Skadden

Privacy & Cybersecurity Update

1 European Parliament Panel Releases Report on Blockchain and the GDPR

7 First Monetary Settlement in a False Claims Act Case Involving Cybersecurity Claims

8 Delaware and New Hampshire Enact Insurance Data Security Laws

European Parliament Panel Releases Report on Blockchain and the GDPR

A recent report by a European Parliament panel provides a comprehensive overview of the application of the General Data Protection Regulation (GDPR) to blockchain technology.

Since the EU's GDPR went into effect in May 2018, many have questioned how the regulation can be applied to blockchain applications, given the technology's highly decentralized and immutable structure. Concepts in the GDPR, such as identifying data controllers and data processors and providing data subjects with the right to have their data erased, seem inapplicable in a blockchain environment. A recent 105-page report commissioned by the European Parliament Panel for the Future of Science and Technology (STOA) (the STOA Report or the report) provides the most comprehensive and thorough analysis to date of these issues. Until the STOA Report, the only official report on blockchain and GDPR was a much shorter overview of the issues published by the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (the CNIL Report).[1]

Three themes emerge from the STOA Report. First, blockchain developers need to take GDPR requirements into account and cannot simply determine that the law is incompatible with the technology. This is consistent with a 2018 European Parliament resolution on blockchain and the GDPR.[2] Second, it is inaccurate to speak in general terms about the intersection between blockchain and the GDPR since there are a number of different types of blockchain platforms (permissioned vs. permissionless, private vs. public, etc.). Thus, each use of the technology needs to be examined on its merits. Finally, regulators need to provide more guidance as to how certain key provisions of the GDPR are to be interpreted when applied to blockchain technology. As the STOA Report notes, attempts to draft the GDPR to be technology-agnostic have created a number of ambiguities that require further clarification. Whether such guidance emerges, and whether that guidance resolves these ambiguities, remains to be seen. Below, we summarize the key findings of the STOA Report.

[1] Commission Nationale Informatique et Libertés (September 2018), "Premiers Éléments d'analyse de la CNIL: Blockchain" can be read here. There also was a report on blockchain and the GDPR prepared for the European Union Blockchain Observatory and Forum in October 2018.

[2] Proposition de Résolution déposée à la suite de la question avec demande de réponse orale B8-0405/2018 (24 September 2018), para 33.

Defining Personal Information

A common reaction among blockchain technologists is that GDPR issues are not relevant to blockchain technology since, in many use cases, personal information is not stored or processed on-chain. However, since the GDPR broadly defines "personal data" to include data that could be used to identify an individual — even where the data in itself would not allow one to do so — many types of data stored on-chain, including public keys, ostensibly meet this definition. Moreover, the STOA Report notes, as data mining technology becomes more sophisticated, the types of data that could be used to identify an individual will only expand. The report also makes the interesting observation that since data on a blockchain is permanent, data that could not be used to identify an individual today might be able to in the future as technology evolves. The STOA Report also cautions against the assumption that public keys are pseudonymous and therefore not covered by the GDPR. As the report explains, "pseudonymization" is viewed in the GDPR as a potential security step, not as a category of data that is outside the coverage of the GDPR.

The STOA Report comes to the conclusion that public keys qualify as personal data, and advocates the use of one-time public keys as a possible solution to be explored, while acknowledging that this may be easier to do on private and permissioned blockchains rather than public and permissionless ledgers "due to existing governance mechanisms and institutional structures allowing for such a design."

However, the STOA Report also notes that further guidance is required to clarify the standard of reasonableness to be applied when determining how possible it is to identify an individual based on a single set of data (*e.g.*, public keys), as well as whether this should be viewed from the perspective of the data controller or from any third party who might be able to access the data. Similarly, the report notes that further guidance is required as to whether encrypted data can be deemed anonymous data — thus, outside of the GDPR — to anyone other than the holder of the decryption key.

Additionally, the STOA Report notes ambiguity with respect to hashed data. While some consider hashed data anonymous, the report explains that hashing is only truly anonymous when there is a limitless possibility of inputs. However, where the input list is finite (such as all possible Social Security numbers) one could compare a hashed Social Security number with all possible options and quickly discover the input. The report recognizes similar ambiguity with techniques such as "salting" or "peppering" a hash, and calls for further regulatory guidance in the area of hashing, including whether a hash of off-chain data that has been deleted remains personal data.

