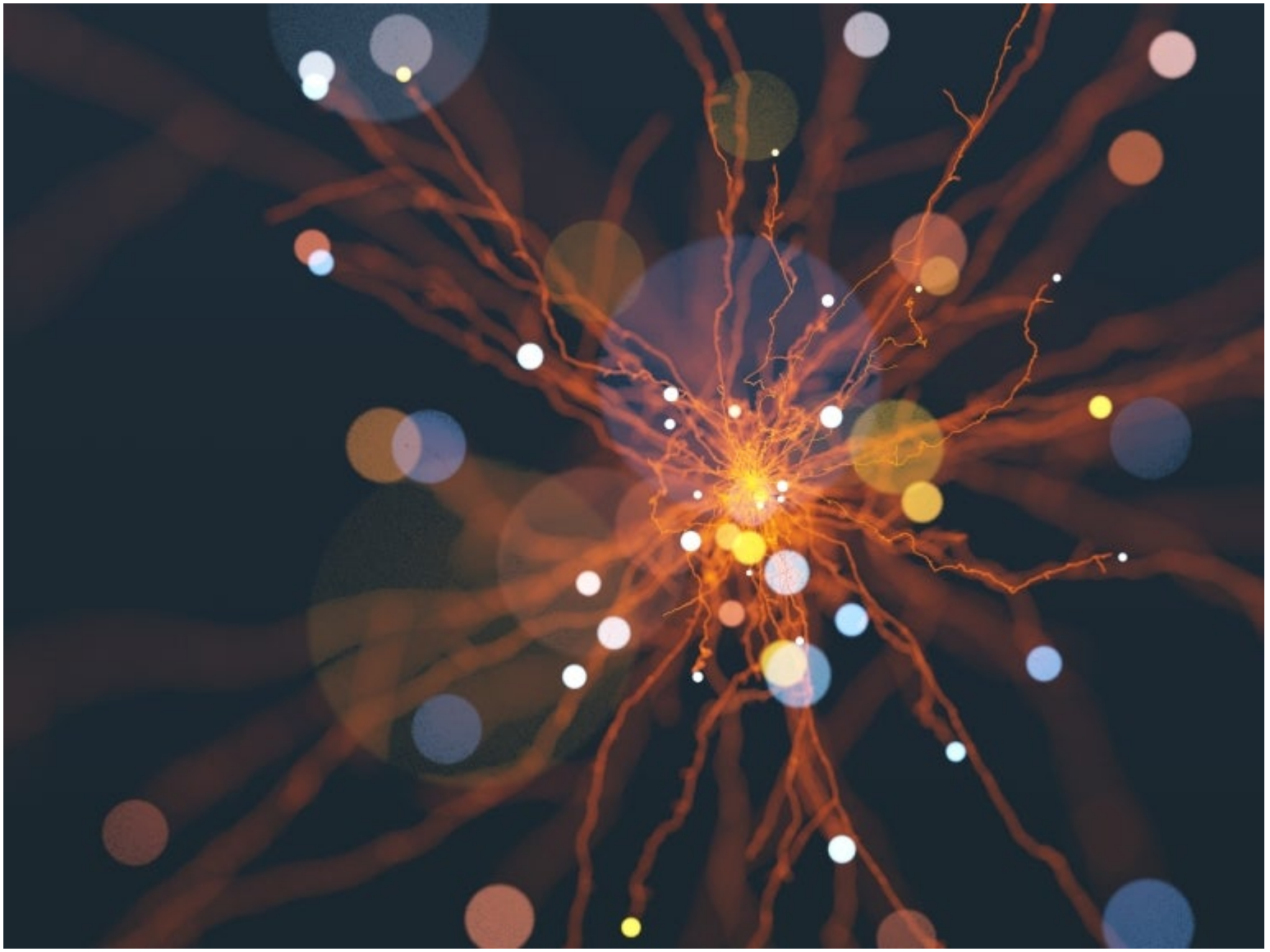
Blogs
October 04, 2023



The U.S. Department of Homeland Security (DHS) announced new policies on September 14, 2023, regarding its use and acquisition of artificial intelligence (AI) technologies, including facial recognition and face capture technologies. DHS also appointed Eric Hysen as the department's first chief AI officer.

