



U.S. Department of the Interior ADAPTED PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires completion of this Adapted Privacy Impact Assessment (Adapted PIA) for all third-party websites or applications (TPWAs) utilized for agency communication, outreach, public engagement, or data collection activities. This assessment ensures compliance with federal privacy requirements including the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, Office of Management and Budget (OMB) Memorandum M-10-23, OMB Circular A-130, and the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5. The Adapted PIA evaluates potential privacy risks, clearly documents how personally identifiable information (PII) is handled and safeguarded on external platforms and outlines specific mitigation measures to protect individual privacy. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via this [form](#). For further guidance, consult the [DOI PIA Guide](#).

System or Project Name:	Clearview AI
System or Project Acronym:	N/A
Date submitted for review:	January 23, 2026
System Operational Status:	Operational

Point of Contact

Name:	Dianna Taylor
Title:	Privacy Officer
Office:	Department Privacy Office
Phone:	(202) 208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: Specific Purpose of the Agency's Use of the Third-Party Website or Application

1. What is the specific purpose of the agency's use of the TPWA, and how does it align with DOI's mission?

The U.S. Department of the Interior (DOI), through the Bureau of Indian Affairs Office of Justice Services (BIA OJS), uses **Clearview AI** (<https://www.clearview.ai>), a third party web based application, to support authorized law enforcement and investigative activities. The primary purpose of this TPWA is to allow trained BIA OJS personnel to upload photographs and receive links to publicly available images on the internet that may contain visually similar faces, to develop investigative leads. Clearview AI's facial recognition technology analyzes uploaded photos by comparing them with publicly accessible images from the Internet. When matches are found, it provides URL links to help users identify and locate missing persons, crime victims, and potential suspects.

Clearview AI is used in support of investigations involving missing persons, crime victims, and criminal suspects. The system does not make final determinations regarding identity. All outputs are treated as investigative leads and must be independently reviewed and verified by BIA OJS personnel prior to any law enforcement action. Use of Clearview AI directly supports DOI's mission to protect public safety and uphold the rule of law within



Indian Country by:

- Assisting law enforcement investigations involving serious public safety concerns
- Supporting timely identification efforts for missing persons and victims
- Enhancing investigative capabilities while maintaining human oversight and accountability

Clearview AI is used as a supplemental investigative tool and does not replace DOI systems of record or official case management systems. All investigative records derived from Clearview AI use are maintained within DOI authorized systems in accordance with applicable privacy, security, and records management requirements.

2. Is the use of the TPWA authorized by applicable law, regulation, or policy? Provide the legal authorities.

Yes. The use of Clearview AI is authorized under the following laws, regulations, and policies:

- **OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications"** - Establishes agency responsibilities for privacy, security, and records management when using third-party websites and applications, including requirements for transparency and risk assessment.
- **Federal Records Act (44 U.S.C. Chapters 21, 29, 31, and 33)** - Governs the creation, maintenance, and disposition of federal records. Investigative records derived from Clearview AI use that meet the definition of federal records are managed in accordance with approved DOI records schedules.
- **25 U.S.C. § 2803 - Authority of Bureau of Indian Affairs Law Enforcement**
Authorizes the Bureau of Indian Affairs Office of Justice Services (BIA OJS) to conduct criminal investigations, enforce federal law, and support public safety and justice services in Indian Country. This authority supports the use of investigative technologies, such as Clearview AI, to generate leads related to criminal activity, missing persons, and victim identification.
- **25 C.F.R. Part 12 - Indian Country Law Enforcement**
Implements statutory authority for BIA law enforcement operations, including investigative activities necessary to carry out BIA OJS's public safety mission.

Collectively, these authorities establish BIA OJS's legal authority to use Clearview AI as an investigative tool in support of its law enforcement mission, while ensuring compliance with applicable federal privacy, security, and records management requirements.

3. Does the TPWA involve any integration with DOI systems?

- ☐ Yes: Describe the nature of the integration and data flow.
- ☒ No

Clearview AI operates independently from DOI-managed systems and does not have any direct technical or data exchange integrations with DOI databases. There are no application programming interfaces (APIs), automated data feeds, single sign-on connections, or system-to-system integrations between Clearview AI and DOI systems.

