Clearview.ai

Clearview AI's current position addresses the recommendations made by the Government Accountability Office (GAO), as outlined in their recent Artificial Intelligence (AI) Accountability Framework

> *"To help managers ensure accountability and responsible use of artificial intelligence (AI) in government programs and processes, GAO developed an AI accountability framework. This framework is organized around four complementary principles, which address governance, data, performance, and monitoring. For each principle, the framework describes key practices for federal agencies and other entities that are considering, selecting, and implementing AI systems. Each practice includes a set of questions for entities, auditors, and third-party assessors to consider, as well as procedures for auditors and third-party assessors".*[1]
>
> https://www.gao.gov/assets/gao-21-519sp.pdf, June 2021

With its AI-driven intelligence platform, Clearview AI is proud to support law enforcement and government agencies in their shared mission to keep our communities safe. By leveraging innovative technologies, such as facial recognition, law enforcement agencies can generate leads, insights, and relationships to close cases faster. With so many technology options available to the public safety community today, it is essential for agencies to have strong policies and protocols in place to ensure responsible use.

Recently, the GAO developed an accountability framework to guide agencies in their assessment and implementation of AI technologies. Clearview AI supports this framework and is equipped to support organizations adopting these technologies. Every day, our products are being used to investigate crime, rescue victims, and make significant contributions to public safety. Our technology is proven to help law enforcement reveal leads, insights, and relationships they did not know, by leveraging open source online imagery and facial recognition to help ensure public safety.

Below, we showcase how Clearview AI has built an industry-leading investigative platform, meeting the four principles of compliance, responsibility, transparency, and performance outlined in the GAO's framework for law enforcement agencies considering the use of facial recognition technology.

[1] GAO-21-519SP, *ARTIFICIAL INTELLIGENCE: An Accountability Framework for Federal Agencivtities*

DATA:

ENSURE QUALITY, RELIABILITY, AND REPRESENTATIVENESS OF DATA SOURCES AND PROCESSING

This method exponentially improves matching accuracy, greatly reduces false positives, and greatly reduces the potential for accuracy bias across different ethnicities.

Older facial recognition algorithms used manual forms of measurement focusing on facial landmarks such as the length of a person's nose, the size of a person's lips or the length of a jawline. Many of today's advanced facial recognition algorithms rely on an artificial intelligence called a "neural network". Neural networks use millions of faces to train algorithms. The training data set is consistently fed more examples to train the algorithm and diversify the database. This method exponentially improves matching accuracy, greatly reduces false positives, and greatly reduces the potential for accuracy bias across different ethnicities. The technology as a whole at times is inaccurately portrayed in the media and as a result is often misunderstood. In fact, facial recognition has improved dramatically over the last few years. As of April 2020, the best face identification algorithm has an error rate of just 0.08% compared to 4.1% for the leading algorithm in 2014, according to tests by the National Institute of Standards and Technology (NIST).[2] As of 2018, NIST found that more than 30 algorithms had achieved accuracies surpassing the best performance achieved in 2014.

To date and with due diligence, Clearview AI is not aware of a single instance where the technology was used by a client and it resulted in a wrongful arrest conviction.

TRAINING DATA SETS AND BIAS:

Unlike most facial recognition vendors, our algorithm was trained on a large, diverse, custom-built dataset, as opposed to pre-packaged training galleries, which may favor a certain gender or ethnicity and impact the accuracy of the results. Clearview AI has instead trained its algorithm on millions of facial images from diverse sources. As a result, the racial bias and accuracy disparities that have affected other applications are substantially eliminated. To date[3] and with due diligence, Clearview AI is not aware of a single instance where the technology was used by a client and it resulted in a wrongful arrest conviction.[4]

[2] CSIS: *How Accurate are Facial Recognition Systems – and Why Does It Matter?*

[3] As of 9/1/2021

[4] Clearview AI's application is intended to be used only in full accordance with the Clearview AI terms of service and user code of conduct.

MONITORING:

ENSURING, RELIABILITY, SECURITY AND RELEVANCE OVER TIME

Clearview AI recognizes the importance of ensuring reliability and accuracy in our algorithm and search results. We constantly evaluate the overall efficacy of the end-user experience.

Data storage and security are paramount concerns for our software development and data security teams. Our engineers routinely conduct automated code scans, looking for vulnerabilities in our dependencies within our source code and immediately flag and patch these issues upon discovery. Professional code audits are regularly conducted and a bug bounty program is in place with an industry-leading provider. All traffic routed through Clearview AI's secure data center is end-to-end encrypted with the latest TLS specifications and is protected by Cloudflare reverse proxy technology. All live data is stored on multiple servers inside a secured data center located in Northern Virginia with internal levels of access control.

