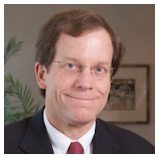
haynesboone

MEDIA, ENTERTAINMENT AND FIRST AMENDMENT NEWSLETTER

APRIL 2020



Thomas J. Williams

Chrissy Long

Transparency vs. Safety: Restrictions to Open Government During COVID-19

Thomas J. Williams and Chrissy Long

Every part of life has been affected by the COVID-19 pandemic, and access to open government is no exception. The rise of COVID-19 has seen government agencies scrambling to modify ordinary procedures aimed at ensuring the transparency of government in light of federal, state, and local mandates to limit face-to-face contact. Almost without exception, these "temporary" measures have the effect of reducing, or at least making more difficult, public access to government information. For the time being, that may be a necessary price for society to pay to contain the pandemic; it will remain to be seen whether any of these new restrictions survive the current emergency.

All states have public information and open meetings law. According to a USA Today Network survey, as of early April 2020, at least 35 states, including Texas, have temporarily altered their public information and/or open meetings laws in response to COVID-19. Each state's open government laws are different, and so the temporary changes to those laws vary, but the changes that have been seen so far in Texas illustrate the kinds of emergency measures that have been implemented across the country.

Catastrophe-Suspensions of Deadlines under the Texas Public Information Act

The Texas Public Information Act ("TPIA") requires that a governmental body produce requested public information "promptly," which is defined as "as soon as possible under the circumstances, that is within a reasonable time, without delay." If an agency cannot produce public information within ten "business days" after the request, the TPIA requires it "to certify that fact in writing to the requestor and set a date and hour within a reasonable time when the information will be available for inspection or duplication."

In 2019, the Texas Legislature amended the TPIA to allow a governmental body to suspend the statute's requirements when it is impacted by a "catastrophe," defined as "a condition or occurrence that interferes with the ability of the governmental body to comply" with the TPIA, including an epidemic. The suspension may last for an initial period of up to seven consecutive days and may be extended once for up

to another seven consecutive days. A governmental body invoking this procedure must post notice of the suspension in the same manner it posts notices of public meetings under the Texas Open Meetings Act and must also provide notice to the Office of the Attorney General ("OAG"). A request for public information received during a catastrophe-suspension period is considered to have been received on the first "business day" after the suspension period ends, and deadlines associated with all requests received before a catastrophe-suspension period are tolled until the first business day after the suspension period. In March 2020, the Attorney General received 80 catastrophe notices from governmental bodies around the state who were unable to comply with the TPIA's requirements due to the coronavirus. To put that into perspective, the OAG had previously only received two catastrophe notices since the TPIA was amended to allow for such suspensions.

It is noteworthy that the maximum length of a "catastrophe suspension" is 14 days, which generally is sufficient for the types of catastrophes one normally sees, such as a hurricane, tornado, or fire. But the COVID-19 catastrophe has already exceeded 14 days, and the current limitations on activity will be in place at least until April 30, 2020, and perhaps longer.

In March 2020, the OAG, having received dozens of inquiries about the TPIA's catastrophe-suspension procedure related to COVID-19, issued guidance stating that a catastrophe suspension is appropriate only when the governmental body is open for business but determines that a catastrophe has interfered with its ability to comply with TPIA, and is not necessary at all if the governmental body is not open for business. The guidance also noted that a "business day" for purposes of calculating TPIA deadlines does not include:

- skeleton crew days;
- a day on which a governmental body's administrative offices are closed;
- a day on which the governmental body closes its physical offices because of a public health response, or, is unable to access its records on a calendar day, even if the staff is working remotely or the staff is onsite but involved directly in the public health response.

This interpretation of the term "business days," which is not defined in the TPIA, is consistent with the OAG's long standing practice. Normally, however, the effect on a TPIA deadline is minimal and limited to days which are not legal holidays but on which governmental offices customarily close (for example, the Friday after Thanksgiving), or days on which unforeseen circumstances, such as weather, require an office to close for a short period.

Now, however, with some governmental bodies "closing" indefinitely (albeit working remotely) the beginning of a TPIA response period may effectively extend indefinitely. Then, upon "re-opening," a governmental body could invoke the catastrophe declaration and potentially extend the response period for an additional 14 days, a far cry from the "prompt" production of public information the TPIA mandates.

