Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

APRIL 2020

IN THIS ISSUE

Practical Wisdom, Trusted Advice.

www.lockelord.com

Privacy and Cybersecurity Work from Home Considerations in the Context of Coronavirus

By Theodore P. Augustinos and Laura L. Ferguson

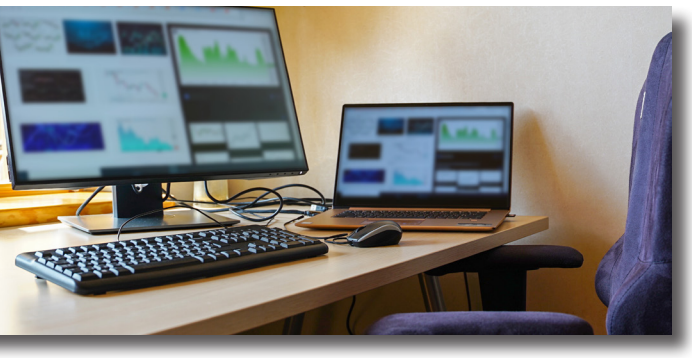
We want to enable our personnel to work from home during this health crisis. What do we need to worry about from a privacy and cybersecurity perspective?

1. Equipment. Personnel working remotely will need equipment, and you may not have enough company issued laptops, tablets and other devices to enable personnel to perform their functions outside of company premises. Personnel without company-issued equipment may have personal devices that can be connected and supported for purposes of working remotely, but this may not be the case with outdated equipment. Security issues introduced by using personal equipment to connect must be considered. Programs and apps may need to be installed or downloaded in order to address the issues presented by the use of personal devices. Usual cybersecurity hygiene should be "kicked up a notch" in this new, challenging environment. Require the use of a virtual private network and multi-factor authentication before permitting access to company systems through a personal device. In addition, now is a good time to require employees to update settings on their computers to keep information secure, such as the use of strong passwords or passphrases and automatic log off when not in use.

   Consider also the company's side of the equipment equation. The IT infrastructure may or may not have the capacity to increase, probably drastically, the number of personnel working remotely.

Locke Lord has mobilized across disciplines to create a COVID-19 Task Force and Resource Center that provides a coordinated response to our clients' range of needs. This includes an FAQ section covering a host of issues, as well as links to recent QuickStudies.

We encourage you to regularly visit our COVID-19 Resource Center for the most up-to-date information. You will also find access to key contacts at Locke Lord who can put you in touch with appropriate team members.



2. IT Support. Demands on IT will increase, particularly for those working remotely for the first time, who may be installing new programs and apps for this purpose, and who may be unaccustomed to navigating company systems in the remote environment. Consider whether existing IT support staff is up to the task. Phasing in first-time remote users over time may help to spread out and ease the demands on IT support staff. Prepare FAQs on how to utilize programs and apps remotely for first-time remote users, if such FAQs do not already exist.
3. Policies and Protocols. Given that the company and many of its personnel may be operating in a new environment, with every new remote access presenting new risks and vulnerabilities, a careful consideration of privacy and cybersecurity policies and procedures would be well advised. For example, if the remote access policy restricts remote access to company-issued devices, appropriate and well-documented adjustments should be considered to avoid violations of an existing policy that could present additional exposures in the event of a security incident. Similarly, existing policies could restrict the removal of data, including paper, from the company's secure environment, but personnel may need more access to more data for a longer period than contemplated by existing policies, and appropriate adjustments should be considered to permit personnel to perform their job functions off-site. Consider the sensitivity of the information contained in paper records and the corresponding need to keep such information secure. Implement a method to track the physical movement of such records to enable the business to verify that all such records are returned to the worksite when the remote worker returns to onsite working. In addition, review whether current policies include a prohibition on the use of personal connected devices that use Alexa, Google, or Siri, when working from home given the devices can listen to conversations occurring in the background, which could include confidential work-related calls.

As always, limit remote access as much as possible. Don't let the current panic, and the need to get personnel fully functioning as quickly as possible, distract from sound privacy and cybersecurity risk mitigation practices.

As Companies Seek Alternative Ways to Sign Contracts and Other Records During COVID-19 Pandemic, E-Processes Take Center Stage

By Patrick J. Hatfield

Companies are scrambling to complete transactions with customers and suppliers faster and cheaper, and in the current COVID-19 environment, now at a safe distance. E-contracting and e-signatures have been in the marketplace for over 20 years, but organizations which have not adopted the framework may be taking a closer look at e-processes in light of the crisis. Below is a primer to understanding and managing the risks associated with an e-process, along with some practical pointers on using e-signatures/e-contracting.

Authentication Risk

This is the risk that the electronic signature obtained is from a forger, not from the actual person whose name is associated with the electronic signature. The risk is that a company relying on an applicant's electronic signature to be that of a given person seeks to enforce the document bearing the person's signature and the person claims, "That is not my signature!"

There are ways to authenticate the identity of a person. A popular and simple method is to use a "shared secret," such as combination of questions that nobody other than the real person would know: social security number, mother's maiden name, date of birth, employee number, etc. There are firms that can authenticate a person on a real time basis as well, using the shared secret approach.