Authorized users access Clearview AI through a secure, web-based interface. Any investigative records or documentation derived from Clearview AI use are transferred manually by authorized personnel and maintained only within DOI-authorized law enforcement systems in accordance with applicable privacy, security, and



records management requirements.

Section 2: PII Collection and Source

1. What types of PII might become available to DOI through the use of the TPWA? Check all that apply.

- | | | |
|--|---|---|
| ☒ Name (full, first or last) | ☐ Home telephone number | ☐ Employment or resume info |
| ☐ Aliases/nickname | ☐ Personal Email | ☐ Full or Truncated SSN |
| ☐ Driver's license | ☐ Mailing or home address | ☒ Physical characteristics |
| ☐ Citizenship | ☐ Religious preference | ☒ Biometrics/facial recognition |
| ☐ Legal Status | ☐ Mother's maiden name | ☐ Vehicle information |
| ☐ Sex | ☐ Marital status | ☐ Passport information |
| ☐ Race or ethnicity | ☐ Spouse Information | ☐ Travel information |
| ☐ Date of birth | ☐ Child or family information | ☐ Parent's name |
| ☐ Place of birth | ☐ Emergency contact info | ☐ Credit card number |
| ☐ Personal cell phone number | ☐ Financial information | ☐ Nationality |
| ☐ Tribal or other ID number | ☐ Education information | ☐ Disability Information |
| ☐ Military records | ☒ Other: Describe below | |

Through the use of Clearview AI, DOI may have access to the following types of personally identifiable information (PII):

- **Biometrics / Facial Recognition and Physical Characteristics** - Photographs uploaded by authorized BIA OJS personnel may contain facial features and physical characteristics that constitute biometric PII. These images are submitted by users in support of authorized law enforcement and investigative activities and are used solely to generate investigative leads. Names are not submitted with the photographs.

Photographs uploaded by authorized BIA OJS personnel may contain facial features and physical characteristics that constitute biometric PII. Images are uploaded without accompanying names or other identifiers and are used solely to generate investigative leads by comparing against publicly available images. Clearview AI does not make identity determinations, and all results are independently reviewed and validated by BIA OJS personnel.

- **Name (For establishing Employee Account Information Only)** - First and last name, business email address, and business phone number are provided by BIA OJS personnel during account creation for authentication, access control, and audit purposes.

Clearview AI does not collect Social Security numbers, financial information, home contact information, geolocation data, or other sensitive personal data from members of the public. PII is not collected directly from individuals by DOI through the TPWA, and members of the public do not interact with Clearview AI. Providing employee account information is required for authorized users to access the system; submission of photographs is limited to images relevant to official investigative purposes.



All PII made available through the TPWA is handled in accordance with applicable DOI privacy, security, and records management requirements.

2. What is the source of the PII?

- | | |
|--|---|
| ☐ User-submitted (e.g., contact forms) | ☒ Publicly visible profile data |
| ☐ Automatically collected (e.g., cookies, trackers) | ☒ Other: <i>Specify below</i> |
| ☐ Derived analytics (e.g., engagement trends) | |

The PII available to DOI through the use of Clearview AI comes from the following sources:

- **Authorized User Submission** - Photographs are uploaded by authorized Bureau of Indian Affairs Office of Justice Services (BIA OJS) personnel in support of official law enforcement and investigative activities. These images may contain biometric identifiers and physical characteristics and are provided by DOI personnel, not by members of the public.
- **Publicly Visible Third-Party Content** - Clearview AI returns links to images that are publicly available on the internet. These images originate from third-party websites and social media platforms where the content is publicly visible at the time it is accessed.
- **Employee Account Information** - Limited employee account information, including first and last name, business email address, and business phone number, is provided directly by BIA OJS personnel during account creation for authentication and access management purposes.

Clearview AI does not automatically collect technical or tracking information such as IP addresses, cookies, device identifiers, or geolocation data for DOI use, and DOI does not receive platform analytics or administrative reporting from the TPWA. DOI personnel access PII through the Clearview AI interface and retrieve any investigative information manually for documentation within DOI-authorized systems.

3. Will DOI collect, store, or retain any of this PII?

- ☐ Yes: *Describe where/how it will be stored and protected*
- ☒ No: Only accessed/viewed through the TPWA

No. DOI does not collect, store, or retain PII within the Clearview AI platform. Photographs and search results are accessed and reviewed solely through the TPWA's web-based interface. Uploaded images are processed by the vendor to generate potential matches and are not retained by DOI within the TPWA.