Virtual Meetings and Teleconferences under the Texas Open Meetings Act

On March 13, 2020, Texas Governor Greg Abbott declared a state of disaster for all counties in Texas due to COVID-19. As in other states, a disaster declaration allows the Governor to suspend any state statute that prescribes procedures for conducting state business that would "in any way prevent, hinder, or delay necessary action in coping with a disaster."

The Texas Open Meetings Act ("Open Meetings Act") requires most meetings of governmental bodies to be open to the public and be preceded by public notice of the time, place, and subject matter of the meeting. Meetings by videoconference are allowed, but for most governmental bodies a quorum must be physically present at one location, the notice must specify that location as the "place" of the meeting, and the videoconference must be both visible

and audible at that location. On March 16, 2020, responding to a request from the OAG, Governor Abbott temporarily suspended:

- statutes requiring a quorum or presiding officer to be physically present at the specified location of the meeting (provided that a quorum must still participate);
- statutes that require physical posting of a meeting notice (provided that the online notice must include a toll-free dial-in number or free videoconference link along with an electronic copy of any agenda packet);
- statutes that require that the telephonic or videoconference meeting be audible to members of the public who are physically present at the specified location of the meeting (provided that the dial-in-number or video-conference link allow for two-way communication, and, that the meeting be recorded and made public); and
- statutes that may be interpreted to require face-to-face interaction between members of the public and public officials (provided that governmental bodies provide alternative ways of communicating with public officials).

Thus, during this period of suspension, a meeting of a Texas governmental body may be truly remote with no two members of the governing body in the same location, and with no member of the "audience" in the same location.

In theory, the Governor's declaration provides the public the same rights to access meetings of governmental bodies as before COVID-19, it is just that the access must for the time being be remote. Indeed, the Governor's press release announcing the move carried the headline "ensures continued government operation while preserving transparency." However, it is not clear that all governmental bodies affected by the Open Meetings Act have the technical capabilities to comply with Governor Abbott's order. Further, "attending" a meeting of a governmental body now requires access to at least an internet or telephone connection, since there is no longer a requirement for a fixed "meeting location" at which audio and video are provided, and that is something that may still present a barrier to attendance for interested citizens. And finally, as is well known to the many Americans who have attended business meetings by Zoom recently, a certain level of interaction and understanding is lost when meetings shift from in-person to remote means. While it may not be possible to quantify that difference, that could ultimately prove to be the most significant aspect of these changes.

These temporary changes to Texas' open government laws, and the similar modifications made in other states, are understandable in light of the current public health crisis, but it will be important to ensure that once the COVID-19 situation improves, these "temporary" measures do not become permanent.

Cases Highlight the Growing Conflict Between AI and Data Privacy

Lee Johnston

Lee Johnston

No one can question the explosive growth in the use of artificial intelligence ("AI"). Seizing on its powerful predictive capabilities, private sector companies and government entities alike now employ machine-learning ("ML") algorithms to assist in diverse applications ranging from detecting and preventing fraudulent online credit card transactions to optimizing traffic flow to blocking dangerous phishing attempts.

Against this backdrop of AI's speed and efficiency, however, lies increasing concerns about the protection of personal data. Machine-learning algorithms are not born with the advanced predictive capabilities seen in products like Alexa or Google Maps. Rather, like their human counterparts, they require food, care and training that can only be

provided by being fed vast amounts of real-life and experimental data about the experiences, perceptions and interactions of humans; i.e., personal data, to achieve deep learning.

Recent cases highlight the growing tension between AI's thirst for and use of huge amounts of personal data to train ML algorithms and personal data's status as a protected commodity under recent U.S. privacy laws like Illinois's Biometric Information Privacy Act (BIPA) and the California Consumer Privacy Act (CCPA), as well as under older privacy statutes like the Health Insurance Portability and Accountability Act of 1996. Many of these cases have been brought even where the allegedly illegal use of the personal data is intended to correct the discriminatory "bias" in ML algorithms, or otherwise achieve laudable goals, such as enhancing healthcare providers' ability to predict patients' future clinical events.

