Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

NOVEMBER 2019

IN THIS ISSUE

1 CCPA Proposed Regulations Are Out!

2 Deletion Completion Under the CCPA

3 Looking Ahead to the CCPA's "Look Back" Requirement

4 Summary Comparison of CCPA With California Financial and Insurance Privacy Laws

4 EU's Top Court Makes Key "Right to Be Forgotten" Decision

6 New York SHIELDs Private Information

8 Proposed Changes to Regulations Governing the Confidentiality of Substance Abuse Disorder Treatment Records Reflects Concerns About Opioid Crisis

9 Drone Operators Concerned With DJI Cybersecurity Concerns Have Few Options

10 Our Authors

CCPA

CCPA Proposed Regulations Are Out!

By Theodore P. Augustinos and Paul B. Sudentas

On October 10, 2019, the California Office of the Attorney General (AG) published the long-awaited proposed text of the California Consumer Privacy Act Regulations (the "Proposed Regs"). The Proposed Regs provide guidance on how covered businesses are to comply with California Consumer Privacy Act of 2018 (CCPA). In preparing these Regulations, the AG received over 300 written comments and held seven public forums.

Before the Proposed Regs are finalized and promulgated, the AG will hold four public hearings (December 2-5, 2019) to allow opportunity for statements or comments concerning the Proposed Regs. In addition, the AG will allow written comments regarding the Proposed Regs made before 5:00 pm PST on December 6, 2019.

Highlights of the Proposed Regs include:

- The Notice (at the time personal information (PI) is collected) must include the list of categories of PI and, for each category, the categories of sources, business or commercial purpose for which it will be used, and the categories of third parties with whom the business shares PI;
- The "Do Not Sell My Personal Information" link is only required if the covered business sells consumers' PI;
- Notice is not required from businesses that do not collect PI directly from consumers, but the PI cannot be sold unless the consumer is contacted or the source of the PI is contacted with notice;

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

- Businesses shall use a two-step process for online requests to delete PI: the consumer must first make the request to delete and then the consumer must separately confirm that they want their PI deleted;
- If a request to delete cannot be verified, the business shall treat the request as a request to opt-out of sale;
- Businesses that store PI in archives or backup systems do not need to delete the PI until the archived or backup system is next accessed or used;
- A person or entity directed by a business to collect PI is considered to be a service provider;
- A service provider that is a business shall comply with the CCPA;
- A request to opt-out does not need to be a verifiable consumer request; and
- Businesses must maintain records of consumers' requests for at least 24 months and may maintain information therein so long as it is not used for any other purpose other than record-keeping.

Deletion Completion Under the CCPA

By Molly McGinnis Stine and Paul B. Sudentas

The effective date for the California Consumer Privacy Act (CCPA) is January 1, 2020. With fewer than 60 days remaining, covered businesses must be ramping up to meet the requirements of the CCPA. The CCPA affords several rights to California residents (as the term "consumer" is defined by the Act) as to personal information collected by a covered business. Among these rights is: (1) the right to request disclosure of personal information collected and uses therefor (§ 1798.110(a)); (2) the right to request deletion of personal information collected by the covered business (§§ 1798.105(a) and (c)); and (3) the right to receive that information from the covered business (§ 1798.100(d)).[1]

This article focuses on the second – the consumer's right to request deletion of personal information, often called the "right to be forgotten." This right obligates covered businesses, which must obligate their service providers. Under § 1798.105:

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

* * *

(c) A business that receives a verifiable consumer request to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

If the Proposed Regs are adopted, we note that before any information is deleted, the covered business must acknowledge within 10 days the receipt of the verifiable consumer request to delete. *See* Proposed Regs § 999.313(a).

What must be deleted?

But, what does "delete" mean in the context of the CCPA? Absent a definition, the CCPA simply requires that a covered business remove from its files the requesting consumer's personal information. We stress that the 12-month look back pertaining to requests to identify information that is collected does not apply to the deletion requirement. Instead, personal information collected, regardless of when collected, must be deleted in response to a request for deletion. The proposed California Consumer Privacy Act Regulations ("Proposed Regs"), issued by the California Attorney General, note in § 999.313(d)(7) that, if the regulations are adopted as presented, a business may present the consumer with the choice to delete select portions of their personal information but only if an option is available to delete *all* of the consumer's personal information.