Responsibility for GDPR Compliance — Data Controllers and Processors

The GDPR is based on the concept of defined roles of data controllers and data processors. The controller is defined, in relevant part, as the person or entity that alone or jointly with others, determines the purposes and means of processing personal data. The controller must implement technical and organizational measures to demonstrate that any data processing complies with the GDPR. In many cases, the data controller is a single and easily identifiable party. In the blockchain context, however, one could argue that multiple players in the ecosystem satisfy the data controller definition. This creates a "joint controller" situation, a concept the GDPR accounts for. However, the STOA Report acknowledges that there is a fair amount of uncertainty as to the concrete practical application of the joint controller test, and what degree of involvement is necessary to be designated a joint controller. Some possibilities of what can be defined a "controller," the report notes, include any party that exercises influence over the software, hardware and data centers that are used for a blockchain platform; any entity that determines the means of processing at the application layer; and intermediaries, such as a wallet provider.

The STOA Report explains that identifying the controller may depend on the type of blockchain. For example, in a private blockchain there is typically a clear legal entity that determines the means and purposes of personal data processing that would be defined as the data controller. However, even in these cases, the STOA Report notes, one could argue that other participants also meet the joint controller definition.

In public blockchains, determining which participants meet the definition of "controller" needs to be assessed on a participant-by-participant basis. The STOA Report addresses certain participants, agreeing with the CNIL Report, for example, that miners — solely in their capacity as miners — are unlikely to qualify as controllers since they do not determine the purpose of a specific transaction. However, the report suggests that a node that initiates a transaction (*i.e.*, distributes information to other nodes) or that saves a transaction in its own copy of the ledger, may qualify as a joint controller. This is of particular note because, with the proper level of consensus, nodes have the power to alter the processing rules.

According to the STOA Report, the role of "users" on a blockchain network is even more complex, especially given that in some cases a "user" might be an individual, while in other cases it may refer to an entity uploading personal data of others. The report considers whether the GDPR's so-called "household exemption" means that individuals could never be deemed controllers on a blockchain network, but cautions that this exemption may not apply where personal data is shared with an indefinite number of other individuals. Overall, the report finds support for the notion that users could be deemed controllers since they have, in effect, determined the means and purpose of processing their data.

The STOA Report acknowledges the inherent tension in the concept that users could be the controller of their own data. On one hand, this seems consistent with the underlying objective of the GDPR to give data subjects more "control" over their own data. However, the report cautions that this could lead to "less responsible and accountable forms of personal data processing" since an individual is unlikely to understand the nuances of GDPR compliance as a controller, or even know what those compliance obligations might be. The report concludes that the concept of "user as controller" should be clarified with additional guidance.

The Impact of Determining Joint Controllers

The conundrum with so many blockchain participants meeting the GDPR definition of "controller" is that, practically, many do not have the ability to fulfill the obligations that come along with being a controller. For example, certain nodes could not realistically satisfy data access requests. While the GDPR allows joint controllers to determine their respective obligations under the regulation (Art. 26), suggesting that one controller could be responsible for handling compliance, that very same article states that data subjects could nonetheless exercise their rights against any data controller. The report again concludes that further guidance on these issues is required.

Data Processors

The GDPR defines a data processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Art. 4(8)). As compared to controllers, processors have more limited obligations under the GDPR, such as maintaining a record of "all categories of processing activities carried out on behalf of the controller." However, processing is defined broadly and includes data storage, a fact that has important applications for blockchain technology.

Determining whether all nodes in a public and permissionless blockchain ecosystem are processors has important compliance ramifications, not the least of which is that controllers and processors must have an agreement in place setting forth certain obligations on the processor. The STOA Report notes that a limited solution could be to require nodes and miners to agree to data processing terms when they download the software necessary to operate a node. However, the report acknowledges that this would not cover all participants in the system and does not offer any concrete proposals for how to address this issue.

Principles of Data Processing

The STOA Report also reviews the key principles that must be respected when processing personal data under the GDPR and how they apply to blockchain technology. We outline below some of the report's more interesting observations.