Any investigative records or documentation created as a result of Clearview AI use are generated separately by BIA OJS personnel and maintained only within DOI-authorized law enforcement systems, in accordance with the Privacy Act and applicable NARA-approved records schedules. No PII is downloaded, copied, or transferred from the TPWA into DOI systems outside of established investigative documentation processes.

4. Does the use trigger the Paperwork Reduction Act (PRA)?

- ☐ Yes: Provide OMB Control Number or describe PRA compliance
- ☒ No



No. The use of Clearview AI does not trigger the Paperwork Reduction Act. DOI does not solicit or require standardized information from members of the public through surveys, forms, or questionnaires using the TPWA. Clearview AI does not involve DOI requesting the same information from ten (10) or more individuals within a 12-month period for agency use.

Public interaction with the TPWA does not occur, and any information processed through Clearview AI is provided by authorized DOI personnel or accessed as publicly available content. Based on these factors, PRA applicability criteria are not met.

Section 3: Use and Handling of PII

1. How will DOI use the PII?

The Department of the Interior (DOI), through the Bureau of Indian Affairs Office of Justice Services (BIA OJS), will use biometric and image based PII obtained through Clearview AI solely to support authorized law enforcement and investigative activities that align with DOI's mission to protect public safety and uphold the rule of law within Indian Country.

Specifically, PII used through Clearview AI consists of photographs containing facial features and physical characteristics submitted by authorized BIA OJS personnel, as well as limited employee account information (name and business contact information) used for DOI employee system access and audit purposes.

PII accessed through Clearview AI may be used to:

- **"Support Investigative Activities** - Perform facial recognition comparisons between uploaded photographs and publicly available images to generate investigative leads related to missing persons, crime victims, and criminal suspects."
- **"Verification and Corroboration** - Assist investigators in corroborating potential identities by comparing Clearview AI results with official records, case files, and other reliable investigative sources."
- **"Law Enforcement Decision Support** - Provide investigative context and leads to inform law enforcement activities, while ensuring that all determinations are made by trained personnel and not by automated systems."

Clearview AI does not make final determinations regarding identity. The system's outputs are treated as investigative leads only and must be independently reviewed and validated by trained BIA OJS personnel before any operational or investigative action is taken. PII is not used for automated decision-making, profiling, marketing, public engagement, or any non-law enforcement purpose.

2. Will the PII be used to create new data, profiles, or inferences?

- ☐ Yes: *Describe purpose and safeguards for derived data*
- ☒ No



No additional data, profiling, or inference generation will occur beyond the original information provided.

3. What measures are in place to validate the accuracy and completeness of data received from external sources?

No. DOI will not use PII accessed through Clearview AI to create new datasets, profiles, or draw inferences about individuals beyond the scope of the original information reviewed. Clearview AI is used solely as a facial comparison tool to identify potential visual similarities between an uploaded image and publicly available images. When a Clearview AI user uploads an image, the technology processes it and returns Internet URLs to publicly available images with similar faces. The BIA Office of Justice Services (OJS) personnel will review these links to identify and locate missing persons, crime victims, and suspects. Clearview AI does not perform identification or verification of the person in the uploaded image.

DOI will not develop profiles of individuals, conduct behavioral analysis, or generate inferred attributes based on Clearview AI results. Any investigative conclusions are made by trained BIA OJS personnel based on independent review and corroboration with official records and other reliable sources, not through automated profiling or inference generation. All use of PII remains consistent with applicable Privacy Act requirements, published Systems of Records Notices, and DOI privacy policy.

4. Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

- ☒ Yes
☐ No

Yes. DOI's use of Clearview AI may result in records derived from investigative activities being incorporated into existing DOI law enforcement recordkeeping systems that are retrieved by personal identifiers. These records do not create a new standalone system of records specific to Clearview AI, nor do they modify existing retrieval practices.

Rather, records created as a result of Clearview AI use are incorporated into established DOI law enforcement systems of records that already support investigative and case management activities.