While the language of the CCPA leaves open the issue of the extent to which a covered business must go to its archives and back-ups and delete all personal information from those locations as well, the Proposed Regs explain that, if the regulations are adopted as presented, personal information stored in archives or backup systems must be deleted, but the deletion may be delayed:

> If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next assessed or used.

Proposed Regs at § 999.313(d)(3).

1 This third right will be addressed in a future publication.

What are exceptions to the deletion requirement?

There are, however, exceptions to the deletion requirement. Section 1798.105(d) allows a covered business to forego deletion if the information is necessary to perform any of nine specified activities including, for example, completing the transaction for which the personal information was collected, detecting security incidents, exercising free speech, engaging in public or peer-reviewed scientific, historical, or statistical research, and complying with a legal obligation.

In addition, § 1798.145 identifies other exceptions to the mandates of the CCPA, providing that the deletion requirement, shall not restrict a business's ability to perform various tasks including complying with federal, state, and local laws, exercising or defending legal claims, using deidentified or aggregated consumer information, or collecting or selling a consumer's personal information if every aspect of the commercial conduct takes place whole outside of California.

The definition of "personal information" is also helpful in that it does not include deidentified, aggregated, or pseudonymized information in its definition of "personal information." Thus, it appears that only personal information, as defined, must be deleted, but information that does not permit reasonable identification of a consumer—such as, deidentified, aggregated, or pseudonymized information—is not required to be deleted.

What to do after personal information is deleted?

Once personal information is deleted, then what? Although the CCPA, as amended, does not specifically require a covered business to provide the consumer with any type of confirmation that his/her personal information has been deleted, the Proposed Regs shed some light on the subject. If adopted, the covered business must respond to the consumer's request to delete within 45 days, with the possibility of extending the time to respond by an extra 45 days. See Proposed Regs § 999.313(b). In addition, the Proposed Regs require that upon deletion of the consumer's personal information the covered business must: (1) specify the manner in which it has deleted the personal information, and (2) disclose that it will maintain a record of the consumer's request to delete. See Proposed Regs §§ 999.313(d)(2), (4) and (5). As a practical matter, we encourage covered businesses to include a written confirmation that the personal information has in fact been deleted. Such confirmations may serve business purposes, such as to satisfy internal audit requirements for documentation that deletion was complete, or to establish compliance for potential litigation, enforcement or regulatory proceedings. Confirmations should have sufficient information to show that the covered business timely complied with the requirement. Any information retained about the deletion of a consumer's personal information may remain in conflict with the request to delete personal information unless the retained information falls under an exception in § 1798.105(d) or § 1798.145 or is used solely for record-keeping purposes. We note that Proposed Regs § 999.313(d)(5) require, if adopted as presented, that the covered business "disclose that it will maintain a record of the request pursuant to Civil Code section 1798.105(d)." The records will be maintained for at least 24 months, and the maintenance of such records, where the information is not used for any other purpose, is not a violation of the CCPA. See Proposed Regs. § 999.317(b)-(f).

Looking Ahead to the CCPA's "Look Back" Requirement

By Molly McGinnis Stine and Paul B. Sudentas

Under the California Consumer Privacy Act (CCPA), covered businesses must comply with myriad requirements starting January 1, 2020. Within those requirements, covered businesses must be prepared to deal with the "look back" requirement. Under the CCPA, the disclosure of information to California consumers must cover—that is, "look back" at—the 12-month period preceding the date upon which the covered business receives a verifiable consumer request. See Cal. Civ. Code § 1798.130(a).

As we previously discussed, a California consumer may submit to a covered business a "verifiable consumer request" for certain specified information about their personal information. See Cal. Civ. Code § 1798.100(c). For example, within 45 days, a covered business must provide the categories and the specific pieces of personal information collected, sold, and/or disclosed, the categories of sources from where the personal information was collected, the business or commercial purpose for which the personal information was collected, and the categories of third parties with whom the personal information is shared, for the 12-month period preceding the request. See Cal. Civ. Code § 1798.130(a)(2). Further, the response "may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance." See Cal. Civ. Code § 1798.100(d).