Recent Cases Involving Collection and Use of Machine Learning "Training" Data

Janecyk v. International Business Machines, Case No. 1:20-cv-00783 (N.D. Ill.) (filed January 22, 2020). This putative class action, arises out of IBM's use of publicly available images to create the "DiF" (Diversity in Faces) dataset.[1] The plaintiff, Tim Janecyk, is a photographer who uploaded photos of himself and others at political rallies to the photo sharing site Flickr, which in turn used these and other images to create a database of 99 million images for use as a reference library to train AI models. According to Janecyk, IBM coded a subset of the photos to describe the appearance of the people in the photos, and then offered its collection to researchers as a tool to help reduce bias in facial recognition models.

Notwithstanding its good intentions, IBM now faces potential liability under BIPA of $1,000 to $5,000 per violation for each Illinois resident "who had their biometric identifiers, including scans of face geometry, collected, captured, received, or otherwise obtained by IBM from photographs in its Diversity in Faces Dataset."

Mutnick v. Clearview AI, et al., Case No. 1:20-cv-00512 (N.D. Ill.) (filed January 22, 2020). This putative class action arises out of Clearview AI's creation of a facial recognition database of millions of Americans trained from more than 3 billion photos Clearview scraped from online social media and other internet-based platforms such as Venmo.[2] The plaintiff, David Mutnick, alleges that Clearview's AI facial recognition database has been sold to over 600 law enforcement agencies, as well as other private entities, to biometrically identify individuals who had no knowledge of, and did not consent to, Clearview's capture and use of their biometric data. In addition to monetary damages under BIPA, the plaintiff recently filed a motion for preliminary injunction, seeking to stop any further dissemination or use of the biometric data and affirmatively requiring Clearview to implement more robust security measures to protect database from further data breaches.[3]

Burke v. Clearview AI, Inc., Case No.: 3:20-cv-00370-BAS-MSB (S.D. Cal.) (filed February 27, 2020). The *Burke* putative class action alleges the same facts and claims complained of in *Mutnick*, but also seeks relief under CCPA based on Clearview's alleged failure to inform consumers "at or before the point of collection" about the biometric information it was collecting and the purposes for which this data was going to be used.[4] Seeking to side-step the absence of a private action for this claim under CCPA, the Burke complaint frames the CCPA violations as violations of California's Unfair Competition Law (UCL), which prohibits business practices that violate other laws.[5]

Dinerstein v. Google, Case No. 1:19-cv-04311 (N.D. Ill) (filed June 29, 2019). The *Dinerstein* putative class action alleges that through a series of corporate transactions allowing it to acquire and absorb an AI data-mining company called DeepMind, and its partnerships with healthcare systems, including the University of Chicago, Google illegally obtained access to hundreds of thousands of patients' medical files in violation of HIPPA. According to the *Dinerstein* plaintiffs, Google utilized this ill-gotten personal healthcare data to "train" machine-learning diagnostic and search algorithms, which in turn it seeks to patent

and commercialize in a fee-for-service, subscription or standalone service. The *Dinerstein* complaint asserts a panoply of claims against the University of Chicago, including violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505 ("ICFA") and breach of express and implied contract, and against Google for tortious interference with contract and unjust enrichment.[6]

These recent cases underscore the increased risk associated with the collection and use of data to train machine-learning algorithms and AI models. To mitigate these risks, companies should first inventory the source of all data used to train and develop AI, and then document the intellectual property rights and privacy consents associated with each data set. By doing this audit-based work proactively, companies can better evaluate the risks associated with each data set and develop strategies to mitigate those risks.

---

1 Shortly after the Janecyk state court case was filed, a second complaint against IBM based on the same alleged conduct was filed in Illinois federal court, styled Vance v. IBM, Case No. 1: 20-cv-577 (N.D. Ill.).

2 On February 5, 2020, a second putative class action complaint was filed against Clearview in Illinois federal court alleging similar claims for relief under BIPA. See Hall v. Clearview AI, et al., Case: 1:20-cv-00846 (N.D. Ill).

3 In late February 2020, Clearview disclosed that its client list had been hacked. See Plaintiff's Mem. of Law in Support of Motion for Preliminary Injunction, Dkt. No. 32 at p. 10 (citing Betsy Swan, Facial-Recognition Company that Works with Law Enforcement Says Entire Client List Was Stolen, The Daily Beast (Feb. 26, 2020) ("Clearview Client List Stolen").

