March 2023

Skadden

Privacy & Cybersecurity Update

Iowa Becomes Sixth State To Enact Consumer Privacy Law

On March 28, 2023, Iowa became the sixth state to enact a consumer privacy law when The Act Relating to Consumer Data Protection was signed by the state's governor.[1] While this means there is yet another state with a privacy law that companies must comply with, the Iowa law closely tracks those passed in Virginia and Utah, and should impose few new obligations on companies already complying with the laws of those states. The Iowa law is set to go into effect in January 2025.

Scope of Coverage

As with the other five states that have enacted privacy laws, the Iowa law applies to companies based in the state as well as to the treatment of personal data of residents of that state, regardless of where the company is located. The law does not apply to employee data or data collected through business-to-business contacts, meaning California remains the only state that has included those groups in privacy laws.

The law applies to organizations that control or process personal data of at least 100,000 Iowa consumers in a calendar year, or that derives more than 50% of its gross revenue from the sale of personal data and controls or processes personal data of at least 25,000 Iowa consumers. There is no "revenue" threshold as there is in some other states, although nonprofits are exempt.

Consumer Rights

Iowa residents will be protected with four of the basic rights that have been included in other state privacy laws: the right to access personal data, the right to obtain a portable copy of personal data, the right to delete personal data (although limited to data collected from the consumer) and the right to opt out of the sale of personal data (as in California and Utah). As with Utah's law, consumers do not have a right to correct erroneous data. In addition, there is no requirement to have separate opt-out page or to honor a consumer's browser setting, each of which is required in the laws in California, Colorado and Connecticut.

The Iowa law does not require an opt-in choice for the processing of sensitive personal data (as required in Colorado, Connecticut and Virginia).

[1] The others are California, Colorado, Connecticut, Utah and Virginia.

Organizations need to respond to consumer requests within 90 days, which is a longer period than the 45 days required by the other states' laws. Organizations also can extend the 90-day period by 45 days when reasonably necessary, depending on the complexity and number of requests.

Internal Compliance

Compared to the other states' laws, Iowa's version imposes fewer requirements on organizations with respect to how they manage personal data. For example, there is no obligation to disclose data retention periods, to minimize data usage or to conduct a data privacy impact assessment.

Privacy Notices

Data controllers must provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes the categories of personal data being processed, the purpose for processing, how consumers may appeal a controller's decision, the categories of personal data shared with third parties and the categories of such third parties.

Third-Party Contracts

Data controllers are required to have a contract with their data processors that specifies processing instructions, including the nature and purpose of the processing, its duration and the obligations of each party. That contract also must specify appropriate processes for the retention, deletion and access of the data.

No Private Right of Action

The Iowa law does not provide a private right of action and violations are only enforceable by the state attorney general, with fines up to $7,500 per violation. There also is a 90-day cure period for violations, longer than that offered by any other state (California has entirely eliminated any cure period).

Key Takeaways

With Iowa becoming another state with its own set of privacy rules, companies must continue to monitor whether further laws will impact their operations. Though this law tracks in line with other states, future laws may provide more complex rules and affect how organizations conduct business. We will provide updates should further laws be passed.

Return to Table of Contents

Biden Administration Announces New National Cybersecurity Strategy

On March 1, 2023, President Joe Biden issued a new national cybersecurity strategy seeking to bolster the country's approach toward cyberthreats and align business incentives to favor long-term investments in cybersecurity. The new strategy calls for accountability for owners and operators of systems that maintain personal data or fail to take reasonable precautions in developing software. It also seeks to strengthen the security of the systems and assets that make up U.S. critical infrastructure and increase many areas of federal coordination and public-private collaboration.[2]

Background

Since the release of the 2008 Comprehensive National Cybersecurity Initiative, previous presidents have enacted various national strategies and executive orders focused on cybersecurity, particularly surrounding critical infrastructure of the country. The Biden administration's new National Cybersecurity Strategy replaces the Trump administration's 2018 National Cyber Strategy while continuing the momentum of its priorities through five pillars: (i) Defend Critical Infrastructure, (ii) Disrupt and Dismantle Threat Actors, (iii) Shape Market Forces To Drive Security and Resilience, (iv) Invest in the Resilient Future and (v) Forge International Partnerships To Pursue Shared Goals.

We outline each of these pillars below.