Legal Grounds for Processing

Personal data can be processed only where there is legal grounds for doing so, such as by having the data subject's consent. While one could argue that any user who has interacted with a blockchain has implicitly provided such consent, the STOA Report points out two problems. First, the GDPR requires clear, affirmative and informed consent. Thus, implicit consent is likely not a solution. Second, a user can withdraw consent at any time, and it is not clear how this would work given the permanence of blockchain data.

The report also analyzes whether personal data could be processed under the "legitimate interest" prong, which allows personal data to be processed where "the legitimate interests of the controller or a third party override the interests and freedoms of the data subject" (Art. 6(1)(f)). The report cautions that there are challenges in relying on this exception since users may not even realize their personal data is being processed (*i.e.*, not realize a public key may be personal information) or that a transaction may reveal information about them.

Transparency

The GDPR requires that it should be transparent to data subjects as to whether, and to what extent, their personal data is being collected, used or processed (Recital 39). The report notes that, in certain blockchain uses, such as private ones, enabling such transparency will be achievable. But, in contexts where there are no channels of communication between the controller or data subjects, the requisite transparency requirements may be hard to achieve.

Purpose Limitation

The purpose limitation presents one of the more interesting challenges for reconciling blockchain technology with the GDPR. Under this requirement, data may "only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (Art 5(1)(b)). As the report notes, the question that becomes readily apparent is whether the post-transaction "processing" of personal data by virtue of the fact that such data is now part of an immutable chain of blocks violates the purpose limitation principle. The report proposes that data controllers using blockchain technology should clearly disclose to users how their personal data will be used, including how it may processed in the future as new blocks are added, although it suggests that the purpose limitation might be satisfied if users would have reasonably expected their personal data to be used in this fashion (*i.e.*, a user knowing how blockchain technology functions). The report concludes that a case-by-case analysis is required to determine if the purpose limitation is being violated.

Data Minimization and Storage Limitation

Similar in some respects to the purpose limitation, the GDPR requires that data processing should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Art. 5(1)(c)). Again, the issue is how to interpret this requirement for blockchain technology where historical data is stored, copied and reused to assure the authenticity of the latest block and for the technology to function. The STOA Report opines that this issue requires an analysis similar to the purpose limitation; namely, can one argue that the subsequent use of data for the ecosystem to operate is consistent with the data's initial purpose. Importantly, the report concludes that further guidance is required on how data minimization is to be interpreted in the blockchain context and whether storing certain data off-chain addresses this issue.

With respect to storage limitation (*i.e.*, data is "kept in a form which permits identification of data subjects for no longer than is necessary") (Art. 5(1)(e)), the report proposed additional guidance on possible solutions, such as whether it would be sufficient if the data controller could not use the stored historical data in any way that impacts the data subject, or if the controller commits to delete historical data if and when that becomes possible.

Rights of the Data Subject

The lynchpin of the GDPR are the rights bestowed on data subjects. The report analyzes whether such rights, which must be facilitated by the data controllers and cannot be delegated, are compatible with blockchain technology. Once again, the report cautions that a case-by-case analysis is required, and notes that while some rights do not seem to present any issues, others may be more challenging to honor in a blockchain ecosystem.

Right of Access

Data subjects have the right to obtain from the data controller various details about their data, such as the purpose of processing, the recipients or categories of recipients of the data, and where possible, the period of time for which the data will be stored or how that determination will be made (Art. 15). The report asserts that data controllers in a blockchain ecosystem should be able to comply with this obligation, but acknowledges that if the concept of data controller is broadly construed, it may be more complicated for certain controllers, such as nodes, to comply.

Right to Rectification

A data subject has the right to require the controller "without undue delay" to rectify any inaccurate personal data about that data subject (Art. 16). However, in order to secure data integrity and trust in the network, most blockchains are "append-only," meaning that no one can go back and change any historical data. The report notes that while private and permissioned blockchains may be able to honor the right to rectification, public blockchains could not easily do so since it would mean achieving consensus among a vast body of nodes, and such consensus would be difficult to achieve for one-off requests, even if bundled together periodically.

One potential solution, the STOA Report explains, is the right under the GDPR to rectify data through a supplementary statement. In a blockchain this might mean adding new data to a block that effectively rectifies erroneous data. However, the report explains, it is not clear whether the addition of new information on-chain will always satisfy the GDPR rationale inherent in the right of rectification. The report recommends regulatory guidance to clarify when rectification could be accomplished through supplementary information, and encourages developers to facilitate technology solutions to this issue.

