterprises (SMEs). If adopted, the Proposal is likely to come into force by mid-2024.**

### Background and Scope of Application

The EC has previously noted that the potential opportunities derived from the commercialization and sharing of data are being stifled by access and use barriers. While manufacturers often ensure that they retain ownership of the data generated by their products, the Data Act would allow for other stakeholders to have the opportunity to create value from that data, while also compensating manufacturers for third-party access. Unlike the GDPR, the Data Act would apply to all data, not merely personal data, and is aimed at creating a single, open market for data sharing in Europe.

### Key Provisions

The Data Act would grant rights to a "user" (a natural or legal person (*e.g.*, individual customers, other businesses and the government)) who generates data through their use of "products" (a movable item that generates or collects data concerning its use and is connected to the internet). Notable provisions of the act include:

- **B2C and B2B data sharing.** The act would grant users rights regarding the data generated when they use a connected device, including (i) the right to access the data collected (either directly through the product itself or through a request to the data holder, which includes entities such as the manufacturer), and (ii) the right to authorize the data holder to port data to a third party. The act would impose obligations on manufacturers to ensure that products are designed in such a way that data is easy to access and port. In addition to affording users

greater transparency and control, these provisions also would allow for seamless access to data-driven service providers or aftermarket sales (*e.g.*, a person desires car enhancement services from a different manufacturer who can access relevant data to create and install bespoke car parts). Chapter II of the act also would place restrictions on data holders, who would be prohibited from using the data to derive insights about a user's economic situation or assets, to the extent that such access could undermine the user's market power.

- **Obligations for data holders and data sharing agreements.** The proposed act also details the obligations imposed on data holders and the rules applicable to a business-to-business relationship. If, under the Data Act, a data holder was obliged to make data available to a recipient (for example, if a user requested their data be ported to a third party), Chapters III and IV provide the legal framework for this transfer. Importantly, data holders and recipients would have to enter into a data sharing agreement and the EC has committed to developing nonbinding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations. Generally, any conditions under which data is provided must be fair and non-discriminatory, any compensation for the data must be reasonable, and any compensation provided by SMEs cannot exceed the costs incurred by the data holder to provide access. Member states also would be required to establish dispute settlement bodies in the event of disputes arising from data sharing agreements.
- **Making data available to public bodies.** The act would provide for public access to data held by businesses in times of exceptional need (*e.g.*, accessing aggregated and anonymized location data from mobile network operators during a pandemic). Where public bodies require data to respond effectively to public emergencies, the act also would require the data to be made available by data holders at no cost. Requests from public bodies must be proportionate, and competent authorities would be responsible for ensuring all requests are transparent and publicly available, and for responding to complaints.
- **Switching between data processing services and non-personal data transfers.** Chapters VI, VII and VIII would impose obligations on service providers that enable remote access to a pool of shareable computing resources (*e.g.*, cloud and edge services). Under Chapters VI and VII, these providers would be obliged to make it easy to switch to alternative providers (including through the elimination of technical and commercial constraints) and to restrict access to users' non-personal data to recipients outside the EU. Chapter VIII also would impose obligations on data processing services to ensure their data sharing mechanisms and services are interoperable to allow their customers to switch seamlessly between cloud environments.
- **Clarity on Database Rights.** The act clarifies the framework of EU law that regulates rights in databases. The Database Directive, introduced in 1998, effectively created the possibility of two distinct intellectual property rights in a database: (i) the structure of the database, which is protected by copyright, and (ii) the *sui generis* database right, which protects the contents of the database. A principle emerged in the case law that followed, however, to suggest that intellectual property rights protect the collection of data but not its creation. Therefore, it was unclear whether the *sui generis* right applied to data generated by users of connected products. Chapter X of the Data Act aims to resolve this uncertainty, and states that the *sui generis* database right does not protect the contents of databases generated through use of connected devices and services.

### Key Takeaways

The potential benefits of the Data Act's increased data accessibility are clear, but businesses and their customers will have to ensure that the confidentiality of their information and trade secrets is not lost. As such, we anticipate large manufacturers will invest in more robust data security frameworks. While manufacturers are compensated under the act, it will be interesting to see how they process the potentially high volume of requests for data access and portability alongside their day-to-day business operations. As more SMEs and customers utilize these rights, larger businesses may have to employ dedicated staff to manage these processes.

The territorial scope of the Data Act will be recognizable to those familiar with the GDPR, as the Data Act similarly affords protection to users and data recipients in the EU, users of products that have been placed in the EU or any data held in the EU, and the location of the product manufacturer or data holder will not determine the act's application. It is therefore in the interest of entities outside the EU to consider whether they need to apply the Data Act to its operations.

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