Defend Critical Infrastructure

Through several initiatives, this first pillar addresses concerns that damage to U.S. critical infrastructure may disrupt essential services provided to the American public. First, the strategy seeks to implement new regulations based on existing cybersecurity frameworks to set necessary cybersecurity requirements in critical sectors. It also seeks to ensure new and existing regulations are harmonized and streamlined to minimize the cost and burden of compliance. Second, the administration will look to take steps to improve public-private collaboration for information sharing and proactive and coordinated defensive efforts.

The strategy also focuses on several federal government improvements, including integrating federal cybersecurity centers to drive coordination, updating federal incident response plans and procedures, and modernizing federal defense systems. One key aspect in this area for critical infrastructure companies is the

[2] See the full text of the press release by the White House, including a link to the full text of the National Cybersecurity Strategy.

upcoming rulemaking and implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which requires rapid reporting of covered cyber incidents to the Cybersecurity and Infrastructure Security Agency. Initial implementing regulations must be published by March 2024.

Disrupt and Dismantle Threat Actors

The second pillar focuses on disabling avenues for malicious actors to mount sustained cyber-enabled campaigns that would threaten U.S. national security or public safety. First, the administration is looking to increase federal government coordination for "defending forward" and disrupting online criminal infrastructure and resources, including updating the Department of Defense's National Security Strategy and National Defense Strategy. As with the first pillar, the administration also is encouraging more operational public-private collaboration, including via quicker identification of malicious uses of U.S.-based infrastructure and increasing the speed and scale of cyber threat intelligence sharing with cyber defenders and victims when the government receives information that may impact such entities. Furthering its ongoing efforts, including convening the Counter-Ransomware Initiative, the strategy will focus on combating ransomware, particularly by exploring effective ways to prevent malicious parties from profiting from such attacks.

Shape Market Forces to Drive Security and Resilience

The third pillar focuses on areas that will likely be some of the most difficult to implement, but which could have widespread effects as a result of shifting some risk responsibility to different market actors. For example, the strategy contemplates setting national requirements to secure personal data consistent with standards and guidelines developed by the National Institute of Standards and Technology (NIST). It also considers working to develop legislation that would impose liability (which could not be disclaimed by contract) on software developers that fail to take reasonable precautions to secure their software or that distribute software with known vulnerabilities. The strategy seems to recognize that any such legislation should include safe harbors, which would draw from current best practices, and cites the NIST Secure Software Development Framework as an example. Moreover, for entities that contract with the federal government, the strategy signals that the administration intends to monitor and enforce the cybersecurity obligations created under such contracts. Finally, the administration is exploring the need for, and feasibility of, a federal insurance response to catastrophic cyber events that would support the existing cyber insurance market.

Invest in the Resilient Future

The fourth pillar addresses the need for cybersecurity research and development. The administration targets investing in frameworks to strengthen the technical foundations of the digital ecosystem, focusing on improving U.S. leadership in computing-related technologies, including microelectronics, quantum information systems and artificial intelligence; biotechnologies and biomanufacturing; and clean energy. The strategy also calls for federal efforts to prioritize research and development in cybersecurity; prepare for a timely transition of hardware, software and services that could be easily compromised by quantum computing; develop digital identify solutions; and strengthen the nation's cyber workforce.

Forge International Partnerships To Pursue Shared Goals

The fifth and final pillar of the strategy focuses on developing international relationships to strengthen the global digital ecosystem. It proposes utilizing coalitions focused on cybersecurity priorities to increase cybercrime cooperation and advance U.S. foreign policy and cybersecurity goals. It also proposes policies and efforts to strengthen allies' and partners' cybersecurity postures for critical infrastructure, incident response and data sharing, as well as regarding the deployment of U.S. resources to assist these countries.

Key Takeaways

The new strategy significantly increases the administration's focus on both collaborations and public-private partnerships as compared to presidential administrations' prior strategies. The Biden administration's strategy also builds upon many existing policy elements or initiatives in development through prior policy changes and executive orders. However, the strategy also highlights "fundamental changes to the underlying dynamics of the digital ecosystem," some of which will require new laws and regulations that, if enacted, could significantly impact how companies view cybersecurity. Whether through requiring cybersecurity actors to implement new controls and measures to align with minimum cybersecurity requirements or by subjecting cybersecurity actors to potential liability for failing to develop and distribute secure software, companies will need to closely monitor implementation of the National Cybersecurity Strategy.