Ideally, because the CCPA goes into effect on January 1, 2020, all covered businesses would have already

implemented policies and procedures to be able to identify the requisite information starting January 1, 2019. For those covered businesses that have not yet implemented such policies and procedures, it is imperative to begin now, even if work should or could have started sooner.

Covered businesses should at least:

1. identify and map all of the information required under the CCPA going back to January 1, 2019;
2. implement policies, procedures, and training for the collection and retention of such information going forward; and
3. implement procedures that will allow for ready access to the information so as to comply with the 45-day response period to provide such requested information.

Although enforcement of the CCPA will begin no later than July 1, 2020, compliance must be in place by January 1, 2020. One must work under the assumption that the Attorney General's enforcement on July 1, 2020 will retroactively look to a covered business's compliance as of the effective date of the CCPA.

There are two exceptions to the "look back" requirement where the covered business need not disclose information collected for the 12-month period preceding the request:

The same information need not be provided to the same consumer more than twice within a 12-month period. See Cal. Civ. Code § 1798.100(d).

Information need not be retained if used for a single, one-time transaction or if the information will not be sold or retained by the covered business. See Cal. Civ. Code § 1798.100(e).

Summary Comparison of CCPA With California Financial and Insurance Privacy Laws

By Elizabeth Tosaris and Paul B. Sudentas

As the world is now well-aware, the California Consumer Privacy Act of 2018 (CCPA) takes effect on January 1, 2020 with enforcement beginning July 1, 2020. The CCPA is not, however, the first consumer privacy act to make it through the state legislature, even though it seems to be garnering a significant share of the limelight. California privacy laws implicate a number of economic sectors including financial institutions, insurance companies, and medical providers. This chart compares the CCPA to financial- and insurance-related privacy laws.

Three of the financial and insurance California privacy laws that impact a large number of businesses that conduct business in California are: (1) the Insurance Information and Privacy Protection Act (IIPPA), (2) the California Financial Information Privacy Act (CFIPA), and (3) the Consumer Credit Reporting Agencies Act (CCRAA). Whether the privacy of a California resident's personal information is governed by one or more of the CCPA, IIPPA, CFIPA, or CCRAA depends largely on the business that possess the resident's personal information. The CCPA, IIPPA, CFIPA, and CCRAA differ in various ways and require that businesses remain cognizant of what privacy act(s) to which they must adhere. Here, we provide a side-by-side summary comparison of the CCPA, IIPPA, CFIPA, and CCRAA.

Please note that while all of these laws deal with privacy, they are in fact different in application and in scope, and compliance with one of them does not necessarily mean that there is complete compliance with any of the others. As a practical matter, different industries are going to be subject to different acts; the CCPA, however, puts on an overlay that (so far) applies to a large number of businesses.

EU's Top Court Makes Key "Right to Be Forgotten" Decision

By Andrew Shindler, Molly McGinnis Stine and Stephen B. Anastasia

On 24 September 2019, the European Union's top court issued a landmark ruling declaring that Google does not have to extend the "right to be forgotten" rules to its search engines globally.[1] This decision provides important guidance about this right, one of the well-known provisions of the General Data Protection Regulations (GDPR).

Prior Treatment of the "Right to Be Forgotten"

The "right to be forgotten" originates from a 2014 decision, where a Spanish businessman successfully argued that it was contrary to data protection law for links to 12-year-old news reports revealing his financial difficulties to come up against Google searches of his name. The decision was based on the principle that the data in the search results was no longer relevant and was excessive.[2]

1 Judgment in Case C-507/17, Google LLC, successor in law to *Google Inc. v Commission nationale de l'informatique et des libertés* (CNIL) (2019), accessed HERE.

2 Judgment in Case C-131/12, Google Spain SL, *Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014). Google was required to remove links to search engine results that "appear to be inadequate, irrelevant or no longer relevant or excessive in the light of the time that had elapsed…."