Repudiation Risk

This is the risk that a document bearing a person's signature is altered after the document is signed electronically and the person repudiates the contents of the document bearing his or her signature. The risk is that a company relying on an applicant's electronic signature seeks to enforce the terms of the signed document bearing the applicant's signature and the applicant claims, "Yes, that is my signature, but the terms and conditions of what I signed are different than that document!"

There are ways to mitigate the repudiation risk considerably; in fact, the repudiation risk can be reduced below the repudiation risk associated with traditional methods. The simplest way to mitigate repudiation risk is to have each document "electronically sealed" immediately after it is signed to prevent any alteration to the document without such change being visible. Storing the documents in secure environments also mitigates the repudiation risk.

Compliance Risk

This is the risk that the rules and regulations governing such a transaction, such as regulation requiring certain consumer disclosures to be provided by a certain stage in the transaction, are not satisfied. The risk is that the company is sanctioned by regulatory authorities or the other party to the transaction avoids its obligations.

There are ways to mitigate this risk as well. Again, as with the repudiation risk, with a little bit of logic embedded in an e-process, compliance can actually be better than in the traditional process. For example, an e-process with logic that requires all the disclosures to be provided and acknowledged by a consumer can prevent completion of the process without all required disclosures being provided to the applicant.

Admissibility Risk

This is the risk that an e-contract is not admissible into evidence when the company seeks to enforce it. In a 2007 landmark case in the U.S. District Court of the District of Maryland, Lorraine v. Markel, the Court's decision put both litigators and litigants on notice that simply offering electronic evidence, without laying the proper foundation, can deem such evidence inadmissible, and thus an e-contracting business process unenforceable.

There are various ways to improve the likelihood of the admissibility of e-contracts, for example, by using an exemplar business process to designing customized systems for the creation, storage and production of electronic information.

Adoption Risk

This is the risk that the e-process takes longer than the traditional process or is not as convenient as the traditional process and consequently, adoption of the process is slow. The risk is that a company invests considerable resources to design an e-process only to find that there is little use of the e-process.

The best way to mitigate this risk is to field test a proposed e-process.

Relative Risk

There are authentication risks, repudiation risks and compliance risks with the traditional process of using wet ink and hard copy paper to complete transactions. Many companies have not examined such risks until they begin developing an e-process. For most electronic signature and e-delivery processes, the goal will be to have the transaction, on the whole, be no riskier than the current processes.

The Effective Date of the California Consumer Privacy Act of 2018 Has Come and Gone: What To Do Now?

By Theodore P. Augustinos

The CCPA became effective January 1, 2020. Some businesses prepared to meet the deadline, while others have become partially compliant but still have more to do. Some may not have begun. What should a business be doing at this point?

1. **Note the Important Dates.**

   The CCPA, enacted June 28, 2018, was amended several times prior to its effective date of January 1, 2020, and will be enforceable by the Attorney General on July 1, 2020. Concerning the delayed enforcement date, keep in mind two points: First, as of January 1, 2020, consumers have a private right of action (with statutory damages) for violations of the CCPA requirement to provide reasonable security that result in an unauthorized disclosure of personal information. Second, the Attorney General presumably could bring actions starting July 1, 2020 for failures to comply dating back to January 1, 2020. Therefore, if a business was not in full compliance as of January 1, 2020, time is of the essence in order to mitigate the risks of enforcement and private litigation.

2. **Assess (or Reassess) Scope and Applicability.**

   As we discussed here, businesses must begin by assessing the applicability of the CCPA to the business. Is the business "doing business" in California? Does it collect personal information from California residents? Does the business meet one of the thresholds based on annual revenue and data collection? Do CCPA exemptions (such as the GLBA, HIPAA, FCRA and other exemptions) apply? If one of the exemptions applies, does the business also collect personal information not covered by an exemption?

   The temporary, limited exemption for personnel (such as employees, job applicants, officer, directors and owners) enacted by AB-25 solved significant challenges for many businesses, as further discussed here. Note, however, that this exemption for the personal information of personnel is temporary, with a scheduled sunset of January 1, 2021, and also partial, given that the business must provide a notice at collection to its personnel, who also continue to have a private right of action under the CCPA.

   Similarly, the exemption for business to business (or B2B) contacts provided by AB-1355 is scheduled to sunset on January 1, 2021 and is limited in that B2B contacts retain the CCPA's "do not sell" right and private right of action.

3. **Analyze Collection and Use of Personal Information.**

   After determining the CCPA applies, the business must: analyze its collection and use of personal information, and, as suggested here, create a project plan to map the collection, use and sharing of personal information; draft internal policies and procedures for CCPA compliance; prepare the required notice at collection and privacy policy; and review relevant vendor contracts. It is also advisable to prepare forms and mechanisms for consumers to submit requests to exercise their rights under the CCPA, and create procedures and forms for responding to these requests.

   The notice at collection and privacy policy are the two central documents required by the CCPA. The content and other requirements for these documents were clarified by the draft regulations issued by the Attorney General. As the draft CCPA regulations make clear, they are two separate documents presenting different disclosures. A common question is whether the requirements for the CCPA privacy policy can be addressed through the business's existing online privacy policy. Note, however, that the particular disclosure requirements and consumer rights of the CCPA are unique in the U.S., and most companies will not elect to extend the CCPA rights to all individuals. Therefore, the common and safest approach is to prepare separate CCPA disclosures through a CCPA Privacy Policy and a CCPA Notice at Collection.