Return to Table of Contents

UK Government Publishes Revised Proposals To Amend Data Protection Regime

On March 8, 2023, the U.K. government published the Data Protection and Digital Information (No. 2) Bill. This follows the July 2022 publication of the Data Protection and Digital Information Bill and the U.K. government's withdrawal of that original bill in September 2022 in connection with the election of newly installed U.K. Prime Minister Liz Truss. We previously discussed the measures included in the consultation to the original bill, and this new bill includes many of the measures envisaged in that consultation.

The second iteration of the bill includes a range of measures designed to simplify data protection compliance obligations for organizations. U.K. Innovation and Technology Secretary Michelle Donelan said when she introduced the bill that it would make the UK's data protection regime "easier to understand [and] easier to comply with." While some provisions of the bill may require organizations to modify their data protection compliance program, some key elements, including changes to the international transfers regime and a new "recognised legitimate interest" legal basis for processing, have been designed with the aim of enabling organizations that are compliant with the U.K. General Data Protection Regulation (U.K. GDPR) today to stay compliant with the revised regime without being required to make material and costly changes.

Key Changes

Some key changes outlined in the bill that are likely to be relevant to organizations that conduct data processing activities subject to the U.K. GDPR include:

- **The introduction of a "recognised legitimate interest" basis for processing, with potential for the U.K. government to expand this list in the future.** The list of processing activities currently designated as recognized legitimate interests in the bill are those necessary for (i) the purposes of direct marketing, (ii) the intra-group transmission of personal data necessary for internal administrative purposes and (iii) ensuring the security of network and information systems. An organization will be able to rely on this legal basis for processing, but must still consider the balance of the organization's interests in processing such personal data against the rights and interests of the relevant data subjects by undertaking a legitimate interest assessment.
- **Restrictions on automated decision-making are loosened and the scope of provisions relating to automated decision-making is redrawn to apply to processing where "no meaningful human involvement" is present.** The bill amends the current prohibition on automated decision-making involving any personal data (unless certain conditions are met), limiting this prohibition to automated decision-making relating to special category personal data only. Automated decision-making that does not relate to special category personal data can be used in connection with any legal basis for processing (subject to data subject safeguards materially unchanged from those under the U.K. GDPR), other than the recognized legitimate interest basis described above. The bill also requires organizations to consider the extent to which a decision has been taken on the basis of profiling when establishing whether or not human involvement has been meaningful in a decision (and therefore determining whether automated decision-making has occurred). These provisions, along with the recent publication of the U.K. government's artificial intelligence (AI) white paper, highlight the government's aim to develop a clearer regulatory framework in which innovative AI technologies can operate, including a continued focus on transparency, accountability and the ability for outcomes generated by AI to be contested.
- **The removal of the requirement for organizations to keep records of processing activities, apart from high-risk processing activities.** High-risk processing is defined as processing that — taking into account the nature, scope, context and purposes of the processing — is likely to result in a significant amount of risk to the rights and freedoms of individuals. This is a marked relaxation compared to the current regime under the U.K. GDPR, which requires all organizations that employ 250 or more people to maintain records of all processing activities. However, organizations operating in both the U.K. and the European Economic Area (EEA) should be aware that they will still be required to keep records of processing activities for their EEA operations, which will require the inclusion of any data flows to/from their U.K. business. Therefore, this relaxation is likely to provide limited benefit, if any, to such businesses unless a U.K. and EEA business conducts separate and distinct processing activities.
- **A new, go-forward regime for international transfers.** The test applied by the U.K. government when considering whether a transfer is an "approved" transfer to a third country (replacing the previous label of an adequacy decision) is that the standard provided for data subjects with regard to general processing of data in the third country should not be "materially lower" than the standard provided for data subjects with regard to general processing of data in the U.K. The new regime also gives the U.K. government flexibility to designate transfers to certain international organizations, sectors, regions or recipients, or transfers of certain types of data or for certain purposes, as approved transfers. When a transfer has been designated as an "approved" transfer, organizations will not require any further authorization to make such a transfer that is compliant under the U.K. GDPR. Importantly, the bill also confirms that international transfers made in compliance with the U.K. GDPR today (such as use of the applicable EU Standard Contractual Clauses (SCCs) together with the U.K. Addendum to the EU SCCs, or use of the U.K. Intra-group Data Transfer Agreement) under Article 46 of the U.K. GDPR will still be recognized as compliant after the bill comes into force, and organizations' arrangements will not need to be updated.
- **The replacement of the role of data protection officer (DPO) with a senior responsible individual (SRI).** Public bodies and organizations that carry out high-risk processing activities must designate a senior member of its management team as an SRI responsible for data protection compliance to be responsible for certain specified activities. While the SRI will be able to delegate performance of the activities required of them, in particular they will be required to delegate any such activity if performing the activity would present a conflict of interests with their senior

management role. Organizations will need to consider whether an individual currently appointed as DPO can act as their SRI, or whether the SRI can delegate performance of specified activities to the DPO individual.

