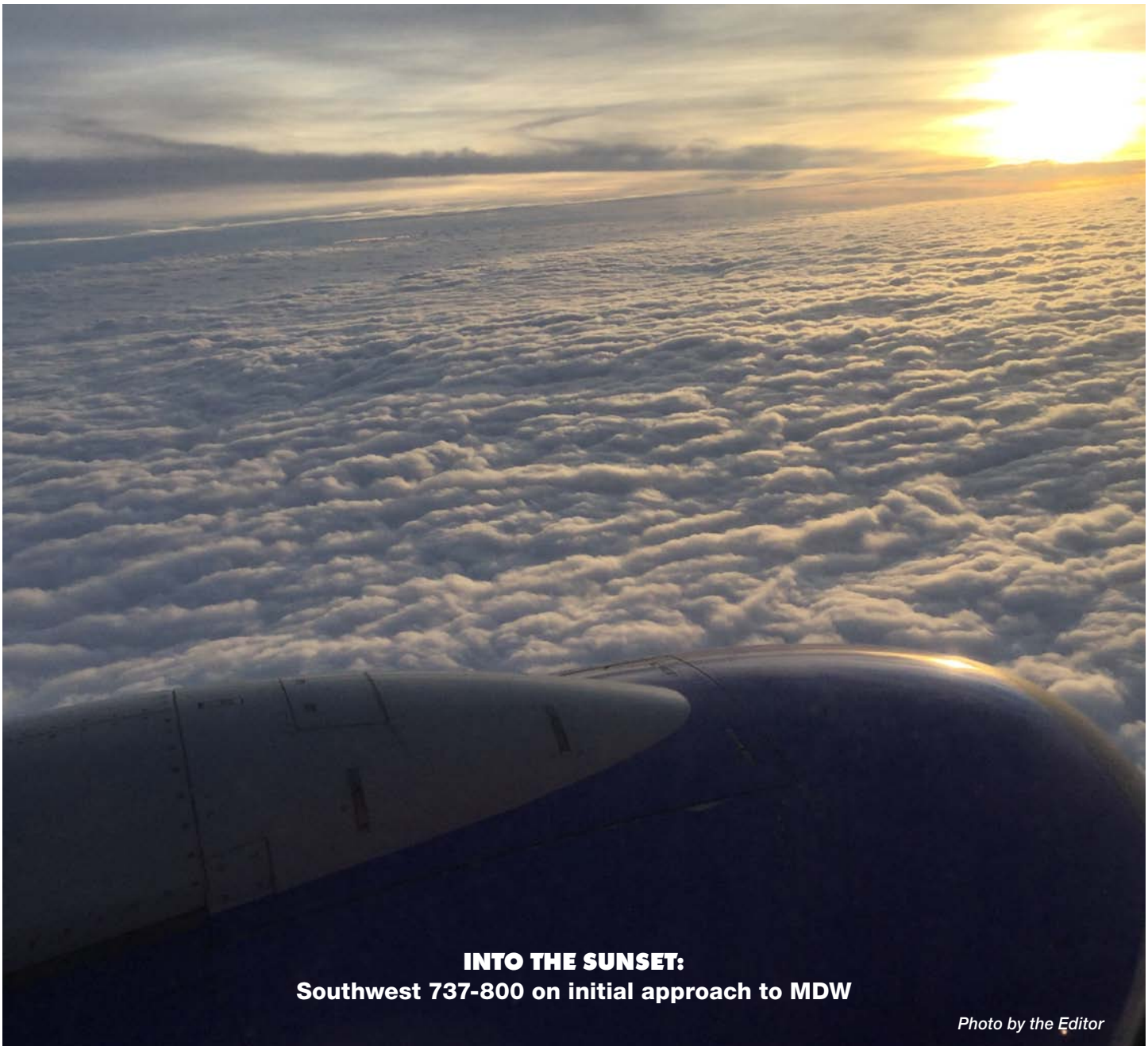
LAWYER-PILOTS BAR ASSOCIATION JOURNAL

"dedicated to aviation safety, the just administration of the law and continuing legal education."

VOL. XLII NO. 1 **CLEVELAND, OHIO** **SPRING 2020**



INTO THE SUNSET:
Southwest 737-800 on initial approach to MDW

Photo by the Editor

SUMMER MEETING – Seaview Dolce Hotel – Galloway, NJ – August 26-30, 2020

DRONES AND DATA PRIVACY:

How Lawyer-Pilots Can Best Assist Clients in Complying with the New Federal Drone Privacy Law

Bradford P. Meisel, Esq., Albert J. Pucciarelli, Esq. and Diane D. Reynolds, Esq.