4. **Track Statutory Amendments and Regulatory Developments.**

   Another important task for pursuing CCPA compliance is the tracking of amendments to the statute itself and developments in the proposed regulations. Whether a business was prepared for the January 1 effective date, or whether it is getting a late start, the statutory amendments made to the CCPA between June 2018 and October 2019, including those discussed above, have been significant and largely helpful. It is important to follow the proposed statutory amendments that are currently pending in the legislature.

   There is, however, a new initiative by the activists who propelled the CCPA that would effectively replace the CCPA with a new California privacy law (proposed as the California Privacy Rights Act of 2020). This new proposal would be more onerous for businesses, and more punitive in enforcement, than the CCPA. All businesses should track its progress.

   In addition, the regulations to be promulgated by the Attorney General will be highly important to every business's CCPA compliance effort. The draft regulations, which were recently amended on February 10, 2020, answer a lot of questions and provide clarity. For example, the draft regulations address the verification process necessary to properly identify the subjects of consumer requests, the ability of consumers to use agents, and the presentation of CCPA disclosures themselves. The current form of the draft regulations is available here.

   As for developments in other jurisdictions, several states are considering legislation inspired by or identical to the CCPA, and nearly 20 have recently adopted or are considering some form of privacy legislation. CCPA compliance efforts will need to track and account for these developments as well.

CCPA Update: Important Modifications to the Proposed Regulations

By Theodore P. Augustinos

As we reported here the California Attorney General released proposed regulations pursuant to the California Consumer Privacy Act (CCPA) on October 10, 2019. These proposed regulations were modified on February 7 and again on February 10, 2020. These modifications, which followed additional hearings and comments, would effect several important changes and clarifications.

- **Clarification of "Personal Information."** A new section 999.302 provides guidance for interpreting the CCPA definition of "personal information." A helpful example is provided for IP addresses, indicating that IP addresses are not personal information if collected by a business through its website where the business could not reasonably link the IP address with a particular consumer or household.
- **Further Clarification of Notices.** The proposed regulations released in October 2019 provided helpful guidance as to the notices to be provided to consumers, particularly by clarifying the distinctions between the notice at collection and the privacy policy. The modifications to the proposed regulations go further to:
  - provide more specificity as to delivery, including for use with mobile apps and devices such as a new

CCPA CORNER

Our Privacy & Cybersecurity Practice Group has organized a CCPA Initiative of lawyers in various offices throughout our Firm to work with clients on CCPA compliance. We have developed templates and checklists that are available for a fixed fee. If you would like to talk with a member of our CCPA Initiative, and to learn more about our CCPA templates and checklists, please contact:

Theodore P. Augustinos ted.augustinos@lockelord.com or 860-541-7710

Molly McGinnis Stine mmstine@lockelord.com or 312-443-0327

"just-in-time notice" to address the collection of personal information for a purpose that would not be reasonably expected; and
    - limit to registered data brokers the originally proposed relief from the requirement for notice at collection in the context of information collected indirectly (i.e., not directly from consumers).
- Clarification of Accessibility Requirements. The CCPA's requirement that the notice at collection and privacy policy must be accessible is further defined by reference to generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018 from the World Wide Consortium.
- Streamlining Disclosures in the Notice at Collection and Privacy Policy. The modifications delete the requirement to disclose in the notice at collection "for each category of personal information" the business or commercial purpose(s) for which it will be used, although the business or commercial purpose(s) for which "the categories" will be used must still be disclosed under the modified proposed regulations. Similarly, the requirements for privacy policy disclosures appear to be streamlined by the deletion of the requirement to disclose "for each category of personal information collected . . . the categories of third parties from whom information was collected, the business or commercial purposes for which it was collected, and the categories of third parties with whom the business shares personal information." The privacy policy must, however, disclose categories of personal information collected, categories disclosed for a business purpose or sold to a third party, and "for each category", the categories of third parties to whom it was disclosed or sold.
- Exceptions to Right to Know. The modifications also create exceptions from the obligation to search for information in response to the exercise of the right to know where the business:
    - does not have the information in a searchable or readily accessible format;
    - maintains the information solely for legal or compliance purposes;
    - does not sell the information and does not use it for any commercial purpose; and
    - describes to the consumer the categories or records that may contain the requested information that it did not search because of one of the foregoing reasons.

Certain biometric data was also excepted from the required response to the exercise of a right to know.