- **A relaxation on cookies.** The bill creates an exception to the consent requirements with respect to nonessential cookies on websites. The use of cookies for statistical purposes with a view to understanding how a website is used and make improvements to that website will no longer require the user's consent. However, under the new rules, users must still have the option to object to such cookies. The U.K. government has stated that the bill aims to "reduce the number of consent pop-ups people see online."

Key Takeaways

While not a radical overhaul of the U.K.'s data protection regime, the bill does propose measures that will affect organizations' day-to-day compliance obligations. The U.K. government has confirmed that the bill is designed "ensure data adequacy," but as the measure progresses through the U.K.'s legislative process, we will gain clarity on how closely aligned the U.K.'s data protection regime will stay to the U.K. GDPR and whether the U.K. can retain its adequacy decision under Article 45 of the GDPR.

The bill, which is not anticipated to come into force until late in 2023, will continue to be scrutinized in the U.K. Parliament and substantive amendments are possible during this process.

Return to Table of Contents

New Jersey District Court Denies Insurer's Motion To Dismiss In Coverage Action Stemming From Fraudulent Transfer Loss

The U.S. District Court for the District of New Jersey denied a motion to dismiss by Federal Insurance Company (Federal) in a lawsuit filed by its insured, plastics manufacturer Montachem International, Inc. (Montachem), seeking coverage under its crime insurance policy for an approximately $200,000 loss arising from a fraudulent transfer.[3]

The Alleged Fraudulent Transfer

According to the complaint, between December 2019 and January 2020, a hacker gained unauthorized access to the email account of a Montachem employee and used that account to trick one of the company's customers into making a perceived invoice payment in the amount of approximately $200,000 to the hacker's bank account. The complaint further alleges that in March 2020, after not receiving payment from the customer, Montachem conducted an investigation and learned that it had fallen victim to a hacking incident. The company was unable to recover the fraudulently transferred funds.

Montachem's Insurance Claim

Shortly thereafter, Montachem sought coverage for the funds from Federal under the crime coverage part of its package insurance policy, which provided computer fraud coverage. As relevant here, pursuant to the policy's Ownership clause, such coverage applied only to "*money . . . owned by [Montachem] or for which [Montachem] is legally liable, or held by [Montachem] in any capacity whether or not [Montachem] is liable.*" Citing the Ownership clause, Federal denied coverage, contending that Montachem did not own or hold the funds — stating instead that the customer owned or held the funds — and that Montachem was not legally liable for the funds.

The Coverage Action and Denial of Federal's Motion to Dismiss

Montachem subsequently sued Federal in the U.S. District Court for the District of New Jersey seeking coverage for the loss. Federal moved to dismiss, arguing that the complaint concedes that the funds were not "held" by Montachem given that the complaint alleges that the customer, and not Montachem, transferred the funds, and "the Complaint has not, and cannot, plead that Montachem either 'owned' or 'was legally liable for' the funds," as required to satisfy the policy's Ownership clause. Montachem argued in opposition that under the Ownership clause, the funds could be "held by [Montachem] *in any capacity*," and the company held the funds in its capacity as a holder of an accounts receivable for the invoiced customer. The court agreed with Montachem, noting that "the Complaint does allege, if indirectly, that [Montachem] has 'ownership over the accounts receivable for the invoiced customer,'" which satisfies the Ownership clause. The court therefore denied Federal's motion to dismiss.

Key Takeaways

While the district court found that Montachem's complaint satisfied the liberal pleading standard under the Federal Rules of Civil Procedure, it remains to be seen whether the company ultimately will prevail on coverage. Regardless of the outcome, this decision serves as another important reminder to policyholders and insurers to review their insurance policies to determine the scope of coverage provided for fraudulent transfer losses and other cyber incidents.

Return to Table of Contents

[3] The decision is *Montachem International, Inc. v. Fed. Ins. Co.*, No. 3:20-cv-20100 (D. N.J. Mar. 8, 2023) (ECF No. 18).