As a result of this right, subsequently replicated in GDPR[3], it is open to EU individuals to request Google to "de-reference" data from search results linked to their name. Google receives well over 100,000 such requests per year, nearly half of which it finds justified. When Google delists the results, it does so only on EU domains, such as Google.co.uk or Google.fr, and not on Google.com or other non-EU domains.

2019 Ruling's Limitation on the Geographic Scope of the "Right to Be Forgotten"

The 2019 ruling stems from a 2015 dispute between Google and the Commission nationale de l'informatique et des libertés (CNIL), the French data protection supervisory authority. In 2015, CNIL required Google to delist results from all of its search engine domains to effectively protect individuals' rights. Google refused. CNIL then fined Google €100,000. Google appealed to the Court of Justice of the European Union (CJEU), arguing that European authorities should not extend their own privacy rules around the world, where they might infringe other laws such as the right to freedom of expression.

In the court proceedings, Google explained that it had implemented a new system, under which users are automatically directed to the national version of the search engine corresponding to the place where they are conducting the search, as determined by its geo-location process. So even if French users searched Google.com, they would get the results from Google.fr.

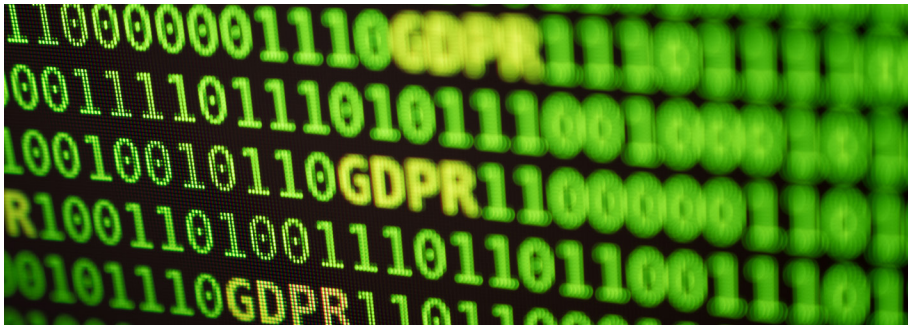
The CJEU first confirmed that Google was subject to GDPR, even though its search engine operated from the US, because the engine obtained financial benefit from advertising activities carried out by Google's French subsidiary.

The Court went on to note that internet search results are ubiquitous and likely to have immediate and substantial effects on people within the EU. This justified EU law requiring a search engine operator to de-reference results from all versions of its search engine, on a worldwide basis. Nevertheless, the Court then emphasized the following points:

- Many non EU states do not recognize the right to be forgotten, in this case a de-referencing right;
- The right to protect personal data must be balanced against other fundamental rights such as the freedom of internet users; this balance varies significantly around the world;
- It was not apparent from the GDPR that it imposed, on operators, a de-referencing operation which extended to the national versions of its search engines located in countries outside the EU.

The CJEU concluded that "[c]urrently, there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject...to carry out such a de-referencing on all the versions of its search engine." However, the ruling further stated, "EU law requires a search engine operator to carry out such a de-referencing on the versions of its search engine corresponding to all the Member States and to take sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights."

Therefore, Google, and other operators, do not need to de-reference links containing personal data from search results on their non EU search engines. They are, however, subject to an obligation to prevent or seriously discourage internet users in the EU from gaining access to the non-EU links concerned. In other words, users in the EU who try and search on Google.com must be automatically directed to the applicable EU google search engine in their own country, and will only obtain de-referenced results.



The Future of the "Right to Be Forgotten"

That may not be the end of the matter. In a final aside, the CJEU emphasized that an authority of an EU member state remained competent to order "where appropriate" a search engine operator to de-reference data from all versions of its search engines, both EU and non-EU. This suggests there may be exceptional cases, but the scope of this exception is at best uncertain.