- Relief for Offline Businesses. The modifications include some relief for business that interact with consumers in person, including the change from a requirement to provide at least one method to submit requests in person to a requirement to "consider" providing an in-person method such as a printed form, a tablet or portal to submit online, or a toll-free telephone number.
- Clarifications for Responses to Consumer Requests. Additional guidance is provided for addressing rights to know and rights to delete for businesses that interact with consumers online, by telephone or in person, and back down on the original proposal to require a two-step process for online requests to delete. In addition, the modifications provide that a business can deny a request if it cannot verify the consumer within 45 days. Category by category disclosures must be provided in response to requests to know. In response to a request to delete, the business must ask the consumer if he or she would like to opt out of sales of personal information, if the consumer has not already made the opt-out request.
- Amplification of Restrictions on Service Providers. The modifications further amplify the restrictions on a service provider's ability to retain and use data. Importantly, internal use by the service provider to build or improve the quality of its services (other than for profiling) or cleaning or augmenting data from another source is permitted.
- Clarifications for the Opt-Out Right. The modifications provide further guidance on the offering and response to opt-out requests, including guidance for resolving conflicts with other consumer settings or a financial incentive program.
- Further Guidance Concerning Household Information. The modifications provide further guidance where a business receives a request to access or delete household information, including for verification.
- Verification Clarification. Guidance is provided for the verification process, including for verifying a consumer using a mobile app.
- Non-Discrimination. The modifications clarify that a financial incentive may not be offered unless the business can show a reasonable relation to the value of the consumer's data. Additional, helpful illustrations are also offered.

We will continue to track and report on further developments concerning the CCPA and its implications for businesses.

Show Me the Data! – Providing Data in Response to a CCPA Consumer Request to Know

By Molly McGinnis Stine

Starting January 1, 2020, California consumers are allowed to make requests for disclosure of certain information under the California Consumer Privacy Act of 2018 ("CCPA"). This article spotlights several practical issues concerning such requests by considering the text of the CCPA and the proposed regulations published by the California Attorney General on February 10, 2020 ("Proposed Regs"). [1]

Under Cal. Civ. Code § 1798.100(a), "[a] consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected."[2] The Proposed Regs at § 999.301(q) refer to this as a "request to know", defined as:

> a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:
>
> (1) Specific pieces of personal information that a business has collected about the consumer;
>
> (2) Categories of personal information it has collected about the consumer;
>
> (3) Categories of sources from which the personal information is collected;
>
> (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
>
> (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
>
> (6) The business or commercial purpose for collecting or selling personal information.

A covered business receiving a request to know shall first, according to the Proposed Regs, "confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request." The Proposed Regs further state that "[t]he confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given on the phone during the phone call." Proposed Regs, § 999.313(a).

The time to respond substantively also begins on the date of receipt of the request,[3] "regardless of time required to verify the request." Proposed Regs, § 999.313(a). The covered business has 45 days to respond, subject to a 45 day extension, and provide the requested information to the consumer. Cal. Civ. Code § 1798.130(a)(2). The Proposed Regs clarify that the deadlines for a response are calendar days. Proposed Regs, § 999.313(b).[4] According to the Proposed Regs, the 45 day extension is available, "provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request."[5]

Assuming a request to know is from a consumer who has been verified and assuming the information to be provided in response has been properly identified,[6] the next hurdle is *how* to deliver the data to the consumer.

The CCPA states that disclosure and delivery is to be "free of charge to the consumer." Further, it describes: "The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance." Cal. Civ. Code § 1798.100(d); *see also* § 1798.130(a)(2).

1 See Cal. Code Regs. tit. 11, §§ 999.300 et seq. (proposed Feb. 10, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf (last visited Mar. 27, 2020).

2 Such requests are for information collected, disclosed or sold within the preceding 12 months. Cal. Civ. Code § 1798.130(a)(2); Proposed Regs, § 999.313(c).

3 This means that the deadline to confirm receipt of the request and the deadline to respond to a verified request run simultaneously.

4 This calendar day approach for a substantive response to the request (Proposed Regs, § 999.313(b)) is distinct from the business day approach for the confirmation of the receipt of the request (Proposed Regs, § 999.313(a)).

5 See Proposed Regs, § 999.313(b).

6 These are each important topics in their own right but are not discussed in this particular piece.

The Proposed Regs provide some additional guidance, saying that "[a] business shall use reasonable security measures when transmitting personal information to the consumer." Proposed Regs, § 999.313(c)(6).

"Reasonable security measures" is not a defined term and would vary by method of transmittal. "Reasonable" could also depend on the nature of the information being sent.

Delivery may be via mail or other delivery service. This approach could provide paper copies of information that are "readily useable" by a consumer, but it is possible that a consumer could argue that the data is not presented in an understandable, and thus not "readily useable", format. Copies of disks or drives containing the information could also be sent this way, although the electronic data may not be "readily useable", an undefined phrase, by the consumer because of formatting or lack of access to necessary software. In addition, it may be inconvenient or difficult for the consumer to send on the information received to "another entity without hindrance," which is also an undefined phrase. There is also some security risk around mail or other physical delivery but "reasonable security measures" could include, among other steps, confirming the mailing address, insuring the physical integrity of the package upon sending, and requiring a signature at delivery. As noted, evaluating the reasonableness of security measures may depend on the nature of the responding business, the type of information involved, and other factors.

Alternatively, electronic delivery of the data is an option, but consideration will need to be given to whether to send the information itself by email or to instead send by email instructions for how to access the information. For example, an email could attach documents. This approach could present security concerns, particularly if encryption is not used or if the consumer's email address is for a free email account. In addition, the consumer may not be able to receive certain kinds of attachments or larger volumes of attachments. Also, as with physical delivery, the consumer may not find the information "readily useable" because of formatting or lack of access to required software.