Highlighting the potential "privacy, civil rights, and civil liberties" issues associated with the use of AI technologies by the department, Secretary of Homeland Security Alejandro N. Mayorkas explained that DHS must harness AI "effectively and responsibly." To that end, the new policies, which were developed by the DHS Artificial Intelligence Task Force, focus on two areas:

1. **Acquisition and use of AI technologies.** Policy Statement 139-06 provides that DHS will acquire and use AI only in a manner that is consistent with the Constitution and all other applicable laws and policies. DHS will not "collect, use, or disseminate data used in AI activities, or establish AI-enabled systems that make or support decisions, based on the inappropriate consideration of race, ethnicity, gender, national origin, religion, gender, sexual orientation, gender identity, age, nationality, medical condition, or disability." The policy statement also provides that DHS will honor Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, which establishes principles for the use of AI in the federal government for purposes other than national security and defense.
2. **Use of facial recognition and face capture technologies.** Directive 026-11 provides that uses of facial recognition and face capture technologies by DHS must be thoroughly tested to avoid bias and disparate impact.

The directive distinguishes between "facial recognition," "face capture," and "face analysis" technologies:

- The directive defines "**facial recognition**" as "technology that compares an individual's facial features to available images or video for verification or identification purposes," with "**verification**" being the "process of confirming an identity claim through [facial recognition] comparison" and "**identification**" being the "process of searching against [a facial recognition] enrollment database to find and return the [facial recognition] identifiers attributable to a single individual or multiple possible candidates."
- The directive defines "**face capture**" technology as "any combination of face detection and face collection technologies used to detect and/or extract a face from an image or video," including "liveness detection used to detect the presence of a live user."
- According to the directive, "**face analysis**" technology is defined as the "use of an algorithm to estimate characteristics of a subject by analyzing or deriving information from an image or video."

The directive includes the following requirements for DHS use of facial recognition, face capture, and facial analysis technologies:

1. Requiring DHS to review existing uses of facial recognition and face capture technologies and conducting periodic testing in the future, including under International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards and National Institute of Standards and Technology (NIST) guidelines.
2. Prohibiting the "use of [facial recognition] or [facial capture] technologies to profile, target, or discriminate against any individual solely for exercising their Constitutional rights or to enable systemic, indiscriminate, or wide-scale monitoring, surveillance, or tracking."
3. Providing U.S. citizens the right to opt out of the use of facial recognition for certain non-law enforcement uses.
4. Prohibiting facial recognition from being the sole basis for a law enforcement or civil enforcement action.
5. Limiting sharing of facial recognition and facial capture data collected, used, or maintained by DHS.
6. Requiring that facial recognition and facial capture technologies be secured against cybersecurity threats.
7. Prohibiting use of facial analysis technologies except for specific uses related to estimating age, which must be specifically approved by DHS oversight bodies.
8. Establishing oversight and technology review procedures under the DHS Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the Chief Information Officer.

Takeaways

These policies lay the framework for the department as it continues to look into how it "can leverage AI to advance critical missions" and how it "should be building defenses to nefarious uses of AI by adversaries."

While the policies apply only to DHS, they could impose new testing requirements on private parties who supply AI technologies to DHS and otherwise influence AI and biometric policies of private entities. Such entities should continue to consult experienced biometric privacy counsel in analyzing the risks associated with these technologies.

Follow us on social media @PerkinsCoieLLP, and if you have any questions or comments, contact us here. We invite you to learn more about our Digital Media & Entertainment, Gaming & Sports industry group and check out our podcast: *Innovation Unlocked: The Future of Entertainment*.

Authors

Nicola Menaldo

Partner
NMenaldo@perkinscoie.com 206.359.8000

Explore more in

Technology Transactions & Privacy Law
Blog series

Age of Disruption

We live in a disruptive age, with ever-accelerating advances in technology largely fueling the disruption permeating almost every aspect of our lives.

We created the *Age of Disruption* blog with the goal of exploring the emerging technologies reshaping society and the business and legal considerations that they raise. Subscribe ?

View the blog