3 The GDPR provides the "right to erasure ('right to be forgotten')." See Art. 17, Regulation (EU) 2016/679 (General Data Protection Regulation). Specifically, the regulation states, "[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay…" under certain conditions. According to the regulation, personal data must be erased where one of the following grounds exists: (1) the data is no longer needed for its original processing purpose, (2) the data subject has withdrawn his or her consent and there is no other legal ground for processing, (3) the data subject has objected and there is no overriding legitimate grounds for the processing, or (4) erasure is required to fulfil a statutory obligation under the EU law or the right of the Member States. Additionally, data must be erased if it was unlawfully processed in the first place. Members of the public can make a request to any organization either verbally or in writing, and the recipient of such request has one month to respond.

In practice, the result in this particular case is that internet users in, say, North America might obtain more comprehensive search results than users in Europe when they search against a person's name.

On a conceptual level, this judgment represents a balanced approach. While still claiming GDPR jurisdiction over non-EU organizations with activities in the EU, the European Court has recognized that there are territorial limits to its effect ("[t]he balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world…."). It remains to be seen whether this approach has wider implications for the application of GDPR to the non-EU activities of organizations subject to GDPR but based outside the EU.

New York SHIELDs Private Information

By Laura L. Ferguson and Paul B. Sudentas

New York's latest attempt to strengthen its breach notification requirements to protect New York residents' private information[1]—the Stop Hacks and Improve Electronic Data Security Act, commonly referred to as the SHIELD Act (S5575-B)—was signed into law on July 25, 2019. The breach notification amendments of the SHIELD Act went into effect on the ninetieth day after being signed into law—October 23, 2019—while the security requirements of the SHIELD Act go into effect on the two hundred fortieth day after the SHIELD Act was signed into law—March 21, 2020. The SHIELD Act follows in the footsteps of other states that have already revamped their data security laws. The SHIELD Act amends N.Y. Gen. Bus. Law § 899-aa and N.Y. State Tech. Law § 208, and adds new Gen. Bus. Law § 899-bb.

Key Changes to the Breach Notification Obligations

Below is a quick summary of the key changes to the breach notification obligations made as a result of the SHIELD Act:

- Broadens the notification obligations as a result of a breach to include notification to residents whose private information was, or is reasonably believed to have been, accessed by an unauthorized individual (instead of just notification to those residents whose information was acquired).
- Exempts breach notifications when the exposure to private information was inadvertent and the covered entity[2] "reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials." The covered entity must maintain documentation of the determination for at least five years, and in the event there were over 500 New York residents impacted by the inadvertent disclosure, the State Attorney General must be notified within 10 days of the determination.
- Expands the definition of "private information" to include (i) the combination of a user name or email address with a password or security question and answer thereto that would allow access to an online account, and (ii) personal information in combination with the following newly added data elements:
  1. account, credit or debit card numbers without additional identifying information if the number may be used to access the individual's financial account (before this amendment, the definition already captured account, credit or debit card numbers with additional identifying information); and
  2. biometric information such as fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data.
- Exempts individual notifications if notice was already provided in accordance with:
  1. the Gramm-Leach-Bliley Act (GLBA),
  2. the Health Information Portability and Accountability Act (HIPAA),
  3. part 500 of title 23 of the official compilation of codes, rules and regulations of the state of New York, or
  4. any other data security rules and regulations of any official department, division, commission or agency of the federal or New York state government.

1 See https://www.insurereinsure.com/2019/07/10/new-york-jumps-on-the-data-security-bandwagon/.
2 A "covered entity" is any person, business or state entity that owns or licenses computerized data which includes private information.

- Note that the notifications to the state attorney general, the state department of state and the division of state police are still required.
- Amends the content requirements for the individual notification to include the provision of telephone numbers and websites of the relevant state and federal agencies that provide information on security breach response and identity theft prevention and protection.
- Amends the notification obligation with respect to the state attorney general, the department of state and the division of state police by requiring a copy of the form of the individual notification.
- Requires that a HIPAA covered entity that is required to provide notification of a breach of unsecured PHI to the Secretary of the Department of Health and Human Services ("HHS") provide a copy of the notification to the state attorney general within five business days after notifying HHS, even if the breach does not include "private information."

New Data Security Obligations

The SHIELD Act adds 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.