An email could also provide directions to have the consumer log into an existing account (if one exists) to obtain documents. The Proposed Regs allow the following: "If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4 [of the CCPA]." Proposed Regs, § 999.313(c)(7). If a consumer did not have an existing password-protected account with the responding business, the business could send a secured link to a portal, whether maintained by the business or by a third-party vendor.

Each electronic method could face security risks, but "reasonable security measures" could include confirming the accuracy of an email address, requiring a password or other access verification, and encrypting the information. Again, reasonableness of security measures will likely be considered in the context of the type of business that is providing the information, the nature of the information being sent to a consumer, and so on.

In addition, whatever electronic approach is employed, the format will also need to be assessed. Although formats such as .doc and .txt are relatively universal and easy to transmit to "another entity without hindrance", those formats risk being altered. Alternatively, the use of a locked .pdf (portable data format) document may be a more secure possibility.

Regardless of the method of electronic delivery, two things must be certain: (1) the delivery method must utilize "reasonable security measures" to protect the information from, for example, unintended disclosure to unauthorized persons, and (2) the format must be "readily useable", as required by the CCPA, such that "the consumer [can] transmit this information to another entity without hindrance."

So, the CCPA invites consumer requests to "show me the data" – but only in a "readily useable" manner that permits sending the data on to another "without hindrance" and only through the use of "reasonable security measures".

NIST Privacy Framework Released

By Stephen B. Anastasia and Thomas J. Smedinghoff

On January 16, 2020, the National Institute of Standards and Technology (NIST) released its Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (the "Privacy Framework") Version 1.0.[1]

The NIST Privacy Framework is not a law or regulation, but rather a voluntary tool that can help organizations manage privacy risk arising from their products and services, as well as demonstrate compliance with laws that may affect them, such as the California Consumer Privacy Act and the European Union's General Data Protection Regulation. It helps organizations identify the privacy outcomes they want to achieve and then prioritize the actions needed to do so.

NIST initially released a draft version of the Privacy Framework for public comment in September 2019. Among the key goals on which it sought feedback were whether the Framework: (1) adequately addressed privacy practices currently in use, including widely used voluntary consensus standards; (2) enabled organizations to use it in conjunction with the Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework")[2] to collaboratively address privacy and cybersecurity risks; and (3) enabled organizations to adapt to privacy risks arising from emerging technologies such as the Internet of Things and artificial intelligence.[3]

After incorporating feedback from industry subject matter experts, version 1.0 of the Privacy Framework aims to support organizations in fostering customer trust by promoting ethical, privacy-focused decision making, fulfilling compliance obligations, and facilitating communication about privacy practice with individuals, business partners, assessors, and regulators.

The Privacy Framework provides a common language for understanding, managing, and communicating privacy risk. The flexibility and interoperability of the Privacy Framework allows it to be used by any business of any size in any data processing ecosystem. Additionally, it can be used to assist in identifying and prioritizing actions for reducing privacy risk, while serving as a tool for managing that risk across different sectors of an organization.

The Privacy Framework uses a structure similar to the Cybersecurity Framework to facilitate the use of both frameworks in tandem. Like the Cybersecurity Framework,

the Privacy Framework is comprised of three parts: the Core, Profiles, and Implementation Tiers ("Tiers").

The Core is a set of privacy activities and outcomes that allow for communicating priorities related to activities and outcomes across an organization from the c-suite level to the operations level. The Core comprises five functions that organize foundational privacy activities at their highest level. They aid an organization in expressing its management of privacy risk by understanding and managing data processing, enabling risk management decisions, determining how to interact with individuals, and improving by learning from previous activities. The functions are then broken down into categories and subcategories, which are discrete outcomes for each Function. The five high-level functions for managing privacy risks arising from data processing are:

- Identify-P. Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
- Govern-P. Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
- Control-P. Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
- Communicate-P. Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.
- Protect-P. Develop and implement appropriate data processing safeguards.

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization

1 https://www.nist.gov/privacy-framework/privacy-framework

2 The Cybersecurity Framework was initially published in 2014, and revised during 2017 and 2018, with version 1.1 being released in April 2018. The Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. https://www.nist.gov/cyberframework/new-framework#background.

3 https://www.nist.gov/system/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf

has prioritized to help it manage privacy risk. They represent the organization's ongoing privacy activities/desired outcomes. When developing a Profile, an organization will review all of the activities/outcomes in the Core to determine which to focus on based on a number of factors, including the business mission, data processing ecosystem roles, types of data processing, and the privacy needs of individuals.

Profiles can be used to identify opportunities for improvement, to conduct self-assessments, and to communicate within an organization about how privacy risks are managed. Organizations are encouraged to develop target Profiles, to identify gaps in their current practices, and identify what actions need to be adjusted to achieve their target goal.

Tiers provide a reference point for how organizations view specific privacy risks, and for determining whether sufficient controls, processes, and resources are in place to handle said risk. Tiers support decision making about how to manage privacy risks, and allow organizations to communicate internally about the allocation of resources needed to progress to the next Tier.