All traffic routed through Clearview AI's secure data center is end-to-end encrypted with the latest TLS specifications and is protected by Cloudflare reverse proxy technology.

GOVERNANCE:

PROMOTING ACCOUNTABILITY BY ESTABLISHING PROCESSES TO MANAGE, OPERATE, AND OVERSEE BETTER TECHNOLOGY IMPLEMENTATIONS

Many available facial recognition solutions on the market today lack advanced system oversight, intake reporting (including requiring a case number and crime type for each search), and administrative tools which are essential and strongly recommended by legislators and privacy groups to ensure responsible use, integrity checks and agency accountability. Clearview AI has met this need with built-in system dashboards and output reporting mechanisms so law enforcement executives can demonstrate "how" and "why" the facial recognition system is being used. This allows greater oversight and for better transparency through audit trail records. These metrics capture and preserve search history, offer usage reports, provide visibility into sign-in history, and allows for greater levels of granularity and classifications such as: probe image retrieval, case number and investigation type, device used, and most recent search. Searches can also be measured by successful hit rates as well as the total counts per day, and per user. This purposely designed administrative functionality quantifies usage and breaks down the total number of search results by individual unit and crime type. This offers agency administrators tangible metrics that may be shared internally, with legislators and policy makers, or the public.

Clearview AI has met this need with built-in system dashboards and output reporting mechanisms so law enforcement executives can demonstrate "how" and "why" the facial recognition system is being used. This allows greater oversight and for better transparency through audit trail records.

Regularly collaborating with law enforcement agencies and legislators, our software development team strives to ensure responsible use of our platform.

Clearview AI is continuously improving upon our products and services. Regularly collaborating with law enforcement agencies and legislators, our software development team strives to ensure responsible use of our platform. All users are required to sign Terms & Conditions on appropriate use and undergo training before use. System oversight and administrative tools capture, catalogue and time stamp the search history and other metrics for each user assigned to the system. To maintain integrity, output reports can be shared with supervisors or any other user-defined stakeholder needing visibility. Clearview AI acknowledges individual policies and state requirements do vary across many states and government agencies. As a result, many of the compliance and auditing features made available to our clients are customizable to facilitate an agency's ability to meet system oversight, accountability and CJIS compliance standards.

PERFORMANCE:

PRODUCING RESULTS CONSISTENT WITH PROGRAM OBJECTIVES

Clearview AI knows that technology procurements must be coupled with an investment in people and processes to maximize the return of a successful deployment within the agency. Responsibly deployed facial recognition technology programs establish clear program objectives defining how the agency intends to utilize, monitor and measure the overall value for public safety initiatives with each deployment.

Clearview AI also recognizes the use of facial recognition technology is a very human centric process. By intentional design, Clearview AI does not include match or percentage scoring with its results. Instead, the platform offers three color-coded classifications for systemwide image search results. A green circle indicates a higher confidence reading that there is a potential match that needs to be verified by a human examiner. A yellow circle indicates there is a medium level of confidence in search results that needs to be examined in greater detail by the face examiner. This lesser confidence rating indicates the probe image may have a minor impediment the system has flagged. This could be backlighting, overexposure, resolution degradation, distance of a subject within the probe photo, variations in head pose or occlusion. In these cases, these lower quality images can be enrolled into the Clearview AI platform and still return quality results when verified by the face examiner. The third classification is a white circle which implies the Clearview AI system has simply detected a face in the photo that can be searched. This helps support the "human-in-the-loop" decision making process and encourages every face examiner using the Clearview AI system to verify and validate results without a sole reliance on facial recognition technology.

Clearview AI also recognizes the use of facial recognition technology is a very human centric process. By intentional design, Clearview AI does not include match or percentage scoring with its results.

Clearview AI is intentionally developed by design to be an assistive technology that narrows down an open-sourced repository of over 20 billion publicly available images to a manageable and accurate list of images for review. By contrast, other facial recognition systems return a standard number of results, usually in the hundreds, with many results being determined as false positives.