Next Steps

In order to be in a position to comply with the requirements of the SHIELD Act, covered entities should begin to:

1. Understand what "private information," including the newly added data elements, of New York residents is in the business' possession, and how the information is processed and maintained.
2. Review the business' physical, technical, and administrative safeguards to determine whether they satisfy the enumerated requirements of the SHIELD Act.
3. Update incident response procedures related to the SHIELD Act's various changes to the notification obligations for data breaches impacting New York residents. Amend or add a procedure for documenting a determination of inadvertent exposure of "private information" of New York residents that is not a reportable incident, including retention requirements for the documentation and the attorney general notification obligation if over 500 New York residents were impacted.

Updated from original article published on July 24, 2019.

Proposed Changes to Regulations Governing the Confidentiality of Substance Abuse Disorder Treatment Records Reflects Concerns About Opioid Crisis

By David S. Szabo

The U.S. Department of Health and Human Services has released proposed amendments to the regulations governing the Confidentiality of Substance Abuse Disorder Treatment Records. The amendments are intended to improve continuity of care for patients, reduce risk of patient injury, and promote research about the use of opioids and the effectiveness of responses to the opioid crisis. Final regulations are expected to be released in early 2020.

Background

The confidentiality of medical records maintained by substance use disorder (SUD) programs is regulated by provisions of the Public Health Services Act, enacted long before the advent of the HIPAA privacy regulations. Providers that operate SUD programs are often referred to as "Part 2 Programs" or simply as "Programs." The regulations, which are codified at 42 C.F.R. Part 2, are administered by the Substance Abuse and Mental Health Services Administration ("SAMHSA"), a unit of the Department of Health and Human Services. The regulations are often referred to as the "Part 2 Rules." The Part 2 Rules are more strict than HIPAA, and require the written consent of the patient for most kinds of disclosures. Notably, if a Part 2 Program discloses treatment records that identify an individual to a third party, the records continue to be protected by the confidentiality regulations. The regulations apply only to healthcare providers that both (i) receive federal assistance and (ii) hold themselves out to the public as SUD-related services. General medical providers, such as hospitals and medical practices, are generally not subject to the regulations, although a specialized sub-unit or department devoted to SUD treatment within a larger health care facility would be subject to the Part 2 Rules.

Key Proposals

SAMHSA made several clarifications and proposals in the notice of proposed rulemaking. These included:

- SAMHSA clarified that if a general medical facility or medical group itself collects and records information from its patients about substance abuse disorders, that information, and the resulting records, are not subject to the Part 2 Rules. By way of contrast, records received by a general medical facility from a Part 2 Program remain subject to the protections of the Part 2 Rules, and should be segregated from the general medical record to prevent improper use or disclosure.
- SAMHSA noted that general medical providers are not permitted to transcribe or copy information contained in a record received from a Part 2 Program into their own medical records.
- SAMHSA proposed amendments to the consent rules that would make it easier for patients to consent to having their SUD records sent to social services programs or to government agencies for the purpose of obtaining benefits.
- SAMHSA proposed amendments to the consent rules to make it easier for patients to consent to sharing their records of SUD treatment with their other treating healthcare providers, such as their primary care physician or their hospital.
- SAMHSA proposed clarifications regarding the disclosures of SUD information that Part 2 Programs can make for their own administrative purposes.
- SAMHSA proposed that Part 2 Programs have greater authority to disclose information to other treatment programs and to central registries to prevent duplicate enrollment in medication assisted treatment programs and to coordinate care with general medical providers.
- SAMHSA proposed to amend the rules to permit disclosures to state-operated prescription drug monitoring programs, but only with the patient's written consent.
- SAMHSA proposed amending the scope of "medical emergencies" to include natural and other disasters, so that SUD treatment information could be disclosed to protect patient welfare in those circumstances.
- SAMHSA proposed amendments to make it easier for state agencies and other entities to conduct research on the incidence of substance abuse disorders and the effectiveness of treatment, subject to HIPAA research rules and the federal Common Rule governing human subject protection.