The Right to Erasure (The 'Right to be Forgotten')

A data subject has the right, with certain exceptions, to require that the controller erase personal data about the data subject without undue delay (Art. 17). Exceptions include where the personal data is still needed in relation to the purpose for which it was collected and for compliance with law purposes. The controller also is required, subject to available technology and resultant implementation costs, to take reasonable steps to inform other controllers that are processing the data of the erasure request.

As with the right of rectification discussed above, deleting data on a blockchain is difficult in that it threatens trust in, and the integrity of, the network (particularly in public and permissionless blockchains). As the report notes, this difficulty is exacerbated by the fact that "erasure" is not defined under the GDPR. If erasure requires complete data destruction, then satisfying this right for blockchains is difficult. However, the report cites the fact that certain data protection authorities have suggested that erasure does not necessarily mean full destruction. The report states that guidance is needed to clarify what steps would satisfy the erasure requirement, such as destruction of the corresponding private key, a solution that has been supported in the CNIL Report. Other technical options suggested by the report, and for which guidance would be required, are anonymization, redactable blockchains that would be "forgetful" by design, chameleon hashes, zero knowledge proofs and corrective operations through the use of smart contracts.

The report cautions that even where technical solutions are found sufficient enough to constitute "erasure," compliance may still be difficult since it requires a level of communication and coordination among all nodes that may not be readily available. The report notes that this issue underlines the importance of designing blockchain governance to ensure compliance.

Right to Restriction of Processing

The data subject has the right to require that the data controller restrict processing, such as where the data subject asserts that the data is inaccurate or that the processing is unlawful (Art. 18). The report identifies two obstacles to complying with this right. First, blockchains are typically designed to make unilateral intervention in data processing burdensome in order to increase data integrity and trust in the network. Second, there are the governance challenges of coordinating what are possibly numerous joint controllers.

Data Controllers' Communication Duties

The GDPR requires that the controller communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort (Art. 19). In addition, the controller must inform the data subject about these recipients upon request. The STOA Report notes that this raises the question of what parties would actually qualify as "recipients" in a blockchain, especially in a multi-node public permissionless system. Moreover, there may be no way to conclusively determine which parties have gained access to the relevant data. The report suggests that in these cases one could argue that the communication duty is waived since it would "prove impossible" or at the least "involve disproportionate" effort.

Right to Data Portability

Data subjects have the right to receive the personal data they have provided to a controller, in a "structured, commonly used and machine-readable format," and also have the right to transmit that data to another controller without hindrance from the controller where technically feasible (Art. 20). The principle of personal data is to empower data subjects regarding their own personal data and to facilitate their ability to move data from one system to another. Importantly, this right is limited to cases where personal data processing is based on consent or contract.

The CNIL Report concluded that blockchain technologies raise few problems when it comes to compliance with the portability requirement. However, the STOA Report notes that this right may only be achievable if the blockchain systems at issue are interoperable. The STOA Report also again cautions that certain entities may meet the definition of controller but may be unable to comply with of the portability requirement as a practical matter.

The Right to Object

The GDPR provides data subjects with the right to object to any processing of their personal data where such data is processed by the data controller based on public interest or legitimate interest justifications (Art. 21). When such a right is exercised, the data controller must stop processing this data unless it can demonstrate "compelling legitimate grounds" for the processing that overrides the interests of the data subject or is defending a legal claim. The STOA Report questions whether the data controller's interest in the integrity of blockchain records could qualify as such a "legitimate interest," and suggests that regulatory guidance is required on this topic.

Decisions Based on Automated Processing

Data subjects have the right to not be subject to decisions based solely on automated processing (*i.e.*, no human intervention) that will have significant legal effects on the data subject (Art. 21). Exceptions exist where such processing is necessary for the performance of a contract or required by law. The report notes

that this right may have ramifications in the context of blockchain smart contracts, which ostensibly are a form of automated processing (*e.g.*, where a smart contract decides whether an insurance premium is paid). While the GDPR authorizes member states or the EU to create exemptions to the prohibition of automated processing provided that data subject rights and interests are safeguarded, no legislation has been passed to clarify whether smart contracts constitute automated data processing. The report suggests that clarity on this topic would be useful.