The four Tiers are defined as Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). Based on the specific needs of an organization, it is not necessary to progress to Tier 4 in all areas. Successful implementation of the Privacy Framework is contingent upon achieving the desired outcomes set in an organization's target Profile.

Additionally, the Privacy Framework lays out best practices organizations should utilize to achieve their goals under the Privacy Framework including mapping to informative references, strengthening accountability, establishing a "ready, set, go" privacy program, applying the system development life cycle, identifying the organization's role within a data processing ecosystem, and informing buying decisions.

Because the Privacy Framework is not a law or regulation, its purpose is not to enforce compliance with federal or state regulatory requirements. Rather, it serves as the structure in which privacy professionals can insert the controls necessary for their organization to become, and remain, compliant with applicable privacy law. The Privacy Framework allows organizations of all sizes to better map privacy and compliance requirements, while remaining flexible to modify the privacy program at every level. This inherent flexibility eliminates the need to overhaul an organization's privacy program every time a new restrictive regulation is passed. The widespread adoption of the Privacy Framework by business will also help raise the standard for privacy protection generally, and ultimately create a safer environment for the individuals those organizations serve.

Much like the Cybersecurity Framework, it is likely the Privacy Framework will be adopted as the foundation organizations use to build their privacy program from the ground up. The ease with which the Privacy Framework can be tailored for any business makes it ideal for the ever-changing regulatory landscape in which organizations must operate.

Brexit and GDPR

By Andrew Shindler

Introduction

GDPR and Brexit are two expressions that have struck fear and confusion into Europeans in recent years. What happens when you put them together?

To quote former UK Prime Minister, Theresa May, the short answer is that "*nothing has changed*" and nothing is likely to change until the end of the year. Then all bets are off.

Withdrawal

The United Kingdom withdrew from the European Union on 31 January under the European Union (Notification of Withdrawal) Act. It did so on the terms of the UK/EU Withdrawal Agreement of 19 October 2019. That Withdrawal Agreement provides for a transition period lasting until 31 December 2020, or such later date as may be agreed.

The Withdrawal Agreement maintains the status quo with regard to data protection throughout the transition period. Specifically:

- Article 71 provides that GDPR will continue to protect data subjects outside the UK, where their personal data is processed in the UK during the transition period, unless the EU Commission makes an earlier determination that UK law provides an adequate level of protection under GDPR Article 45; and
- Article 73 provides that, during the transition period, the EU will treat personal data obtained from the UK in the same manner as it treats data from Member States.

After Transition

The hope is that the UK and EU will reach a wide-ranging trade agreement during the transition period. This would include either an agreement on mutual treatment of personal data or a reciprocal deal with the EU and the UK making cross - adequacy decisions, which would have the same effect. If this happens, then, indeed, little will change.

If the two sides cannot reach a trade agreement, they may nevertheless make adequacy decisions, allowing personal data to continue to flow freely between the EU and the UK. However, for political or other reasons the EU and UK may refrain from making those decisions in the absence of a wider deal. In that case, the UK becomes a genuine "third country" and organisations would need to put in place special measures to allow EU-UK transfers, such as using the EU model clauses. In addition, US organisations subject to GDPR may need to appoint a data protection representative both in the EU and the UK.

Conclusions

For the next few months, Brexit and GDPR is a question of "*watch this space*". The position will need to be re-assessed toward the end of the year, when we may be able to predict whether a deal or adequacy decisions is likely.

June 30, 2020 Deadline Quickly Approaching to Render Unreadable ACH Account Numbers

By Patrick J. Hatfield

Effective June 30, 2020, companies that are not regulated banks who initiated (as debit or credit entries) 6 million or more ACH transactions (with consumers or businesses) in 2019 will need to comply with a new National Automated Clearing House Association ("NACHA") security rule. The NACHA Rules govern participating banks and their customers and how they initiate auto-payments to and from bank accounts via the automated clearinghouse.

The new data security rule requires rendering "unreadable" the bank account number of the person whose account is debited or credited while that account data is at rest. The rule does not apply to the account data in paper format. It is common practice for companies to scan or image signed ACH authorizations. The electronic record containing that bank account number on the paper authorization is subject to the new rule.

Typically, a company collecting funds from consumers (such as periodic insurance premiums) or paying individuals (such as employers paying employee wages and expense reimbursements) enters an agreement with its bank and in that agreement, the company promises to comply with the NACHA Rules. This is how companies are bound to the NACHA Rules. Sanctions for non-compliance can be significant.

The new data security rule takes effect for high-volume initiators (credits or debits) on June 30, 2020. A company initiating six million or more debits or credits in 2019 is a high-volume initiator. Initiators having an annual volume greater than 2 million transactions in 2020 will need to comply with the new rule by June 30, 2021.

Other NACHA Rules require companies using ACH authorizations to debit a consumer's account to be able to promptly provide a full copy of the consumer's signed authorization, or risk forfeiture of the amounts collected via ACH. For this reason, companies will need to render "unreadable" the consumer's account detail in a way that still enables the company to reproduce that ACH authorization in readable form again, if asked to produce the signed authorization.

The FAQs for the new security rule point to the Payment Card Industry (PCI) Data Security Standards for permissible methods to render the account information "unreadable" through encryption. The PCI standards provide examples of encryption methods and implementation guidance.