- SAMHSA proposed to modify the rules governing audits and evaluations to more readily permit disclosure of patient information to state agencies that regulate the health care system and for programs that are part of larger organizations to share information for planning and monitoring purposes.
- SAMHSA proposed amendments to the rules governing the use of undercover investigators and informants when prosecutors investigate alleged wrongdoing, such as drug diversion, at Part 2 Programs.

Many health care providers would like to see further modification of the confidentiality rules governing the treatment records of Part 2 Programs to allow disclosure among health care providers without a specific patient consent. Others feel that the high level of confidentiality imposed by current law remains necessary. While these regulations address some concerns related to sharing of medical information to improve care, further changes may require Congressional action.

Drone Operators Concerned With DJI Cybersecurity Concerns Have Few Options

By Patrick Byrnes and Matthew Kalas

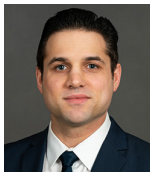
In the 1980s classic *An Officer and a Gentleman*, Richard Gere's character, Zack Mayo, breaks down and cries, "I got nowhere else to go" when threatened with being thrown out of Navy Aviation Officer Candidate School. That sentiment is likely the same felt by drone operators when it comes to drone manufacturer DJI , which is based in China. Many are concerned with the well-publicized cybersecurity concerns associated with DJI, but they've "got nowhere else to go."

In 2017, both the U.S. Military and Department of Homeland Security (DHS) placed bans on the use of DJI products due to concerns about the Chinese government accessing data produced by DJI drones. Waivers are now required for any such use of DJI products, and they are only granted on a "case-by-case" basis. The U.S. Department of the Interior adopted a similar approach because it found that DJI drones "did not meet UAS [unmanned aircraft systems] data management assurance standards." DJI has refuted any suggestion that the Chinese government has access to data produced by DJI drones, and in 2018, DJI hired Kivu to perform a study of its data practices. Kivu issued a report that was largely favorable for DJI. Nonetheless, in an effort to further win back government business, DJI has come forward with "Government Edition" hardware, firmware and software, but the Department of the Interior has only allowed the use of Government Edition equipment on limited "non-sensitive missions that collect publicly releasable data." And, as noted above, the military and DHS bans remain in place. Most recently, bipartisan legislation was introduced that would ban any federal spending on Chinese-made drones.

According to published reports, DJI has a virtual monopoly on the world's non-military drone market, occupying approximately 74% of the market. In gaining such market share, DJI has killed off most of its competition in the hardware space and there is essentially no domestic drone market. As a result, operators that are concerned with the safety of their data have few options to which to turn if they wish to avoid DJI. And, the available options generally come with higher price tags and lower performance standards.

So what is a drone operator that is concerned with the security of its data to do? One option is to only operate with non-DJI equipment, but, as noted above, that is easier said than done. If operators are going to use DJI products (and nearly three-quarters of all drone operators are), it is imperative that they fully understand the options that are available through DJI's software to prevent data sharing, and adjust their settings appropriately. Indeed, data protection should be top of mind for all commercial drone operators, regardless of the platform being used. As such, operators are potentially attractive targets for ransomware and other malicious activity. Even if DJI's claims are true and the Chinese government is not stealing data, hackers and other bad actors may be looking to do so. Thus, a robust cybersecurity program should be put in place to protect data that is captured and that will be shared with clients and other stakeholders. Failure to do so could be deemed negligent or, to round out the movie reference, "conduct unbecoming an officer."

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

T. Patrick Byrnes
Partner
Chicago
312-443-0286
pbyrnes@lockelord.com

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

Matthew J. Kalas
Senior Counsel
Chicago
312-443-0458
mkalas@lockelord.com

Andrew Shindler
Partner
London | +44 (0) 20 7861 9077
Brussels | +32 2 550 36 28
andrew.shindler@lockelord.com

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

Paul B. Sudentas
Senior Counsel
New York
646-217-7716
psudentas@lockelord.com

David S. Szabo
Partner
Boston
617-239-0414
david.szabo@lockelord.com

Elizabeth Tosaris
Partner
San Francisco
415-318-8817
etosaris@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