Michigan Appellate Court Finds No Coverage Under General Liability Policy for TCPA 'Junk Fax' Suit

A Michigan intermediate appellate court has affirmed a lower court's decision that the Hartford Casualty Insurance Company (Hartford) does not owe coverage under a business liability insurance policy issued to residential mortgage provider Top Flite Financial (Top Flite) for a class action settlement stemming from alleged violations of the Telephone Consumer Protection Act (TCPA).[4]

The Underlying TCPA Class Action and Settlement

In March 2006, Top Flite commenced an advertising campaign in which a third-party vendor sent unsolicited fax advertisements to over 4,000 U.S. companies, including Bridging Communities and Gamble Plumbing & Heating, Inc. (collectively, the plaintiffs). In December 2009, the plaintiffs filed a putative class action against Top Flite in Michigan federal court alleging that Top Flite violated the TCPA by sending the plaintiffs and a class of similarly situated persons and businesses unsolicited fax advertisements without their consent.

In May 2019, following a court-approved class action settlement, the plaintiffs were awarded a judgment in the amount of over $2.1 million against Top Flite. The plaintiffs collected $257,000 from Top Flite and then received an assignment of rights to sue Top Flite's insurer, Hartford, for the remaining award amount.

Hartford's Denial of Coverage

In 2012, when the class action was pending, Top Flite had sought coverage for the class action under its commercial business insurance policy issued by Hartford, which denied coverage. As relevant here, the policy provided liability coverage for (i) "property damage" caused by an "occurrence" during the policy period, subject to an exclusion for any such damage "expected or intended from the standpoint of the insured" and (ii) "personal and advertising injury" caused by an offense arising out of the insured's business during the policy period, subject to an exclusion for any such injury "[a]rising out of the violation of a person's right of privacy created by any state or federal act" (subject to exceptions).

Plaintiffs' Coverage Action Against Hartford

In July 2019, shortly after the class action settlement, the plaintiffs filed suit in Michigan state court against Hartford seeking coverage for the unsatisfied portion of the judgment against Top Flite. The parties subsequently cross-moved for summary disposition. The court sided with Hartford, finding that there was no coverage under the policy because: (i) the "expected or intended injury" exclusion barred coverage under the "property damage" coverage part; and (ii) although Top Flite's unsolicited advertising constituted an advertising injury, the "statutory right of privacy" exclusion nevertheless barred coverage under the "personal and advertising injury" coverage part.

On appeal, the Michigan Court of Appeals (Wayne Circuit Court) affirmed the lower court's decision. With respect to the "personal and advertising injury" coverage part, the court held that the class action arose out of alleged violations of the plaintiffs' right of privacy created by the TCPA, thereby bringing the class action within the "statutory right of privacy" exclusion. The court rejected the plaintiffs' argument that the class action fell within an exception to the exclusion for "liability for damages that the insured would have in the absence of such state or federal act" because the class action only alleged TCPA violations, and therefore "Top Flite would not have been liable in the absence of the TCPA."

Turning to the "property damage" coverage part, the court observed that coverage "hinges on whether the property damage alleged by plaintiffs was caused by an 'occurrence,' which the policy defines as an 'accident.'" The court concluded that it was not an occurrence "because the events giving rise to this action were in their entirety the specific and intentional result of plaintiffs' specific and intentional business strategy and plan, the events could not and do not meet the definition of an 'occurrence' covered under the policy." The court further held that even if Top Flite's conduct constituted an "occurrence," the "expected or intended injury" exclusion barred coverage.

Key Takeaways

As the court's decision in *Bridging Communities* illustrates, TCPA claims may not fit neatly into coverage. However, given the increased frequency of TCPA lawsuits in recent years and the potentially significant costs associated therewith, policyholders should nonetheless consider all coverage lines that may respond to such claims, including, for example, general liability, cyber, errors and omissions liability, and directors and officers liability. In addition, policyholders faced with TCPA exposure would be well-advised to proactively ensure that their insurance carriers, brokers and advisers are offering most favorable coverage possible and understand the scope of coverage before a claim arises.

Return to Table of Contents

[4] The decision is *Bridging Communities, Inc. v. Hartford Casualty Insurance Co.*, No. 355955, 2023 WL 2334582 (Mich. Ct. App. Mar. 2, 2023).

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

Avia M. Dunn
Partner / Washington, D.C.
202.371.7174
avia.dunn@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

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@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

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@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

Nicole L. Grimm
Counsel / Washington, D.C.
202.371.7834
nicole.grimm@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