5. Provide the name and identifier for the Privacy Act system of records.

Records created or maintained as a result of Clearview AI use are covered under the following existing DOI Systems of Records Notices, based on the nature of the investigative activity:

- **INTERIOR/DOI-10, Law Enforcement Records Management System (LE RMS)**, published in the Federal Register on January 10, 2024 (89 FR 1594). This SORN covers records related to criminal investigations, law enforcement activities, and associated investigative materials derived from Clearview AI that are retrieved by personal identifiers.
- **INTERIOR/BIA-18, Case Incident Reporting System**, published in the Federal Register on January 6, 2005 (70 FR 1264), applies only to photographs or imagery not associated with a criminal investigation.

No new system of records is established by the use of Clearview AI.



Section 4: Sharing and Disclosure of PII

1. With whom will the PII be shared?

- ☒ **Within the Bureau/Office:** Describe how the data will be used below.
- ☒ **Tribal, State or Local Agencies:** Describe how the data will be used below.
- ☐ **Other Bureaus/Offices:** Describe how the data will be used below.
- ☐ **Contractor:** Describe how the data will be used below.
- ☒ **Other Federal Agencies:** Describe the federal agency and how the data will be used
- ☐ **Other Third-Party Sources:** Describe how the data will be used below.

Personally identifiable information (PII) derived from the use of Clearview AI may be shared only in limited circumstances and solely in support of authorized law enforcement and investigative activities, in accordance with the Privacy Act of 1974, applicable Systems of Records Notices (SORNs), and DOI privacy policy.

- **Within the Bureau/Office (BIA OJS)** - Investigative information derived from Clearview AI results may be shared internally among authorized BIA OJS personnel on a need to know basis to support active investigations. Access is restricted to personnel with appropriate authority and training, and information is protected by DOI access controls and law enforcement safeguards.
- **Other Federal Agencies** - PII may be shared with other federal law enforcement agencies when necessary to support joint active investigations, information sharing, or coordination related to criminal matters, missing persons, or public safety concerns. Such sharing occurs under established law enforcement authorities and routine uses described in applicable SORNs, and information is shared only in identifiable form when necessary for the investigative purpose.
- **Tribal, State, or Local Agencies** - PII may be shared with Tribal, state, or local law enforcement agencies in furtherance of active investigations or cooperative law enforcement efforts. Sharing is conducted in accordance with applicable law enforcement agreements, routine uses, and information sharing protocols, and is limited to the minimum PII necessary to accomplish the authorized purpose.

PII is not shared with contractors, vendors, or the general public through Clearview AI. Clearview AI does not provide public access to search results, and DOI does not disclose PII outside authorized law enforcement channels. All sharing is subject to applicable privacy, security, and records management requirements.

2. What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

PII associated with the use of Clearview AI is protected from unauthorized or unintended use through a combination of administrative, technical, and procedural safeguards that align with DOI privacy and security requirements.

- **Access Controls** - Access to Clearview AI and any investigative information derived from its use is restricted to authorized BIA OJS personnel with a demonstrated need to know. User access is managed



through individual credentials, and use of the system is limited to official law enforcement purposes.

- **Data Minimization and Purpose Limitation** - PII is shared or accessed only to the extent necessary to support authorized investigative activities. Clearview AI results are treated as investigative leads only, and information sharing is limited to the minimum PII necessary to accomplish the authorized purpose.
- **Encryption and Secure Transmission** - Data transmitted between authorized users and the Clearview AI platform is encrypted in transit using industry-standard encryption protocols. Investigative records derived from Clearview AI use are protected within DOI-authorized systems in accordance with DOI security requirements.
- **Oversight and Auditability** - User activity within Clearview AI is subject to oversight, and investigative use of results is governed by BIA OJS investigative protocols. Any suspected misuse, unauthorized access, or inappropriate disclosure is addressed in accordance with DOI incident response and privacy breach handling procedures.
- **Training and Rules of Behavior** - Authorized personnel using Clearview AI are required to complete annual privacy and security awareness training and are subject to DOI Rules of Behavior and law enforcement conduct standards.

These safeguards ensure that PII is used only for purposes authorized by law and described in this PIA and are consistent with DOI privacy policy and applicable federal security and privacy requirements, including relevant controls from NIST SP 800-53 Rev. 5.

Section 5. Retention and Data Minimization

1. Will DOI retain any PII from the TPWA?

☒ Yes: Describe where, how long, and under which records schedule

☐ No

Yes. DOI does not retain PII within the Clearview AI third party website or application. Any PII accessed through Clearview AI is viewed only within the TPWA for the limited purpose of generating investigative leads and is not downloaded or stored directly from the platform.