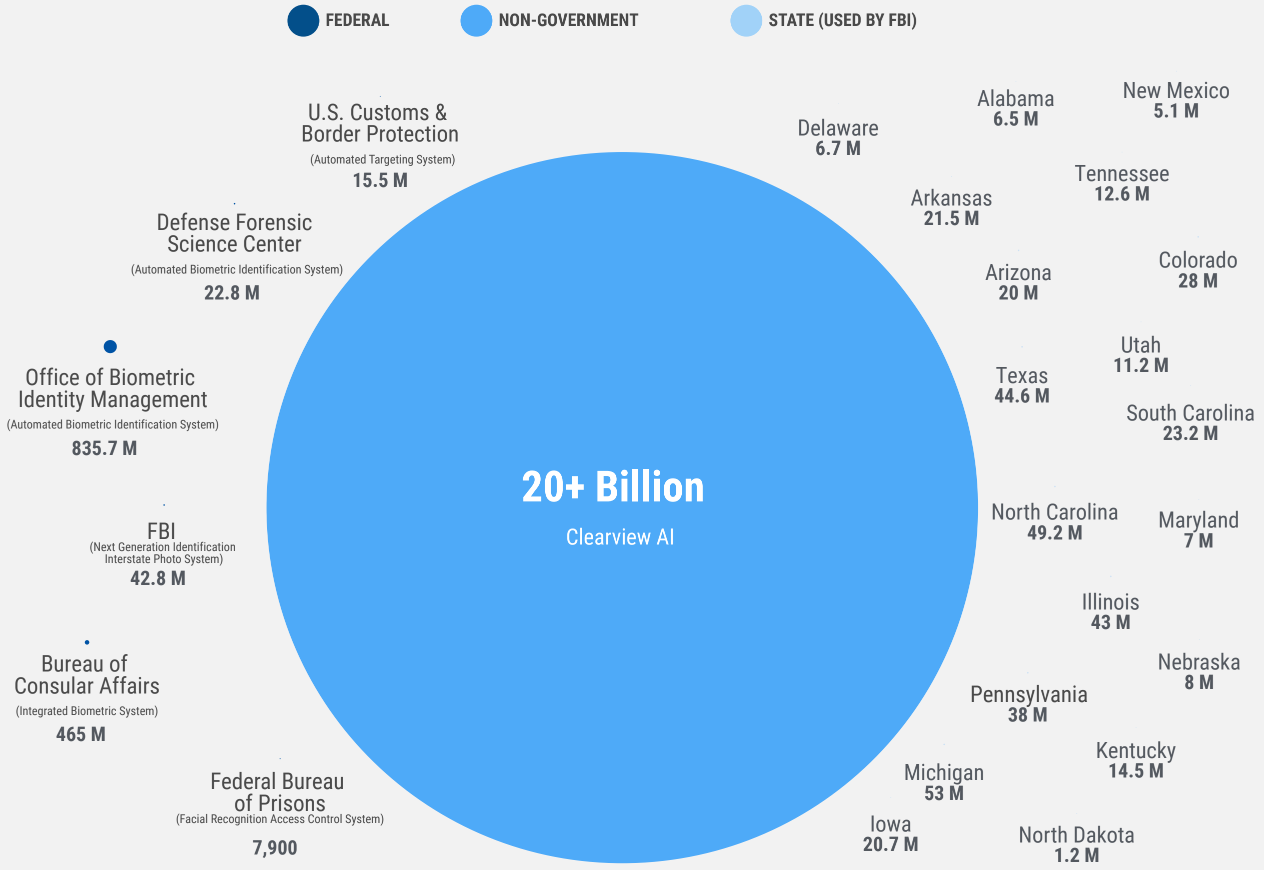
These design decisions lessen the chance of a face examiner making a wrongful identification, improve lead efficiency, and contribute to the integrity and workflow of every investigation requiring the use of facial recognition technology. Additionally, when used as a forensic application for investigative purposes, results from a Clearview AI search are not intended to be used as evidence in court. The onus always falls on the agencies deploying facial recognition systems to consider all application results as investigative leads which require additional identity validation using traditional law enforcement means. A Clearview AI lead is to be considered only one part of the greater investigative process.

Additionally, when used as a forensic application for investigative purposes, results from a Clearview AI search are not intended to be used as evidence in court.

CONCLUSION

Clearview AI embraces its role partnering with law enforcement and government organizations to provide solutions that support their mission for public safety and is committed to working alongside the Government Accountability Office to ensure AI driven technology is used responsibly and effectively. We welcome your feedback and look forward to ongoing discussions to better address privacy concerns, help gain a better understanding of our technology offerings and meet the needs of our public safety partners and the communities which they are sworn to protect.

Selected Federal, State, and Non-government Systems with Facial Recognition Technology Used by Federal Agencies that Employ Law Enforcement Officers, and the Number of Photos in Them



Source: United States Government Accountability Office: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks June 2021

CONTACT US TO REQUEST A PRODUCT DEMONSTRATION

www.clearview.ai | info@clearview.ai

Clearview.ai