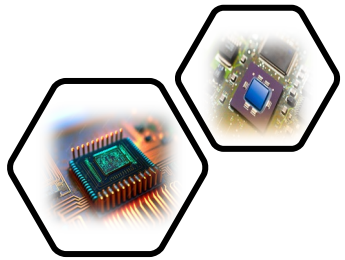
Recent Developments in Constitutional Law and AI

- Lee Harville
- The Harville Law Firm, LLC
- lee.harville@theharvillelawfirm.com

- December 18, 2025


I heard the government is putting chips inside of people...
I hope I get Doritos...
@artmemescentral



Constitutional Rights and Modern Technology

A. Technology and the Fourth Amendment/Privacy Right

In ***United States v. Hay***, 95 F.4th 1304, 1308 (10th Cir. 2024), the Court asked:

Does the Fourth Amendment permit the government to surveil a home for months on end without a warrant? This case requires us to decide.

The Department of Veterans Affairs (VA) offers lifetime benefits to permanently disabled veterans. A Kansas jury convicted Bruce Hay of ten counts of stealing government property and six counts of wire fraud as part of a scheme to defraud the VA by exaggerating his disability. As part of its investigation, VA agents installed a pole camera across the street from his house to film his activities.

Mr. Hay appeals his conviction. He contends that (1) the evidence presented at trial is insufficient to support a conviction, (2) the VA's installation of a pole camera violated his Fourth Amendment rights, and (3) the district judge wrongfully admitted evidence to the extent that it deprived him of a fair trial.

We affirm the district court.

Constitutional Rights and Modern Technology

The ***Hay*** court concluded:

> [f]ew technologies have expanded more rapidly than the ubiquitous camera, which is worn by police officers, built into cellphones that the *Carpenter* court called 'almost a feature of human anatomy,' and strapped to front doors. *United States v. Moore-Bush*, 36 F.4th at 372 (Lynch, J., concurring) (citing *Carpenter*, 585 U.S. at 311). Cutting edge drone technology enables police to conduct discreet aerial investigations, *see State v. Stevens*, 2023-Ohio 889, 210 N.E.3d 1154, 1157 (Ohio App. 2023), while satellite images of homes are free and readily available to citizens and law enforcement alike. *See In re Murphy*, No. 771 Sept. Term 2022, 2023 Md. App. LEXIS 279, 2023 WL 2999975, at *6 (Md. App. 2023). Artificial intelligence software accelerates facial identification and pattern recognition to a previously unimaginable degree. As video cameras proliferate throughout society, regrettably, the reasonable expectation of privacy from filming is diminished.

In conclusion, Mr. Hay had no reasonable expectation of privacy in a view of the front of his house. The district court did not err in denying suppression of that footage.

95 F.4th at 1317-18.

Constitutional Rights and Modern Technology

- Domain Awareness System (DAS), a crime-fighting and counterterrorism tool, jointly developed by the NYPD and Microsoft, which utilizes the largest network of cameras, license plate readers, and radiological sensors in the world.
- As many as 18,000 cameras.
- Bryan Lagarde, the organization's executive director, said Project NOLA operates the "largest, most cost-efficient and successful networked HD crime camera program in America."
- Before founding Project NOLA in 2009, Lagarde was involved in various surveillance efforts.
- Today, Project NOLA has more than 5,000 cameras installed throughout New Orleans. Some of the cameras use artificial intelligence to control their movements, and others have thermal imaging capabilities.
- Researchers were able to find data for 39 of the 50 most populated cities. Across these, they found that nearly 270,000 cameras monitor a population of 44.2 million people (6 cameras per every 1,000 citizens).
- While Chicago has the highest number of cameras (32,000), Atlanta is the most surveilled city with a ratio of 48.93 cameras per 1,000 people.

Constitutional Rights and Modern Technology

B. Facial Recognition

In ***In re Clearview AI, Inc.***, 21-cv-0135 (N.D. Ill. 3-23-22), 2022 U.S. Dist. LEXIS 52012, at pp. 3-4, the plaintiffs,

> [i]n their April 22, 2021 complaint filed in the Superior Court of the State of California, Alameda County, . . . allege[d] that they are two community-based organizations and four political activists. They seek injunctive relief and damages against defendant Clearview based on allegations that Clearview illegally acquired, stored, and sold their likenesses, and the likenesses of millions of Californians via Clearview's searchable facial recognition database. Plaintiffs assert that Clearview scraped billions of photographs from websites like Facebook, Twitter, and Venmo and used artificial intelligence algorithms to scan the faceprints. Thereafter, Clearview created a searchable database containing plaintiffs' faceprints allowing users, including law enforcement agencies, to identify unknown individuals by uploading a photograph. Plaintiffs bring claims under California common law, the California Constitution, and California's Unfair Competition Law.