4 *The Burke plaintiffs recently consented to the transfer of venue in the case to the Southern District of New York, where two other Clearview AI cases are pending. See Joint Motion to Transfer Venue, Dkt. No. 10 (filed April 14, 2020). The two New York federal cases are styled Calderon et al v. Clearview AI, Inc. et al, Case No. 1:20-cv-01296-CM (S.D.N.Y.) and Broccolino v. Clearview AI, Inc., Case No. 1:20-cv-02222-CM (S.D.N.Y.)*

5 Cal. Bus. & Prof. Code §§ 17200. The language of the CCPA attempted to avoid the "backdoor" assertions of CCPA violations through the UCL. See Cal. Civ. Code section 1798.150(c) ("Nothing in this title shall be interpreted as the basis for a private right of action under any other law."); cf. Cal-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co., 20 Cal. 4th 163, 182 (1999) (statutes containing "absolute bar" to relief may not be recast as UCL violations). However, this provision under the CCPA is untested, and the California attorney general has advocated for a CCPA amendment permitting a more expansive private right of action under the CCPA.

6 The Dinerstein plaintiffs' contract and tort claims are based on the University's failure to abide by the HIPPA restrictions set forth in the hospital admission and treatment forms signed by the patients and the HIPPA-based privacy policy disclosures provided by the University.

Second Circuit Will Not Rehear First Amendment Twitter Suit against President Trump

Wesley Lewis

Wesley Lewis

On March 23, 2020, the Court of Appeals for the Second Circuit denied *en banc* review of a panel's prior decision in the Knight First Amendment Institute's ongoing lawsuit challenging, on First Amendment grounds, President Donald J. Trump's practice of blocking certain users from accessing his @realDonaldTrump Twitter account in response to those users' criticism of his administration and policies. In May 2018, the United States District Court for the Southern District of New York sided with the Knight Institute, holding that President Trump's Twitter account constituted a "public forum," and as a result, that the President's practice of denying some users access to it based on their expressed viewpoints violated the First Amendment. In July 2019, a unanimous Second Circuit panel affirmed the lower court's decision.

President Trump moved for rehearing *en banc*, but the Court's vote fell short of the majority needed to rehear the case. Circuit Judge Barrington Parker filed a statement with respect to the denial of rehearing *en banc* in which he characterized the Second Circuit's 2019 decision as "a straightforward application of state action and public forum doctrines, congruent with Supreme Court precedent." Noting that the President's tweets "cover subjects as diverse as military actions, immigration policies, and senior staffing changes, among other major official

announcements," Judge Parker observed that "Twitter is not just an official channel of communication for the President; it is his most important channel of communication." Accordingly, President Trump's practice of selectively blocking users' access to his Twitter account was unconstitutional.

Judge Michael Park, joined by Judge Richard Sullivan, wrote a separate statement dissenting from the denial of rehearing *en banc*, arguing that @realDonaldTrump is the President's personal Twitter account and does not constitute a public forum simply because it is operated by a public official. The dissent argued further that because Twitter is privately owned and controlled, a public official's decision to block users "involves no exercise of state authority" for purposes of the First Amendment analysis.

Many observers expect President Trump to seek review in the United States Supreme Court. A Petition for Writ of Certiorari, if the deadline is not extended, will be due on June 22, 2020.

The case is *Knight First Amendment Inst. at Columbia Univ. v. Trump*, No. 1:17-cv-5205 (S.D.N.Y.), No. 18-1691 (2d Cir.).

SPEAKING ENGAGEMENTS

Thomas J. Williams

Freedom of Information Foundation of Texas, Open Government Seminar
Speaker: Texas Public Information Act and the Texas Open Meetings Act
June 4, 2020
San Antonio, TX

RECOGNITIONS

59 Haynes and Boone Lawyers to be Honored in 2020 Chambers USA Directory
Laura Prather
First Amendment Litigation (USA - Nationwide)

FOR MORE INFORMATION CONTACT:

LAURA LEE PRATHER
PARTNER
laura.prather@haynesboone.com
+1 512.867.8476

TOM WILLIAMS
PARTNER
thomas.williams@haynesboone.com
+1 817.347.6625