Data Protection by Design

The GDPR includes the concept of "privacy by design," which states that controllers must take privacy rights into account when they determine the means for processing and at the time of the processing itself. The STOA Report notes that this creates two obligations in the blockchain context. First, blockchain developers should take GDPR compliance into account during the development process, and second, data controllers should ensure that governance of their blockchain facilitates GDPR compliance. According to the report, this includes efficient communication between data subjects and data controllers and between various joint controllers.

Data Protection Impact Assessments

The GDPR requires that where data processing is likely to result in a high risk to fundamental rights, the controller should conduct a Data Protection Impact Assessment (DPIA) to determine the impact of processing on personal data protection (Art 35). If a DPIA reveals a high risk, and there are no measures adopted to mitigate that risk, the controller is required to inform the supervisory authority. In some cases, the mere use of a new technology may give rise to a high-risk designation. The STOA Report recommends guidance as to whether the mere use of blockchains creates a high risk to fundamental rights, or whether blockchain developers can consider the need for a DPIA on a case-by-case basis.

Data Transfers to Third Countries

Under the GDPR, personal data can only be transferred from the EU to third countries whose data privacy laws have satisfied the "adequacy" requirement; have appropriate safeguards are in place (such as a processing agreement or binding corporate rules); or are receiving the data on the basis of a derogation (such as explicit consent) (Art. 49). In addition, data subjects need to be informed of the data transfer. The scope of this limitation is important for blockchain technology since nodes will likely be located in jurisdictions outside the EU, and, in the case of public blockchains, the node location cannot be controlled. The report does not offer many concrete proposals in this area other than to note that some have proposed the use of some form of binding corporate rules to satisfy this requirement, and that blockchain technology may actually facilitate transparency as to where data was transferred.

Use of Blockchain to Achieve GDPR Objectives

While much of the STOA Report focuses on the issues that may be raised in applying the GDPR to blockchain technology, the report concludes with the important observation that this nascent technology might be a useful tool to achieve at least some of the GDPR's underlying objectives. Specifically, the report notes that blockchain applications can provide data subjects with more "granularity" over the management of, and access to, their data without reliance on a central trusted intermediary and with increased transparency.

The Need for Regulatory Guidance

As noted throughout the foregoing summary, the STOA Report repeatedly states that further regulatory guidance is needed in order for blockchain technology to be used to help achieve the GDPR's objectives and for developers to be aware of requirements for proper compliance. At the end of the report, a comprehensive list of proposed guidance is provided:

- Can the "household exemption" (under which individuals engage in non-commercial activity are not subject to the GDPR) be invoked in relation to public and permissionless blockchains where data is shared with an indefinite number of people?
- Is anonymization an effective means of satisfying the "erasure" requirement?
  - What is the status of the on-chain hash where the corresponding transactional data stored off-chain is subsequently erased? (*i.e.*, is the on-chain hash no longer personal data?)
- Should anonymization be evaluated from the controller's perspective, or also from the perspective of other parties? (*i.e.*, as long as the controller cannot recreate one's identity is that enough?
  - Does a peppered hash of data render it anonymous?
  - Are anonymity solutions, such as zero knowledge proofs, sufficient to create anonymous data?

- Is there a *de minimis* test regarding influence over the purposes and means of processing that must be crossed before a party is designated as a processor or controller?
- What is the scope of a data controller's responsibility under the GDPR, and is that responsibility limited to the (joint) controller's responsibilities, powers and capacities?
- Does the "purpose limitation" principle only encompass the initial purpose (the transaction) or can that purpose also encompass the continued storage of the data and its further processing, such as to achieve consensus?
- Can a data subject be a data controller in relation to personal data that relates to themselves?
- What is the relationship between the first paragraph of Article 26 (which allows joint controllers to determine their respective responsibilities) and the third paragraph (which allows a data subject to exercise their rights against any controller)? Is there a need for a nexus between responsibility and control?
- How should the principle of data minimization be interpreted in relation to blockchains?
  - Is the off-chain storage of transactional data a means of complying with the data minimization principle?
- Is the provision of a supplementary statement always sufficient to comply with the right to rectification?
- How should "erasure" be interpreted, and is the deletion of a private key sufficient?
- How should the right to restrict processing be interpreted in the context of blockchain technologies?
- Does the continued processing of data on blockchains satisfy the compelling legitimate grounds criterion?
- Does the mere use of a blockchain trigger a need to carry out a data protection impact assessment?