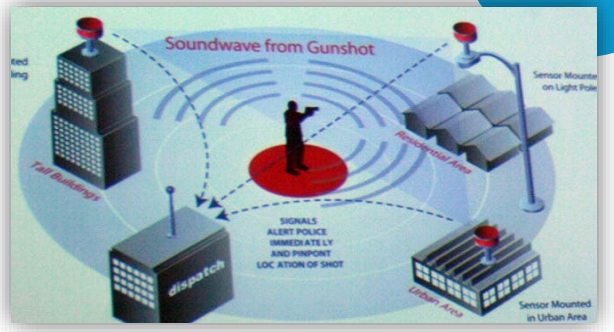
Constitutional Rights and Modern Technology

In a criminal justice setting for instance, how should facial recognition be used and/or regulated. Consider that:

> In 2019, the National Institute of Standards and Technology ("NIST") published a report analyzing the performance, across races, of 189 facial recognition algorithms submitted by 99 developers, including Microsoft, Intel, Idemia, and other major tech and surveillance companies. Many of these algorithms were found to be between 10 and 100 times more likely to misidentify a Black or East Asian face than a white face. In some cases, American Indian faces were the most frequently misidentified. Most algorithms were substantially less likely to correctly identify a Black woman than a member of any other demographic. To understand the reasons for these disparities, it helps to understand the basics of how facial recognition technology works.

B. Finley, *Why Racial Bias is Prevalent in Facial Recognition Technology*, (Nov. 3, 2020), https://jolt.law.harvard.edu/digest/why-racial-bias-is-prevalent-in-facial-recognition-technology#:~:text=Race%20influences%20the%20development%20and%20performance%20of%20facial,the%20algorithm%2C%20usually%20with%20lighter%20skin%20tones%20predominating.

Constitutional Rights and Modern Technology



C. Confrontation Clause

In ***Commonwealth v. Weeden***, 304 A.3d 333, 353-354 (Pa. 2023) (J. Brobson concurring) (internal footnotes and citations omitted), Justice Brobson noted that:

ShotSpotter's proprietary gunshot-detection system is a network of acoustic sensors that is installed throughout a neighborhood to aid and facilitate law enforcement's response to gun violence. When potential gunfire is detected, sensors record the time and capture an audio recording of the sound. Two artificial intelligence algorithms immediately assess the data in order to triangulate the location of the sounds and to filter out noises that are not gunshots (such as fireworks). The information generated by these algorithms is immediately reviewed and interpreted by a trained ShotSpotter employee in California. Within approximately sixty seconds (or less), the analyst listens to the audio recording and conducts a 'visual analysis of the waveform.' If the analyst determines that the noise was, in fact, the sound of gunfire, he or she immediately alerts local law enforcement.

Constitutional Rights and Modern Technology

ShotSpotter compiles all of this information into an 'Investigative Lead Summary.' The data in this document reflects the input of at least one of ShotSpotter's trained analysts, who are known as 'Incident Reviewers.' ShotSpotter admits that the data in the summary is unreliable, and that it should not be used for anything other than initial investigative purposes. Although these summaries are modified by human input and are not amenable to cross-examination, they are introduced as substantive evidence at criminal trials—including in the case at bar—in order to prove that a defendant, in fact, fired a gun at a particular time and location.

Admitting these out-of-court statements as substantive evidence undermines each of the foundational interests underlying the Confrontation Clause of the Sixth Amendment to the United States Constitution. However, as the Majority aptly explains, the 'primary purpose' of the Investigative Lead Summary is to assist law enforcement in responding to, and subsequently investigating, an 'ongoing emergency,' not 'to establish or prove past events potentially relevant to later criminal prosecution.' Thus, the Investigative Lead Summary is nontestimonial, and, pursuant to the United States Supreme Court's precedents, can be admitted at trial without cross-examination and without running afoul of the Confrontation Clause. Bound by those precedents, I join the Majority's opinion. I write separately to highlight the inequity that results from treating nontestimonial statements differently than testimonial ones under the Confrontation Clause.

Louisiana State Analytical and Fusion Exchange (LA-SAFE)

The Louisiana State Analytical and Fusion Exchange (LA-SAFE), also called the State Fusion Center, promotes collaboration in an all-crimes/all hazards environment. It supports local, State, Federal and private sectors by working together to provide timely information for use in promoting public safety and national security against terrorism and other criminal threats.

LA-SAFE supports the State during major disasters and emergencies by gathering, analyzing and disseminating information to assist relevant agencies.

