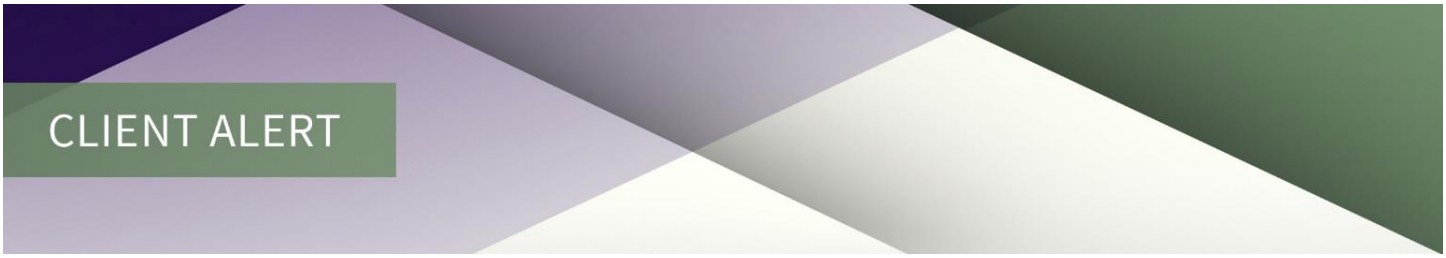

Noteworthy Two Weeks in Privacy

March 28, 2022

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Richard M. Borden | Stefan Ducich
Nicholas Chanin | Amelia Putnam

The last two weeks have brought several notable developments in quick succession in the world of privacy and data security. First, on March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act (the "Cyber Reporting Act") as part of a much larger omnibus appropriations bill. Then, on March 21, 2022, two new transfer tools in the United Kingdom ("UK") came into force. Then, on March 24, 2022, in the United States, Governor Spencer Cox signed the Utah Consumer Privacy Act ("UCPA") into law. Finally, on March 25, 2022, the U.S. and EU Commission announced a preliminary agreement on a new data transfer framework to replace the EU-U.S. Privacy Shield (the "Framework"), which was invalidated by the Court of Justice of the European Union's ("CJEU") *Schrems II* decision in July 2020.

Taken together, these developments underscore the increasingly dynamic and complex nature of the regulatory environment that companies must navigate.

Cyber Reporting Obligations in the United States

The Cyber Reporting Act establishes new reporting requirements for entities dealing with cyber incidents affecting critical infrastructure. Of note, the Cyber Reporting Act delegates rulemaking authority to the Director of the Cybersecurity and Infrastructure Security Agency ("CISA") to determine which incidents are substantial cyber incidents covered by the Cyber Reporting Act.

The various reporting mechanisms established by the Cyber Reporting Act include:

- Mandatory Reporting. The Cyber Reporting Act establishes required reporting to CISA within 72 hours after a covered entity reasonably believes that a covered cyber incident has occurred.

- Ransomware Payments. A covered entity must report to CISA within 24 hours of making a ransom payment, even if the ransomware attack does not otherwise qualify as a covered cyber incident.

- Voluntary Reporting. Covered entities may voluntarily report or provide information to CISA about incidents or payments that otherwise would not be required to be reported in order to enhance the government's situational awareness of cyber threats.

- Supplemental Reporting. Covered entities must promptly submit supplemental reports if substantially new or different information becomes available or if the covered entity makes a ransom payment after submitting an initial report. A covered entity has an obligation to update or supplement submitted reports until such date that it notifies CISA that the covered cyber incident has concluded and has been fully mitigated and resolved.

Of particular note is the significant rulemaking authority delegated to CISA. CISA is required to implement the requirements of the Cyber Reporting Act via rules adopted within 42 months of enactment. Among other things, the final rule must address the types of entities and cyber incidents covered by the Cyber Reporting Act, the specific contents for the reports disclosing cyber incidents, the types of data to be preserved, the deadlines to submit supplemental reports, and procedures to submit reports.

The Cyber Reporting Act includes a number of protections for companies to submit reports, as well as provisions creating a Cyber Incident Reporting Council to coordinate, deconflict, and harmonize federal incident reporting requirements, and a ransomware vulnerability warning pilot program that is intended to develop processes and procedures for identifying information systems that contain security vulnerabilities and notifying owners of such information systems. But the new cyber reporting requirements are the key legal change that will directly affect companies in the critical infrastructure space and may serve as a model for broader reform of breach notification requirements.

Data Transfers: A Step towards Greater Certainty?

The Trans-Atlantic Data Privacy Framework (EU-U.S.)