However, investigative records or case documentation that reference Clearview AI results are retained within DOI authorized law enforcement systems, specifically INTERIOR DOI-10 Law Enforcement Records Management System (LE RMS), when associated with a criminal investigation.

Retention and disposition of these records are governed by applicable NARA approved law enforcement records schedules and existing Privacy Act coverage. Photographs or imagery not associated with a criminal investigation are governed under INTERIOR BIA-18, Case Incident Reporting System, in accordance with its applicable records schedule.

The use of Clearview AI does not create a new system of records and does not alter existing retention practices beyond incorporation into established DOI law enforcement recordkeeping systems.



2. How does DOI ensure minimal and relevant data retention?

DOI ensures minimal and relevant data retention by applying data minimization principles and limiting the use and retention of PII to what is strictly necessary to support authorized law enforcement and investigative activities.

Key measures include:

- **Limited Use Within the TPWA** - Clearview AI results are accessed only for investigative lead development and are not retained within DOI systems unless incorporated into official investigative records consistent with established law enforcement procedures.
- **Records Schedule Compliance** - Any investigative records derived from Clearview AI use are retained only in DOI-authorized systems and managed in accordance with Investigative Records (NC-075-75-001) or its approved successor schedule, which governs retention and disposition of DOI law enforcement investigative records.
- **Purpose Limitation** - PII is used solely for authorized investigative purposes and is not retained for analytics, profiling, or secondary uses unrelated to the original law enforcement mission.
- **Periodic Review and Oversight** - Investigative records are subject to routine review under BIA OJS records management and privacy oversight processes to ensure continued relevance and appropriate disposition.
- **Vendor Retention Controls** - Clearview AI's handling of submitted images and search activity is governed by contractual and policy requirements, and DOI does not direct the vendor to retain PII beyond what is necessary to provide the service.

These practices ensure that DOI retains only the minimum PII necessary to fulfill authorized law enforcement mission requirements, prevents unnecessary data accumulation, and remains consistent with the Privacy Act, DOI privacy policy, and NARA Federal Records Management Records Control Schedule Investigative Records ([NC-075-75-001](#)) or its approved successor.

Section 6: Security and Access Controls

1. Have privacy and security officials coordinated to develop safeguards?

- ☒ Yes
☐ No: *Explain below*

DOI Privacy and Information Security officials have coordinated to identify and implement appropriate safeguards associated with the use of Clearview AI. This coordination included review of privacy risks, security considerations, and compliance with DOI policies and applicable federal requirements prior to and during use of hookup of the TPWA.

Coordination activities included:

- Review of the Privacy Threshold Analysis (PTA) and determination that a Privacy Impact Assessment



(PIA) was required

- Evaluation of privacy risks associated with the use of facial recognition technology and access to publicly available images. OJS reviewed Clearview AI SOC 2 compliance documentation.
- Confirmation that Clearview AI is used solely to support authorized law enforcement and investigative activities
- Alignment on safeguards related to access controls, data minimization, and oversight
- Identification of applicable incident response and breach handling procedures consistent with the DOI Privacy Breach Response Plan

In the event of a suspected or confirmed PII incident, responsibilities are divided as follows:

- Clearview AI is responsible for detecting, reporting, and responding to security incidents affecting its platform in accordance with contractual obligations and applicable law, including prompt notification to DOI when the incident may involve DOI-related data or system use.
- BIA OJS / DOI is responsible for assessing the impact of any incident involving DOI-controlled data or information incorporated into DOI systems, initiating response actions consistent with the DOI Privacy Breach Response Plan, coordinating with OCIO Cybersecurity Team and Privacy Team to fulfill any required notification, mitigation, or reporting obligations.