LA-SAFE is a collaborative effort of two (2) or more agencies that provides resources, expertise and information to the Center with the goal of maximizing their ability to detect, prevent, investigate and respond to criminal and terrorist activity. LA-SAFE serves as an effective and efficient mechanism to:

- Promote interoperability
- Create a framework of situational awareness
- Assists with the an exchange and dissemination of information required to make informed decisions

Fusion Center Partners

Local Partners

- East Baton Rouge Sheriff's Office
- Baton Rouge Police Department

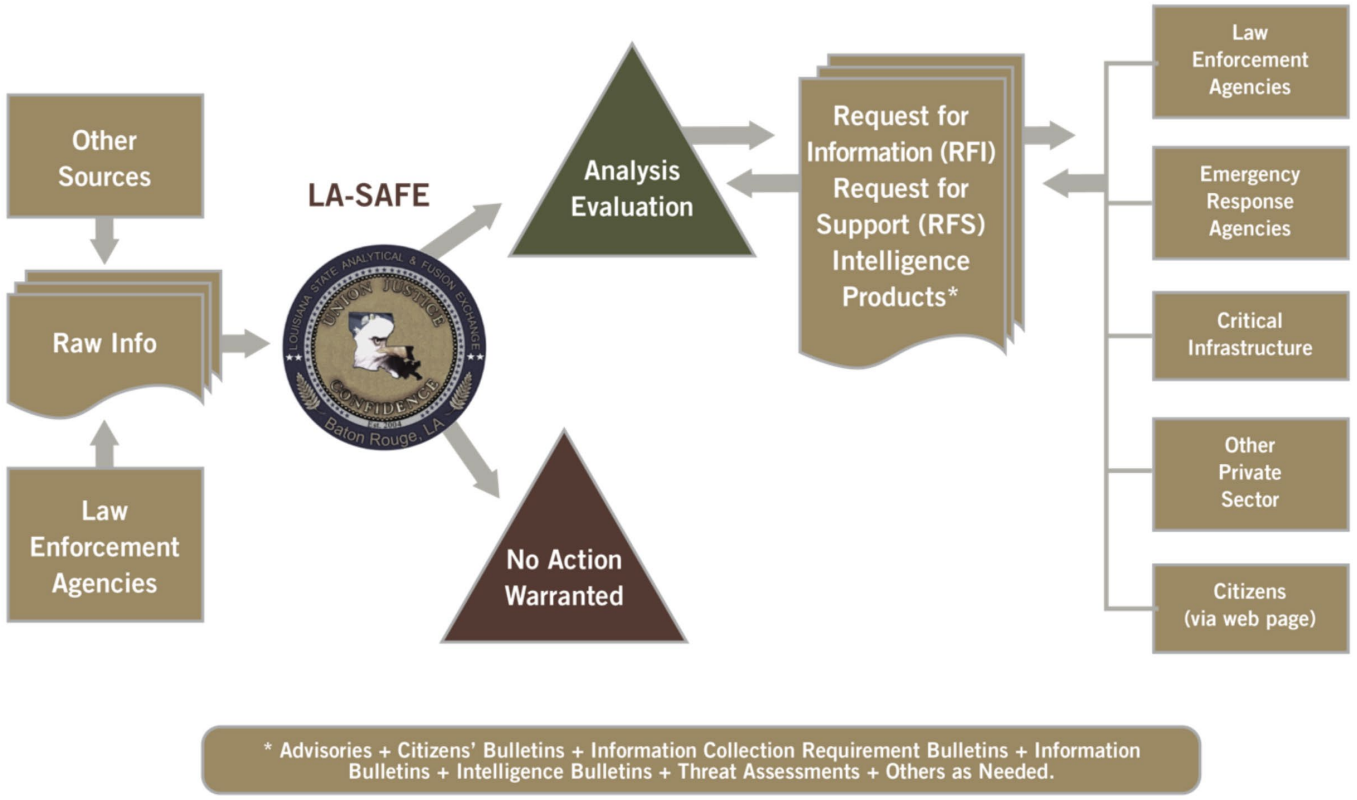
State Partners

- Governor's Office of Homeland Security and Emergency Preparedness
- Louisiana State Police
- Louisiana Department of Wildlife and Fisheries
- Louisiana National Guard
- Louisiana Division of Administration

LA-SAFE (State Fusion Center) - GOHSEP | Governor's Office of Homeland Security & Emergency Preparedness

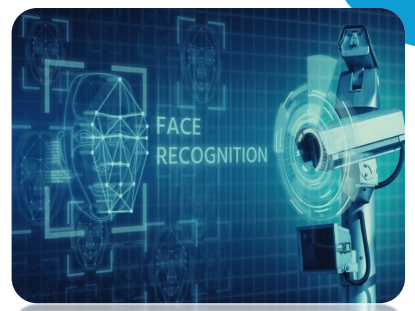
Constitutional Rights and Modern Technology

LA-SAFE Flow of Information



* Advisories + Citizens' Bulletins + Information Collection Requirement Bulletins + Information Bulletins + Intelligence Bulletins + Threat Assessments + Others as Needed.

