CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 7 | April 22, 2021

Table of Contents

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

Virginia adopts the Consumer Data Protection Act

On March 2, 2021, Virginia Governor Northam signed the Consumer Data Protection Act (CDPA) that "[e]stablishes a framework for controlling and processing personal data in the Commonwealth." *Consumer Data Protection Act*, Chapter 36 of the 2021 Special Session I, Virginia Acts of Assembly, available here. By adopting the CDPA, Virginia becomes the second state in the nation to pass a comprehensive data privacy legislation, following California with its California Consumer Privacy Act. *Virginia passes the Consumer Data Protection Act*, available here. This law will become effective on January 1, 2023.

For the purposes of the statute:

- "Consumer" is defined as a Virginia resident acting only in an individual or household context (as opposed to commercial or employment context);
- "Controller" is defined as a person or organization that, alone or jointly with others, determines the purpose and means of processing Personal Data. State or local government entities do not fall within the scope of the CDPA;
- "Personal Data" is defined as any information that is linked or reasonably linkable to an identified or identifiable person. This definition excludes any de-identified data or publicly available information; and
- "Process" or "processing" is defined as any operation or set of operations, whether by manual or automated means, that performs on Personal Data or on sets of Personal Data.

The CDPA grants Consumers certain legal rights over their Personal Data held by Controllers. To benefit Consumers, the CDPA imposes legal requirements to Controllers who conduct business in the state and either (1) control or process Personal Data of at least 100,000 Consumers, or (2) control or process Personal Data of at least 25,000 Consumers and derive over 50% of their gross revenue from the sale of Personal Data. It should be noted that the application of the CDPA does not depend on whether a Controller has a physical presence in Virginia, but rather on where the Consumer resides.

Under the CDPA, Consumers may exercise their rights by submitting a request to a Controller specifying the rights that they wish to invoke. The Controller is mandated to:

- Confirm whether or not it is processing Consumers' Personal Data;
- Correct any inaccuracies of those Data;
- Delete any Personal Data provided by or obtained about the Consumers;
- If technically feasible, provide a copy of the Data in a compatible format that allows the transfer to another Controller; and
- Enable Consumers to opt-out of Personal Data processing for purposes of targeted advertising, sale, or profiling.

Controllers are required to respond to Consumers' requests without undue delay, generally within 45 days of receipt of each request. Also, the CDPA requires Controllers to follow certain security practices with respect to the collection and processing of Consumer's Personal Data,

including employing data minimization techniques (the practice of only collecting and retaining personal data which is necessary), and maintaining proper data security practices.

The statute grants the Attorney General of Virginia with the exclusive authority to enforce violations. It also establishes a Consumer Privacy Fund to fund enforcement operations by the Office of the Attorney General.

In preparation for its coming into force, the CDPA directs the Joint Commission on Technology and Science (a permanent legislative agency under the General Assembly), to create a workgroup to review the provisions of this law, identify issues related to its implementation, and submit its findings by November 1, 2021.

Analysis

At first glance, the CDPA seems to follow the general data protection principles set forth by the California Consumer Privacy Act and the European Union's General Data Protection Regulation (GDPR). The CDPA recognizes Consumers' legal rights to their Personal Data, regardless of who controls or processes the data. The statute also requires Controllers to follow specified data security standards to protect Personal Data. Finally, the CDPA provides an enforcement mechanism, which can lead to civil penalties for noncomplying Controllers.

Enforcement Mechanisms

One of the major distinguishing features of the CDPA is the exclusive authority of the Attorney General to enforce the provisions of the statute. For example, Article 82 of the GDPR allows private individuals to pursue legal action for compensation for damages arising from a violation of the data protection law. *Art. 82 GDPR*, available here; *GDPR ushers in civil litigation claims across the EU*, available here. The California Consumer Privacy Act allows consumers to bring a civil action to recover damages arising out of data breaches caused by failures to implement and maintain reasonable security procedures. Cal. Civ. Code §1798.150(a), available here.

Under the CDPA, only the Attorney General has the authority to enforce this law, and the civil penalties are capped at $7,500 per violation. Compared to the GDPR and the California Consumer Privacy Act, the CDPA's penalties are quite limited and dependent on the Attorney General's willingness to pursue civil action.

De-identified Data and Re-identification Techniques

The CDPA expressly excludes "de-identified data" from the meaning of Personal Data, which carves out a small but consequential exception for data that would otherwise come within the statute. Under section 59.1-571, **de-identified data** is defined as "data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such a person."

The statute proceeds on the assumption that de-identified consumer data does not require the same level of protection as data that identifies a particular person. However, in the Big Data world, there exist re-identification techniques using, for instance, data mining that are capable of de-anonymizing de-identified data. *See De-identified Data and Third Party Data Mining: The Risk of Re-identification of Personal Information*, available here.

Based on the statute's definition of de-identified data, if data could be *reasonably* linked to an individual, regardless of whether a proper de-identification process had been applied, then that data is Personal Data. A critical question is whether advanced re-identification techniques should be considered "reasonable" when determining the de-identified status of Consumer Data. If so, the CDPA may create an incentive for Controllers to apply more sophisticated de-identification techniques that overcome modern re-identification tools, to avoid the risk of de-identified information being *legally* Personal Data.