2. What technical safeguards are in place?

- | | |
|---|---|
| ☒ Access control (role-based) | ☒ Monitoring and alerting |
| ☒ Encryption at rest and in transit | ☐ FedRAMP-compliant cloud security |
| ☒ Multi-factor authentication | ☐ Other: <i>Specify</i> |

The following technical safeguards are in place to protect PII associated with the use of Clearview AI:

- **Role-Based Access Controls** - Access to Clearview AI is restricted to authorized BIA OJS personnel with a demonstrated need-to-know. User access is granted on an individual basis and limited to official law enforcement purposes.
- **Authentication Controls** - User authentication mechanisms, including strong credential requirements and multi-factor authentication where supported, are used to prevent unauthorized access to the platform.
- **Encryption in Transit** - Data transmitted between authorized users and the Clearview AI platform is protected using industry-standard encryption protocols to safeguard information during transmission.
- **Auditability and Oversight** - Use of Clearview AI is subject to oversight through administrative and operational controls. Investigative use of results follows established BIA OJS investigative protocols, and any suspected misuse or anomalous activity is addressed in accordance with DOI security and privacy incident response procedures.
- **Data Minimization Safeguards** - DOI does not integrate Clearview AI with DOI-managed systems, and PII is not automatically transferred or stored within DOI systems through the TPWA. Any investigative records derived from Clearview AI use are documented and secured within DOI-authorized law enforcement systems.

These safeguards align with DOI security and privacy policies and applicable federal standards, including relevant



NIST SP 800-53 Rev. 5 control families, and ensure that access to PII is limited, monitored, and protected against unauthorized use.

Section 7: Additional Privacy Risks and Mitigations

1. What additional privacy risks exist (e.g., persistent tracking, profiling, third-party behavioral ads)?

The use of Clearview AI introduces several privacy risks that are inherent to third-party facial recognition technology and access to publicly available imagery, beyond those typically present in DOI-managed systems.

- **Misidentification and False Positives** - Facial recognition results may generate incorrect or incomplete matches due to image quality, limited context, or algorithmic limitations. Misidentification could impact individuals if results are relied upon without independent verification.
- **Use of Publicly Available Images** - Clearview AI searches publicly accessible images sourced from the internet. Individuals whose images appear in search results may be unaware that their likeness is being used in this context, raising concerns related to notice, consent, and expectations of privacy.
- **Limited DOI Control Over Vendor Architecture** - As a third-party platform, Clearview AI's underlying technical architecture, algorithms, and data sourcing practices are managed by the vendor, limiting DOI's direct control over how facial recognition processes are performed.
- **Residual Access Risk** - Vendor personnel may have technical access to system components as part of system maintenance or operations, which presents a residual risk that must be managed through contractual, policy, and oversight mechanisms.
- **Potential Policy or Technology Changes** - Changes to Clearview AI's privacy practices, system functionality, or data sources could introduce new privacy risks that require continued monitoring and reassessment.

These risks are mitigated through strict purpose limitation, access controls, mandatory training, independent validation of results by trained personnel, and ongoing privacy and security oversight. Clearview AI results are treated as investigative leads only and are not used as the sole basis for identity determinations or enforcement actions.

2. What steps are taken to mitigate those risks?

DOI employs a combination of administrative, technical, contractual, and oversight measures to mitigate the privacy risks associated with the use of Clearview AI.

- **Purpose Limitation and Use Restrictions** - Clearview AI is used solely to support authorized law enforcement and investigative activities. Search results are treated as investigative leads only and are not used as the sole basis for identity determination, enforcement action, or adverse decisions.
- **Independent Verification and Human Review** - All results generated by Clearview AI are independently reviewed and validated by trained BIA OJS personnel using additional investigative methods and official records, mitigating the risk of misidentification or false positives.
- **Access Controls and Authorized Use** - Access to Clearview AI is limited to authorized personnel with a demonstrated need-to-know. User access is role-restricted, and use of the system is governed by DOI



Rules of Behavior and law enforcement policies.

- **Training and Awareness** - Authorized users receive required privacy and security awareness training and are instructed on appropriate use of facial recognition technology, including limitations, risks, and proper handling of PII.
- **Data Minimization** - DOI does not retain PII within the Clearview AI platform and does not integrate the TPWA with DOI-managed systems. Any investigative records derived from Clearview AI use are retained only in DOI-authorized systems in accordance with approved records schedules.
- **Vendor Oversight and Incident Response** - Clearview AI's handling of data is subject to contractual and policy requirements, including obligations related to safeguarding information and reporting security or privacy incidents. Any suspected misuse or incident is addressed in accordance with the DOI Privacy Breach Response Plan.
- **Ongoing Privacy and Security Review** - DOI Privacy and Information Security officials periodically review the use of Clearview AI to assess emerging risks, changes in vendor practices, or updates to applicable law or policy.