Bradford P. Meisel is an Associate specializing in data privacy and drone law at McElroy, Deutsch, Mulvaney & Carpenter, LLP. Albert J. Pucciarelli is the Chair of the Hotels and Resorts and Aviation Practice Groups at McElroy, Deutsch, Mulvaney & Carpenter, LLP. Diane D. Reynolds heads the Cybersecurity, Data Protection, and Privacy practice at McElroy, Deutsch, Mulvaney & Carpenter, LLP.

The federal drone privacy law enacted as part of the FAA Reauthorization Act of 2018, which was signed by President Donald Trump on October 5, 2018, has significant implications for commercial drone operators in numerous sectors. Given lawyer-pilots' unique firsthand experience with federal aviation regulations (FARs) and FAA enforcement procedures and policies, lawyer-pilots may be the 'go-to' advisors for clients seeking to establish effective compliance practices and procedures for the new law.

In recent years, businesses in a diverse array of sectors have begun to employ drones for a broad spectrum of purposes. Commercial and residential real estate brokers now use drones to take aerial photos and videos of listed properties and insurance companies use drones to survey property damage. Construction companies have deployed drones to monitor progress and inspect ongoing projects and public utilities use drones to inspect critical infrastructure and equipment. Mining companies have used drones to survey mining sites and farms have utilized drones for crop monitoring. The coming months and years will likely witness an expansion of commercial drone use as drone package and food delivery and autonomous construction drone technology continues to develop.

The new federal drone privacy law requires all commercial drone operators not using drones for First Amendment-protected activity such as news reporting to develop and implement publically available privacy policies governing the collection of any data regarding any person using a drone. The law provides that any violation of such required privacy policies constitutes an unfair and deceptive trade practice for the purpose of the Federal Trade Commission Act that is subject to Federal Trade Commission enforcement.

The law also provides that the required privacy policies must protect individuals' privacy consistent with state and local laws. Therefore, lawyer-pilots advising commercial drone operators must assist commercial drone operators in complying with the emerging patchwork of state laws governing the privacy and security of personally identifiable information that could be obtained by a drone photographing or filming human subjects despite the fact that multiple courts, including the California Appellate Court in the 2016 case of *People ex. rel. Harris v. Delta Airlines, Inc.* have held that state data privacy statutes are preempted as applied to airlines.

California is a proactive state in the area of privacy regulations. The California Consumer Privacy Act of 2018, which took effect on January 1, 2020, applies to any entity that "does business in California" (A) has annual gross revenues in excess of $25 M; (B) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more customers, households, or devices; or (C) derives 50% or more of its annual revenues from selling customers' personal information.

The California act requires covered entities to disclose to any California resident upon request the categories and specific pieces of information it collected from them and the categories of third parties with whom such information is shared and gives all California residents the right to opt out of any sale of their personal information. It also requires covered entities to delete any personal information collected from a customer upon request. The California act imposes a duty on all covered entities to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" they possess and creates a private right of action for California residents harmed by breaches of this duty. Plaintiffs in such suits are entitled to the greater of actual damages or statutory damages of $100-$750 per incident. All other provisions of the statute are enforceable by the California Attorney General.

Numerous other states including New York, Texas, Pennsylvania, Massachusetts, Washington, and Florida, have enacted statutes requiring entities that possess the personally identifiable information of state residents to implement reasonable proactive security practices to protect the personally identifiable information of state residents. Further, Illinois, Texas, and Washington have implemented statutes prohibiting the collection of biometric data regarding state residents without their consent and requiring companies that possess biometric data of state residents to use reasonable security measures to protect such information. There is also currently pending legislation in numerous other states that would impose significant data privacy and security requirements on entities that collect or process the personally identifiable information of state residents.

Given that state data privacy and security statutes' definitions of personally identifiable information may vary, lawyers representing commercial drone operators would be well advised to evaluate each commercial drone operator's operations and the ways in which their drones monitor, photograph, film, or otherwise collect

continued on page 33

Drones and Data Privacy

continued from page 25

information regarding human subjects, including whether or not such activities could constitute collection or processing of biometric data, in order to determine whether their operations could implicate these statutes and if they do, formulate and implement effective and efficient compliance protocols memorialized and disclosed in their required privacy policies. Given the rapid pace at which states have been enacting new data privacy laws and regulations in recent years and months, lawyers whose clients' drone usage may implicate such statutes may consider consulting or collaborating with experienced data privacy attorneys in order to best assist such clients.

Although these new statutes may pose a challenge to commercial drone operators and aviation attorneys who have yet to confront state data privacy laws due to the federal preemption of such laws as applied to airlines, lawyer-pilots who combine their unique and unparalleled firsthand understanding of aviation and aviation law with up to the minute expertise in state data privacy and security law can become invaluable advisors to commercial drone operators.