Codes of Conduct and Certification Mechanisms

The report notes that the GDPR already includes two mechanisms that could be useful for dealing with the blockchain-GDPR tension: certification mechanisms and codes of conduct. The rationale behind each of these is to establish a co-regulatory environment in which regulators and the private sector collaborate. One example the STOA Report offers is the design of binding network rules regarding international data transfers.

The Obligation of Developers

The STOA Report concludes with the idea that while further guidance may be needed on the regulatory front, developers could also work towards addressing certain issues, such as defining governance mechanisms under which controllers could coordinate effectively on data rights, designing mechanisms that enable the effective revocation of consent in the context of automated personal data processing, designing technical solutions to comply with the right of erasure, and developing protocols that would be compliant by design.

Return to Table of Contents

First Monetary Settlement in a False Claims Act Case Involving Cybersecurity Claims

An $8.6 million settlement from Cisco is the first known payout in a case brought under the False Claims Act (FCA) involving allegations of cybersecurity-related misrepresentations.

On July 31, 2019, Cisco Systems announced that it had agreed to pay $8.6 million to settle claims filed by a whistleblower alleging that the company sold a line of video surveillance systems with known security flaws to federal and state governmental entities. The whistleblower alleged that he first reported the vulnerabilities to the company while employed as a security researcher by a Cisco partner in 2008. In 2011, after the company allegedly failed to patch the vulnerabilities, the whistleblower filed a lawsuit on behalf of the federal government and several state governments under the federal FCA and similar state laws.[3] The whistleblower alleged that the company failed to comply with cybersecurity standards applicable to federal contractors. Cisco issued a statement following the settlement to clarify that the whistleblower did not allege or provide evidence that any unauthorized access to customers' video systems occurred as a result of the vulnerabilities.

Background on the False Claims Act

Under the federal FCA and similar state laws, individuals can file claims on behalf of the federal government or a state government alleging that the defendant — typically a company that has

[3] The complaint is available here.

sold goods or services to the government — has defrauded the government. The individual who files these claims can receive up to 30% of the award granted to the government, which creates a strong financial incentive for whistleblowers. Although an individual whistleblower files the claim on behalf of the government in FCA cases, the government serves as the real party in interest. This point proves especially important for cybersecurity-related claims because the individual who files a claim on behalf of the government does not need to establish constitutional standing on his or her own behalf, removing a significant roadblock typically faced by individuals who sue companies in response to cybersecurity incidents.

Similar False Claims Act Cases

Although this settlement represents the first known payout from a FCA case involving cybersecurity-related allegations, whistleblowers have made similar allegations in the past. In May 2019, the U.S. District Court for the Eastern District of California refused to dismiss a case in which a whistleblower alleged that his former employer, Aerojet Rocketdyne Holdings, Inc., made false assertions regarding the company's compliance with cybersecurity standards mandated by the Department of Defense.[4] That ruling signaled that a federal or state contractor that knowingly misrepresents its compliance with mandated cybersecurity standards — or even makes representations regarding its compliance with such standards as part of an initial agreement, but years later fails to patch a vulnerability that could result in non-compliance — could face significant liability under the federal FCA and its state analogues. With the announcement of the first monetary settlement involving cybersecurity-related allegations, many expect an increase in similar cybersecurity-related FCA claims in the near future.

Key Takeaways

The case and monetary settlement highlight the risks associated with managing and responding to cybersecurity vulnerabilities. Given the significant financial incentives for whistleblowers under the federal FCA and similar state laws, security researchers who find vulnerabilities in products and services that are sold to governmental entities may pursue claims under the FCA in addition to pursuing payouts under "bug bounty" programs sponsored by the company at issue. Companies that work with federal and state governments should establish clear policies for reviewing, patching and publicly disclosing vulnerabilities that are identified by employees or third parties during security audits, especially in cases where the failure to patch vulnerabilities in a timely manner might cause the companies to breach representations regarding its compliance with mandated cybersecurity standards. Companies that implement such policies and respond promptly to notices regarding material vulnerabilities can reduce the likelihood of facing similar claims from whistleblowers.