Constitutional Rights and Modern Technology



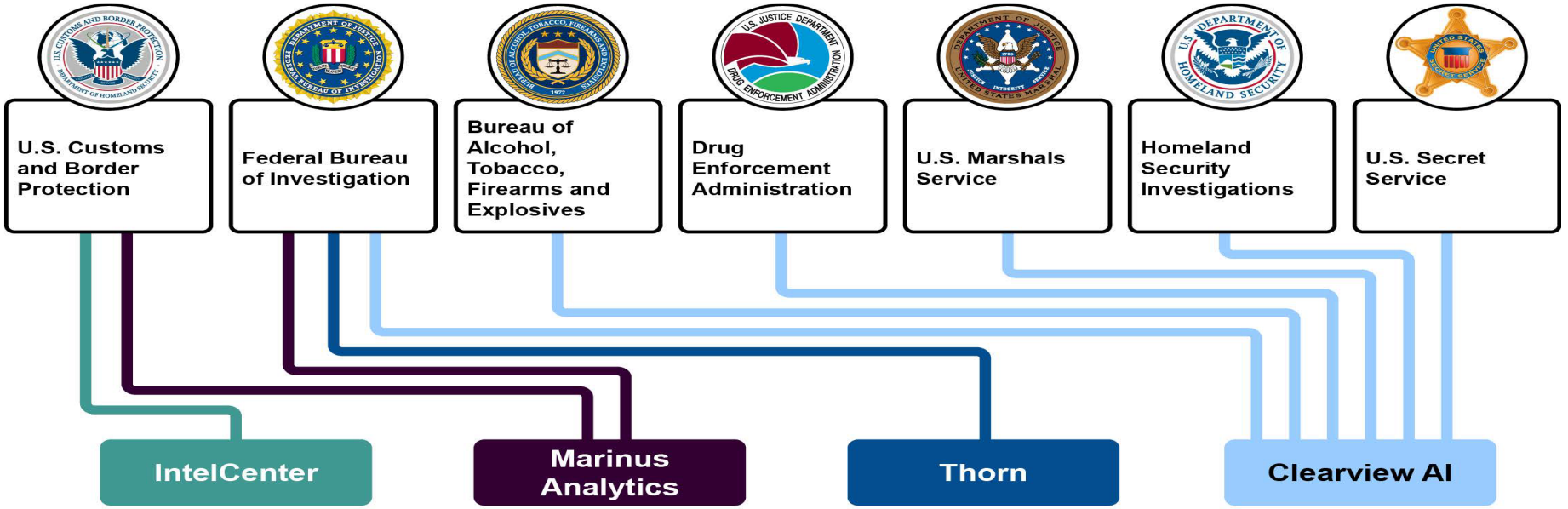
D. The Future

In ***Moody v. NetChoice**, LLC*, 144 S. Ct. 2383, 2438, nn. 54, 57 (2024), the United States Supreme Court cited *Breaking Down the Numbers: How Much Data Does the World Create Daily in 2024?*, Edge Delta (Mar. 11, 2024), https://www.edgedelta.com/company/blog/how-much-data-is-created-per-day

and

T. Xu, *AI Makes Decisions We Don't Understand—That's a Problem*, (Jul. 19, 2021), https://builtin.com/artificial-intelligence/ai-right-explanation.

These reports note (1) the immense volume of data created and collected; and (2) how the use and analysis of this data can be manipulated and abused. More importantly, they demonstrate how this data can be abused. With this knowledge, how do we justify the use of algorithms in litigation that can imprison citizens and determine property rights.



IntelCenter's Terrorist Facial Recognition is a web-based service. The service allows users to search photos against a gallery of over 2.4 million faces extracted from open-source terrorist data, according to service representatives and website materials.

Marinus Analytics's Traffic Jam is a web-based service that includes facial recognition capabilities. Traffic Jam uses images from the online commercial sex market to identify victims of human trafficking both in the United States and abroad, according to service representatives and website materials.

Thorn's Spotlight is a web-based service that includes facial recognition capabilities. Spotlight uses images from the online commercial sex market to find exploited children and identify their traffickers to support sex trafficking investigations, according to service representatives and website materials.

Clearview AI is a web-based facial recognition service using 30+ billion facial images sourced from publicly available websites, including news media, mugshot, and social media websites, among others, according to service representatives and website materials.

Source: GAO analysis of facial recognition service information. | GAO-24-107372

GAO – US Government Accountability Office

https://www.gao.gov/assets/gao-24-107372.pdf

Thank You!