The invalidation by the CJEU of the EU-U.S. Privacy Shield in July 2020 cast significant doubt over the legality of most data transfers from the European Union to the United States under the General Data Protection Regulation ("GDPR"). In the interim, the European Commission has issued new standard contractual clauses (the "EU SCCs") and guidance to ensure European personal data is protected at essentially equivalent levels in third countries (including the United States)

as under EU law. These have resulted in new requirements and significant efforts by affected companies to ensure compliance with GDPR.

Almost two years later, U.S. and EU negotiators have now come to an agreement in principle on a new Framework, which seeks to "reestablish an important legal mechanism for transfers of EU personal data to the United States,"[1] address deficiencies identified by the CJEU in *Schrems II*, and with it, return a level of certainty around the legality of such transfers. Specific language has not yet been released, but the White House confirmed commitments to:

- "Strengthen the privacy and civil liberties safeguards governing U.S. signals intelligence activities;"[2]
- "Establish a new redress mechanism with independent and binding authority;"[3] and
- "Enhance its existing rigorous and layered oversight of signals intelligence activities."[4]

New UK Data Transfer Tools

Following Brexit, the UK Parliament—in consultation with the UK Information Commissioner's Office—issued final versions in February 2022 of two new, UK-specific data transfer tools: the UK International Data Transfer Agreement ("IDTA"), and a UK addendum to the new EU SCCs (the "UK Addendum" and together with IDTA, the "New UK Transfer Tools").[5]

The New UK Transfer Tools entered into force on March 21, 2022, and are now lawful transfer mechanisms under GDPR as applied in the UK. Similar to the EU SCCs, the New UK Transfer Tools provide for a transition period: all new contracts governing UK data transfers must use the New UK Transfer Tools within six (6) months of the effective date, and all existing contracts (assuming no change in processing) may continue to rely on the EU SCCs (as preserved in UK law following Brexit) for 24 months following the effective date. Thereafter, all contracts governing UK data transfers must be based on the New UK Transfer Tools.

1 Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework here.

2 *Id.*

3 *Id.*

4 *Id.*

5 *See* ICO International Data Transfer Agreement and Guidance here.

	EU SCCs *Implementation Date*	*New UK Transfer Tools* *Implementation Date*
New Contracts	September 26, 2021	**September 21, 2022**
Existing Contracts	December 27, 2022	**March 21, 2024**

Not later than the implementation dates above, companies transferring data from the UK must use one of the New UK Transfer Tools. The IDTA is comparable to the EU SCCs in that both require risk assessments to ensure appropriate protection of personal data. However, the IDTA does not distinguish by the transfer relationship (e.g., controller-controller, controller-processor) as with the EU SCCs, and unlike the EU SCCs, the IDTA allows for arbitration as a dispute resolution mechanism. Alternatively, the UK Addendum supplements transfer agreements that are based on the new EU SCCs with respect to choice of law, and clarifying that the UK Addendum prevails if it is in conflict with the EU SCCs.

Utah Joins the Fray

The Utah Consumer Privacy Act[6]

Utah's Governor Spencer Cox, signed the UCPA into law on March 22, 2022, making Utah the fourth state (after California, Virginia, and Colorado) to adopt a comprehensive consumer privacy law. The UCPA, which will go into effect on **December 31, 2023**, generally follows the examples of those previous laws. For instance, it requires covered entities (called "controllers" as in Virginia, Colorado, and Europe) to disclose their practices in a publicly available privacy notice, and provides consumers the rights of access, deletion, data portability, and the right to opt out of certain types of data processing. The UCPA also requires that controllers and third-party processors execute a contract that details the instructions and limits for processing personal data on behalf of the controller, and that obligates the processor to provide reasonable assistance to the controller in discharging its duties under the UCPA. However, the UCPA does not provide a right to correct personal data, and the right to opt out is limited to targeted advertising and the sale of personal data. Additionally, the law has a somewhat narrower scope than previous state laws, and is applicable only to businesses that both meet a certain revenue threshold ($25 million) and certain personal data processing levels, rather than one or the other. Finally, the UCPA does not include a private right of action, and is enforceable only by the Utah Attorney General.

[6] Utah Senate Bill 227, "Utah Consumer Privacy Act" available [here] (last accessed March 25, 2022).

Thus, while largely similar to the other state-level privacy laws that preceded it, Utah seems to be striking a somewhat more business-friendly tone that we expect may be adopted by other Republican-led states.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Stefan Ducich
202 303 1168
sducich@willkie.com

Nicholas Chanin
202 303 1164
nchanin@willkie.com

Amelia Putnam
202 303 1089
aputnam@willkie.com