Return to Table of Contents

Delaware and New Hampshire Enact Insurance Data Security Laws

The state legislatures of Delaware and New Hampshire recently adopted variations of the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (Model Law), joining several other states in establishing data security and breach notification requirements for insurance industry players.

Insurers are often alluring targets for cyberattacks because they routinely collect and retain significant amounts of nonpublic, sensitive information about their insureds and losses. As a result, a growing number of states have enacted variations of the NAIC Model Law,[5] which establishes minimum data security safeguards and data breach notification obligations applicable to a range of insurance industry players. Delaware, whose statute was signed into law on July 31, 2019, and New Hampshire, whose statute was signed into law on August 2, 2019, are the latest states to adopt such laws.[6]

The New State Laws

Both the Delaware and New Hampshire laws focus on protecting "nonpublic information," defined to include individually identifying information, including Social Security numbers, financial account numbers, biometric records and health information. The laws apply to any individual or nongovernment entity required to be authorized, registered or licensed pursuant to the state's insurance laws (licensees, and each a licensee). However, both states exempt small organizations from the laws; Delaware exempts entities with fewer than 15 employees, while New Hampshire exempts those with fewer than 20 employees.

[4] *See United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, No. 2:15-cv-2245 WBS AC, 2019 WL 2024595 (E.D. Cal. May 8, 2019).

[5] See our October 2017 *Privacy & Cybersecurity Update* for a discussion of the NAIC Model Law, available here.

[6] Alabama, Connecticut, Michigan, Mississippi, Ohio and South Carolina have adopted modified versions of the NAIC Model Law. In addition, New York regulates insurers' handling of data via the New York Department of Financial Services cybersecurity rules (23 NYCRR 500).

Under both laws, a licensee is required to conduct a risk assessment and establish a written information security program, detailing the administrative, technical and physical safeguards the licensee will maintain to prevent data breaches. The information security program also must include an incident response plan and schedule for the retention and destruction of nonpublic information. Both laws also require that licensees provide written certification to the insurance commissioner (commissioner) on an annual basis demonstrating that the licensee is in compliance with the insurance data security law.

If the commissioner has reason to believe that the licensee is violating the law, the commissioner is empowered to "examine and investigate" the licensee's affairs and to take any "necessary or appropriate" action to the enforce the law. The New Hampshire law contains a safe harbor provision providing that any licensee in compliance with New York Department of Financial Services cybersecurity regulations is deemed to be in compliance with the New Hampshire law.

The two states' laws also require a licensee to provide notice to the commissioner and to affected consumers of a "cybersecurity event," which is defined broadly to include unauthorized access, disruption or misuse of the licensee's information system or nonpublic information stored on that system. The definition excludes instances in which the nonpublic information was returned or destroyed without being used, or in which the information was obtained in an encrypted format without the corresponding encryption key. After determining that a cybersecurity event has occurred, a licensee is required to notify the commissioner within three business days.

Both laws also require that a licensee provide notice to consumers affected by a cybersecurity event. Delaware's law requires that the licensee notify consumers within 60 days of the event, while New Hampshire's law incorporates the state's general security-breach notification statute (RSA 359-C:20), which requires only that a licensee provide notice "as soon as possible." Both laws provide that a licensee may delay notice if a law enforcement agency determines that the delay is necessary to avoid impeding a criminal investigation. In addition, if a cybersecurity event involves exposure of Social Security numbers, Delaware's law requires that the licensee provide one year of free credit monitoring services to affected consumers.

The laws' compliance deadlines are July 31, 2020, for Delaware and January 1, 2021, for New Hampshire. Both laws provide licensees an additional year after the compliance deadline to ensure that their third-party service providers also comply with the laws.

Key Takeaways

With Delaware and New Hampshire's recent enactments, a total of nine states now have adopted data security laws or regulations specifically geared toward the insurance industry. This trend is likely to continue as more states enact a version of the NAIC Model Law. While insurance providers and other licensees may gain a general understanding of data security laws by reviewing the NAIC Model Law, they nevertheless must pay specific attention to state variations in definitions, deadlines and other requirements. Moreover, licensees will need robust and adaptable systems to ensure that both they and their third-party service providers remain in compliance with this new generation of insurance data security laws.

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
213.687.5381
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

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@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

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

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

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

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

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@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
Four Times Square
New York, NY 10036
212.735.3000