The new NACHA Rule applies also to third party service providers in the process of handling ACH transactions. The FAQs for the rule describe how the volumes of a given service provider's customers are to be aggregated to determine if that service provider exceeds the phase-in threshold of 6 million.

One potential difficulty that organizations may face in implementing the new rule may be to identify where all the ACH authorization data is located, so the appropriate elements can be rendered unreadable. There may be e-discovery tools available that can help.

Implementing the solution to this new rule is also an appropriate time for initiating companies (referred to as "Originators" in NACHA-speak) and third-party service providers alike to revisit their contracting approach to define responsibility for compliance with this new NACHA Rule and the NACHA Rules overall.

New York SHIELDs Private Information (Security Requirements Effective March 21, 2020)

By Laura L. Ferguson and Stephen B. Anastasia

As we first reported on July 24, 2019 (and updated on September 24, 2019), an amendment of New York's data breach notification law—the Stop Hacks and Improve Electronic Data Security Act, commonly referred to as the SHIELD Act—was signed into law on July 25, 2019. While the breach notification amendments of the SHIELD Act went into effect on the ninetieth day after being signed into law—October 23, 2019—the security requirements of the SHIELD Act officially went into effect on March 21, 2020—the two hundred fortieth day after the SHIELD Act was signed into law.

Data Security Obligations

The SHIELD Act added a requirement that covered entities implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information, including the disposal of data. In order to be in compliance, a business must implement a data security program that includes reasonable administrative, technical and physical safeguards, including:

- **Administrative safeguards.** (1) designates one or more employees to coordinate the security program; (2) identifies reasonably foreseeable internal and external risks; (3) assesses the sufficiency of safeguards in place to control the identified risks; (4) trains and manages employees in the security program practices and procedures; (5) selects service providers capable of maintaining appropriate safe guards, and requires those safeguards by contract; and (6) adjusts the security program in light of business changes or new circumstances.
- **Technical safeguards.** (1) assesses risks in network and software design; (2) assesses risks in information processing, transmission and storage; (3) detects, prevents and responds to attacks or system failures; and (4) regularly tests and monitors the effectiveness of key controls, systems and procedures.
- **Physical safeguards.** (1) assesses risks of information storage and disposal; (2) detects, prevents and responds to intrusions; (3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

Small businesses are permitted to scale the above reasonable security requirements as appropriate for the size and complexity of the business, the nature and scope of the business' activities, and the sensitivity of the personal information the business collects. In addition, a business is deemed to be in compliance with the above reasonable security requirements if the business is subject to and in compliance with GLBA, HIPAA, part 500 of title 23 of the official compilation of codes, rules and regulations of the state of New York, or any other data security rules and regulations of any official department, division, commission or agency of the federal or New York state government.

For a full breakdown on the amendments to the SHIELD Act click here to view our September 24, 2019 article, and be sure to Locke-down your SHIELD Act compliance procedures.

Morrison Escapes Responsibility for Cyber-Rogue Employee – The Limits of Vicarious Liability

By Andrew Shindler

On 1 April 2020, the UK Supreme Court handed down its judgment in *WM Morrison Supermarket v. Various Claimants*. The Court's decision, significant under both data protection law and the general law of tortious liability, will come as a relief to all businesses, whatever their size, who employ people to carry out activities in the UK.

Background

The case concerned an appeal by WM Morrison, the supermarket chain, against a 2018 Court of Appeal decision rejecting its earlier appeal against a High Court ruling.

Both the High Court and the Court of Appeal ruled against Morrison in favour of nearly 10,000 current or former employees. Specifically, both courts had held Morrison vicariously liable for the unlawful actions of another employee, Andrew Skelton, who worked in its internal audit team at the relevant time.

Skelton harboured a grudge against Morrison because of disciplinary action it had previously taken against him. With the sole intention of damaging it, he surreptitiously copied the payroll data of Morrison's entire workforce, over 100,000 people, onto a personal USB stick while sending it to KPMG, its external auditor, as part of his duties. A couple of months later, in January 2014, Skelton uploaded a file containing the data to a public website, using a false email account set up in the name of another employee. He also posted links to the data on other websites.

This data breach did not become widely known and did not have the harmful effect on Morrison that Skelton desired. So, in March 2014, as Morrison was due to announce its 2013 financial results, Skelton sent the file anonymously to three UK newspapers pretending to be a concerned member of the public. One of the newspapers alerted Morrison. The police were involved and swiftly detected and arrested Skelton. He was convicted and sentenced to eight years' imprisonment for fraud, securing unauthorised access to computer material and disclosing personal data. Morrison spent over £2 million in dealing with the aftermath.

Legal Proceedings

The claimants brought proceedings against Morrison arising out of Skelton's misuse of their personal payroll data. Their claim was for breach of confidence, breach of the Data Protection Act 1998 (DPA), and misuse of private information. They claimed damages for "distress, anxiety, upset and damage." Although the claim related to the 1998 DPA, the issues in the case apply equally to the GDPR and the UK's related 2018 DPA.