These measures collectively reduce the likelihood and potential impact of privacy risks associated with facial recognition technology and third-party access to publicly available images, while ensuring continued compliance with DOI privacy and security requirements.

3. How are users notified of data collection and risks?

- | | |
|--|---|
| ☐ Privacy Act Statement | ☐ Website banners/notices |
| ☒ Terms of Use | ☐ None: <i>Explain why</i> |
| ☒ DOI Privacy Policy | |

Authorized users of Clearview AI are notified of data collection practices, permitted uses, and associated privacy risks through multiple administrative and policy-based mechanisms.

- **Terms of Use and Vendor Privacy Policy** - Authorized BIA OJS personnel are subject to Clearview AI's Terms of Use and Privacy Policy, which describe the collection, processing, and use of images and associated data within the platform. Users must acknowledge and comply with these terms prior to accessing the system.
- **DOI Privacy Policy and Rules of Behavior** - BIA OJS' Use of Clearview AI is governed by DOI privacy policy, DOI Rules of Behavior, and applicable law enforcement policies. These policies inform users of their responsibilities regarding the handling of PII, authorized uses of information, and potential consequences of misuse.
- **Training and User Awareness** - Authorized users receive privacy and security awareness training that includes instruction on appropriate handling of PII, limitations of facial recognition technology, risks of misidentification, and requirements for independent verification of results.
- **Operational Notice** - Clearview AI is not a public-facing platform. Members of the public do not interact directly with the TPWA through DOI, and DOI does not solicit information from individuals through Clearview AI. As a result, Privacy Act Statements or public-facing website notices are not applicable to this use.

These notification mechanisms ensure that authorized users understand what data is accessed through the



TPWA, how it may be used, and the privacy risks associated with facial recognition technology, consistent with OMB Memorandum M-10-23 and DOI privacy requirements.

Section 8: System of Records Consideration

1. Will use of the TPWA create or modify a Privacy Act System of Records (SOR)?

- ☒ Yes: *Describe whether data is retrieved by name or unique identifier*
☐ No

Yes. Use of Clearview AI supports authorized law enforcement and investigative activities conducted by the Bureau of Indian Affairs Office of Justice Services (BIA OJS). While Clearview AI itself does not serve as a system of record and does not retain user-uploaded images, investigative records derived from the use of Clearview AI may be incorporated into DOI-managed law enforcement systems.

When investigative outputs (e.g., leads, screenshots, case notes, or corroborated findings) are documented and retained within DOI-authorized systems and retrieved by personal identifiers such as name or other unique identifiers, they constitute records subject to the Privacy Act of 1974 (5 U.S.C. § 552a). Accordingly, use of the TPWA relies on existing DOI law enforcement Systems of Records rather than creating a new system of records specific to Clearview AI.

2. If yes, provide the SORN name and citation.

Investigative records derived from the use of Clearview AI are covered by existing DOI Systems of Records Notices, depending on how the information is incorporated into DOI systems:

- **INTERIOR/DOI-10, DOI Law Enforcement Records Management System (LE RMS)**
89 FR 1594 (January 10, 2024)
This SORN applies when Clearview AI results are incorporated into criminal investigative case files or official law enforcement records that are retrieved by personal identifier.
- **INTERIOR/BIA-18, Case Incident Reporting System**
70 FR 1264 (January 6, 2005)
This SORN applies to incident-based records that are not associated with a criminal investigation, where Clearview AI results may be referenced for situational or reporting purposes.

Clearview AI does not independently create or maintain a DOI System of Records. Records derived from its use become subject to the applicable SORN only when incorporated into DOI-authorized systems and retrieved by a personal identifier.

Section 9: Use of AI, Machine Learning, or Automated Processing

1. Does the third-party website or application employ AI, ML, or other algorithmic processing?



☒ Yes: *Describe the functionality (e.g., content recommendations, sentiment analysis, automated responses, facial recognition).*

☐ No

Yes. Clearview AI employs artificial intelligence and machine learning–based facial recognition technology. The system uses computer vision algorithms to compare an uploaded photograph against a database of publicly available images to identify visually similar faces and return corresponding internet links.

The AI/ML processing is used solely to generate potential investigative leads. Clearview AI does not make identity determinations, eligibility decisions, or enforcement decisions. All outputs are advisory in nature and require independent review and validation by trained Bureau of Indian Affairs Office of Justice Services (BIA OJS) personnel before any investigative or operational use.