Conclusion

Although the CDPA is a great start to enhance privacy protections for consumer data, the statute takes an approach that minimizes civil litigation and penalties. Given that the Commonwealth is continuously working to attract IT investments in the region, the CDPA may be attempting to balance the need for enhanced privacy protection and maintaining IT business interests. *See, e.g., Virginia's Southwest counties set lowest data center property tax in state*, available here. Those who argue for greater consumers' control over their personal data will inevitably be disappointed by the absence of a private right of action for consumers. *See, e.g., Virginia General Assembly near to passing major consumer data privacy legislation*, available here. Ultimately, the CDPA should be the first of many steps for the Commonwealth to modernize data regulations as privacy issues increasingly impact Virginia residents.

Pennsylvania woman charged with deep fakes cyberbullying

On March 3, 2021, the Hilltown Township Police Department of Pennsylvania charged Raffaela Marie Spone ("Spone") with three counts of **Cyber Harassment of a Child - Seriously Disparaging Statements** and three counts of **Harassment – Communicates Repeatedly in Anonymous Manner**. *Raffaela Spone Criminal Complaint* (Bucks County District Attorney's Office), available here. According to the arrest affidavit, Spone used deep fake technology to produce realistic but fake media of juvenile victims in order to disparage her daughter's cheerleading competitors.

Deep fake, which is a combination of "deep learning" and "fake," is used to describe synthetic media content (photo, video, or audio) that is often created with the intent to spread disinformation. *Real Fake*, available here. Using deep learning algorithms (which is a subset of Artificial Intelligence technologies), users can create realistic but fake media with minimal manual labor.

According to the Bucks County District Attorney's Office, Spone used online text messaging and phone services to send harassing messages to juvenile victims, who were members of a cheerleading program. *Chalfont Woman Charged with Cyberbullying Daughter's Cheerleading Rivals*, available here. According to police, the victims were cheerleading rivals of Spone's daughter.

Spone allegedly produced and disseminated deep fake photos of victims that appear to be drinking, vaping, and naked. The police also alleged that Spone produced and disseminated a deep fake video that appears to portray one of the victims vaping.

Spone is currently awaiting her preliminary hearing, which is scheduled for May 14, 2021. *Magisterial District Court 07-2-08: Public Court Summary*, available here.

Analysis

Since the first deep fake program was released between late 2017 and early 2018, deep fake media has proliferated in major social media websites and other internet communities. Although early deep fake programs required high-powered computers and certain technical skills to generate realistic face-swapped videos, users can now create deep fakes media by simply uploading pictures to an online service. *See, e.g., Reflect.tech – Face Swap*, available here. Even popular mobile messaging apps, such as Snapchat, have some capability of creating deep fake photos and videos using the user's phone. *See, e.g., Want to try that gender-face-swap thing everyone's doing? Here's how*, available here.

The Commonwealth of Pennsylvania does not have a statute specifically addressing the issue of deep fake technology. Instead, the state has an anti-harassment statute that prohibits a wide range of behaviors that is knowingly intended to harass, annoy, or alarm another. 18 Pa.C.S. 2709. Accordingly, Spone was charged under existing anti-harassment statutes.

Similar to Pennsylvania, Virginia does not have a statute deliberately addressing deep fakes. However, on March 18, 2019, the Virginia General Assembly amended the statute prohibiting the dissemination of revenge pornography (i.e., "unlawful dissemination or sale of images of another person"), to cover media generated by deep fake software. *SB 1736 Unlawful dissemination or sale of images of another person; penalty,* Chapter 515 of the 2019 Session, Virginia Acts of Assembly, available here. Currently, the relevant Virginia law on the distribution or selling of deep fake media states as follows:

Any person who, with the intent to coerce, harass, or intimidate, maliciously disseminates or sells any videographic or still image **created by any means whatsoever** that depicts another person who is totally nude, or in a state of undress . . . where such person knows or has reason to know that he is not licensed or authorized to disseminate or sell such videographic or still image is guilty of a Class 1 misdemeanor. Va. Code Ann. § 18.2-386.2 (emphasis added), available here.

This law could cover cases beyond revenge pornography like those dealing with the distribution of deep fake media that depicts undressed victims without consent. At the time of this publication, there has been no known Virginia criminal case that involved deep fake revenge pornography.

As deep fake creation technologies become more accessible, it is foreseeable that they could be increasingly used to facilitate criminal activities and disinformation campaigns. This issue was serious enough that the Cybersecurity and Infrastructure Security Agency commissioned a graphic novel to illustrate the dangers of deep fake technologies within disinformation operations. *Resilience Series Graphic Novel: Real Fake*, available here.

The community behind deep fake technology has developed even more advanced deep fake creation techniques, including the ability to digitally undress a woman in a photograph. *This*

Horrifying App Undresses a Photo of Any Woman With a Single Click, available here. Lawmakers should take a proactive approach and evaluate ways to limit nonconsensual deep fake pornography dissemination, including enhancing criminal penalties when these technologies are utilized in the furtherance of a crime.