The High Court ruled that Morrison was not primarily liable for any of the claims, Skelton's acts not being authorised by it. However, it did hold Morrison vicariously liable for Skelton's acts.

Morrison appealed. The Court of Appeal dismissed its appeal on similar grounds to the High Court. It ruled:

- the DPA did not exclude causes of action for misuse of private information or breach of confidence;
- The DPA did not exclude the principle of vicarious liability; and
- Morrison was vicariously liable because Skelton's wrongful acts were *"within the field of activities assigned to him …. The relevant facts constituted a seamless and continuous sequence … or unbroken chain of events."*

Morrison appealed again, to the highest court in the UK, on the grounds that this was a point of law of public importance in which the lower courts had reached the wrong conclusion.

The Supreme Court's Decision

The President of the Court, Lord Reed, gave the leading judgment in a unanimous decision. The predominant issue was whether, on the facts and applying the law, Morrison was vicariously liable for Skelton's actions. Analysing previous case law, Lord Reed stated that the general principle (which applied in all but certain exceptional categories of case) is that employers are vicariously liable to third parties where their employees' wrongful conduct is

"so closely connected with acts [they are] authorised to do that … it may fairly and properly be regarded as done by [them] while acting in the course of [their] employment."

His Lordship went on to explain that this principle must be applied with regard to the circumstances. He emphasised: *"'Fairly and properly' is not an invitation … to judges to decide cases according to their personal sense of justice but requires them to consider … the guidance derived from decided cases."*

Lord Reed concluded that the lower courts had erred in their decisions, based on their misinterpretation of the previous Supreme Court case on vicarious liability, *Mohamud v WM Morrison* (2016). In that case, Morrison was held vicariously liable for its petrol station attendant's violent assault on a customer he was serving in the course of his duties.

Lord Reed ruled that the "close connection" test is not based on a temporal or causal connection or a matter of social justice. He considered that the lower courts had taken references in *Mohamud v Morrison* to 'an unbroken sequence of events' out of context and given them an unmerited significance. They had also wrongly discounted Skelton's motive. The following factors were particularly important:

- Disclosing data on the internet was not part of Skelton's functions.
- A temporal or causal connection does not itself satisfy the close connection test.
- It was highly material that Skelton's motive was personal rather than for his employer's business.

The Supreme Court had therefore looked at the facts afresh and compared them to those of previous cases. The key distinction in past cases was between circumstances where employees were engaged, however misguidedly, in furthering their employers' business and those where they were solely pursuing their own interests — to use the time honoured phrase — *"on a frolic of [their] own."* Here, Skelton was pursuing a personal vendetta and his conduct did not meet the close connection test.

The second issue in the appeal was whether the DPA excluded the imposition of vicarious liability. This was of theoretical interest only in the case, given the finding that Morrison was not vicariously liable for Skelton's acts, but is important for future cases where the acts of an employee breach implicate GDPR or other data protection laws. Morrison's argument was a technical construct based on Skelton rather than Morrison being the data controller of the data he unlawfully published. The Court was entirely unpersuaded that there was any explicit or implicit exclusion of vicarious liability in GDPR or the DPA and rejected this argument out of hand.

Conclusions

The Supreme Court's decision will come as welcome relief to Morrison and its insurers, which faced potentially huge financial liability to around 100,000 possible claimants.

The decision will also provide some comfort to other organisations, and their insurers, that they will not be liable for wrongful acts of their employees, which has some connection, however tenuous, with their employment.

However, there remains a reasonably fine line between the circumstances in which the "closely connected" test for vicarious liability is satisfied and those in which it is not. Employers should therefore remain prudent and base their risk management decisions on the general principle that they will usually be liable for their employees' acts, where those acts reasonably relate to their employment.

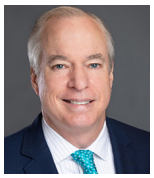
With regard to vicarious liability in the context of data protection and its sister, cyber-security, it is no surprise that English courts will hold employers vicariously liable for breaches of GDPR and other data protection laws committed by their employees where "closely connected" with their employment. This decision does not therefore reduce the need for good data protection practice in the workplace, including training employees and monitoring their knowledge, awareness and compliance. These remain essential to avoid or reduce the risk of GDPR fines, negative publicity and liability for compensation.

OUR AUTHORS:

Stephen B. Anastasia
Associate
New York
212-912-2742
stephen.anastasia@lockelord.com

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Laura L. Ferguson
Partner
Houston
713-226-1590
lferguson@lockelord.com



Patrick J. Hatfield
Partner
Austin
512-305-4787
phatfield@lockelord.com

Matthew Murphy, Editor
Associate
Providence
401-276-6497
matthew.murphy@lockelord.com

Andrew Shindler
Partner
London
+44 (0) 20 7861 9077
andrew.shindler@lockelord.com

Thomas J. Smedinghoff
Of Counsel
Chicago
312-201-2021
tom.smedinghoff@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

Practical Wisdom, Trusted Advice.

www.lockelord.com

Atlanta | Austin | Boston | Brussels | Chicago | Cincinnati | Dallas | Hartford | Hong Kong | Houston | London | Los Angeles
Miami | New Orleans | New York | Princeton | Providence | San Francisco | Stamford | Washington DC | West Palm Beach