2. What types of decisions or actions are influenced by AI/ML algorithms?

AI/ML algorithms within Clearview AI influence only the **generation and ranking of potential facial matches** based on visual similarity between images.

Specifically, the AI/ML processing may:

- Identify images in the Clearview AI database that visually resemble an uploaded photograph
- Rank potential matches based on similarity scores
- Provide links to publicly available source images for analyst review

AI/ML outputs do not make final determinations regarding identity, guilt, eligibility, or enforcement actions. All investigative decisions, case actions, and determinations are made exclusively by BIA OJS personnel following independent verification using authoritative sources and investigative procedures.

3. Is the agency using any AI/ML tools integrated into the TPWA, or analyzing AI-generated data?

☒ Yes

☐ No

BIA OJS personnel use the AI/ML functionality integrated into Clearview AI to review AI-generated facial recognition search results as part of authorized law enforcement investigations.

The agency does not develop, train, or modify the AI/ML models. BIA OJS personnel analyze AI-generated outputs solely as investigative leads. Any information derived from Clearview AI is subject to human review, corroboration, and validation before being documented in DOI-authorized systems or used in investigative decision-making.

4. What safeguards are in place to address fairness, transparency, and accountability in AI/ML use? Check all that apply

☐ Algorithmic bias review or fairness assessment

☐ Clear individual opt-out or redress mechanisms



- ☒ Model documentation and testing
- ☒ Human-in-the-loop validation

- ☐ Use of explainable AI (XAI) tools
- ☐ Federated learning or privacy-preserving AI

Explanation:

The following safeguards are implemented to ensure responsible use of AI/ML within Clearview AI:

- **Human-in-the-Loop Validation** - All AI-generated results are treated as investigative leads only and must be independently reviewed, corroborated, and validated by trained BIA OJS personnel before any operational or investigative action is taken.
- **Model Documentation and Awareness of Limitations** - BIA OJS relies on vendor-provided documentation regarding system functionality, known limitations, and appropriate use. Users are trained to understand the limitations of facial recognition technology, including risks of false positives and misidentification.
- **Operational Controls and Policy Restrictions** - Clearview AI use is limited to authorized personnel for lawful investigative purposes. Use is governed by DOI policy, law enforcement procedures, and privacy requirements that prohibit reliance on AI output as a sole basis for decision-making.

These safeguards promote fairness, transparency, and accountability by ensuring that AI/ML outputs do not replace human judgment and are not used in isolation.

5. Are individuals notified when AI/ML systems make decisions that affect them?

- ☐ Yes: *Describe how notice is provided and whether users can request human review.*
- ☒ No

No. Clearview AI does not make automated decisions that directly affect individuals' rights, benefits, or eligibility. The AI/ML system generates preliminary investigative leads only, and all decisions are made by human personnel following independent review and verification.

Because Clearview AI outputs are not determinative and do not result in automated actions affecting individuals, individual notification specific to AI/ML decision-making is preventing not applicable in this context.

6. What federal guidance informs the agency's use of AI/ML in this context?

DOI's use of AI/ML through Clearview AI is informed by the following federal laws, executive guidance, and frameworks:

- **Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence** - Establishes principles for responsible AI use, including human oversight, risk mitigation, and accountability.
- **OMB Memorandum M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of AI** - Provides requirements for AI governance, risk assessment, and documentation of AI use cases across federal agencies.
- **OMB Memorandum M-21-06, Guidance for Regulation of Artificial Intelligence Applications** - Informs



agency oversight and responsible deployment of AI technologies.

- **OMB Circular A-130, Managing Information as a Strategic Resource** - Establishes federal requirements for information security, privacy, and risk management applicable to AI-enabled systems.
- **NIST AI Risk Management Framework (AI RMF 1.0)** - Provides guidance for identifying, assessing, and managing risks associated with AI systems, including bias, transparency, and reliability considerations.
- **DOI Privacy Policy and AI Governance Practices** - Establish DOI-specific requirements for privacy protection, oversight, and responsible use of AI-enabled tools in mission operations.

Collectively, these regulatory bodies guarantee that the Department of the Interior's application of AI and machine learning through Clearview AI is governed by human oversight, robust privacy safeguards, and comprehensive risk management in accordance with federal standards.