AFP National Guideline on information security

View document details (metadata)Close document details (metadata)

Metadata	
Caption	Information security: ICT systems, hardware and software
Document Identifier	NAT18001
Description	This guideline directs systems users to exercise security responsibility to support the security of AFP ICT systems and hardware.
Governance Function	Security
Owned by	Manager Security
Date First Approved	22/12/2017 0:00
Contact Person	s47E(d) @afp.gov.au
Date Published	8/01/2018 0:00
Date Modified	18/9/2019
Date Last Reviewed	22/12/2017
Authorised by	Manager Security
Date of Next Review	22/12/2019
IPS publishing:	Exempt or unsuitable
IPS decision date	22/12/2017 0:00
Instrument Type	National Guideline
Replaces	NAT13055, NAT13056, NAT13057, NAT13059
Stakeholders	Technology & Innovation, Security, Professional Standards

Metadata	
Instrument Classification	UNCLASSIFIED
Dissemination Limiting Marker (DLM)	For official use only
Current SharePoint Version	8.0

1. Disclosure and compliance

This document is marked **FOR OFFICIAL USE ONLY** and is intended for internal AFP use.

Disclosing any content must comply with Commonwealth law and the AFP National Guideline on information management.

Compliance

This instrument is part of the AFP's professional standards framework. The AFP Commissioner's Order on Professional Standards (CO2) outlines the expectations for appointees to adhere to the requirements of the framework. Inappropriate departures from the provisions of this instrument may constitute a breach of AFP professional standards and be dealt with under Part V of the *Australian Federal Police Act 1979* (Cth).

2. Acronyms & definitions

Acronyms and terminologies are defined in the AFP Security Glossary of Terms.

3. Guideline authority

This guideline was issued by Manager Security using power under s. 37(1) of the *Australian Federal Police Act 1979* (Cth) as delegated by the Commissioner under s. 69C of the Act.

4. Introduction

This guideline observes obligations under the:

- Australian Government Information Security Manual
- Australian Government Protective Security Policy Framework
- AFP Commissioner's Order on Security (CO9).

This guideline outlines the obligations for system users relating to the security of AFP ICT systems.

Information security applies to all system users and AFP ICT systems. All system users must protect AFP ICT systems from unauthorised use, including disclosure, modification, manipulation and destruction.

Exception: This guideline **does not** apply to discreet or covert use. For information on discreet or covert use, refer to the AFP National Guideline for official online activities.

5. Policy

The Security portfolio is responsible for the security of all AFP ICT systems, hardware, software and removable data storage devices (RDSDs).

All controls used for the security of AFP ICT systems, ICT hardware, software, RDSDs and system access must be approved by Security.

Prior to implementation, any new business system, application or major modification to an existing business system or application must be reviewed by Security to determine if a risk assessment is required.

When using AFP ICT systems, RDSDs, ICT hardware or software, system users must:

- protect the security and integrity of the systems or item and any information stored
- only access official AFP databases, intelligence and information for the purpose of their official duties and in accordance with legislation
- only use RDSDs, ICT hardware or software for the purposes of their official duties.

System users using the AFP Secret Network (AFPSec) and AFP Top Secret Network (AFPTSN) must comply with governance and separate security documentation available on those systems.

Further information is available on request from Security.

6. Responsibilities

Deputy Commissioners and COO
The Deputy Commissioners and the COO, as appointed system risk owners for major information systems, must make decisions on the acceptance of ICT security risk for the AFP on behalf of the Commissioner.

Chief Information Security Officer (CISO)
The Manager Security (Chief Security Officer) performs this role and is responsible for the strategic direction for security across the AFP. The CISO is also responsible for ensuring the AFP is compliant with national policy, standards, regulations and legislation.

Agency Security Advisor
The Coordinator Physical Security performs this role and provides high-level authority to support the Information Technology Security Advisor in maintaining the physical security of AFP ICT systems.

Information Technology Security Advisor (ITSA)
The Coordinator Information Security performs this role and is the system certification authority. The ITSA may authorise ICT system shutdown, emergency access and access revocation.

The ITSA must advise on ICT systems security to the Security Committee through Manager Security (Chief Security Officer).

System risk owner
A system risk owner is appointed by the Deputy Commissioner Capability and is responsible for ICT security risk of major ICT systems. They are responsible for the system risk acceptance and formal accreditation approval and are the nominated information owner.

The system risk owner may grant waivers for an ICT Security compliance directive in accordance with Commonwealth security requirements.

System risk owners must:

- determine the eligibility criteria and access rights for users of their systems
- delegate authority, if required, to grant access to other system users
- inform Technology & Innovation of delegation details.

System owner
A system owner is responsible for:

- the operation of the system, ensuring it is managed effectively and securely
- delegating the day-to-day management of the system to a system manager.

The system owner is the authority on:

- ensuring the security risk owner has accepted all residual risks
- placing a system into an operational state
- approving the re-assessment of a systems, based on system changes
- terminating a system.

System manager
A system manager is appointed by the Deputy Commissioner Capability to manage, on behalf of the system risk owner, the designated ICT system on a day-to-day basis to ensure the confidentiality, integrity and availability of all information collected, processed and stored on the designated system.

System users
The action of a system user ‘logging on’ to an AFP ICT system is interpreted as their implicit agreement to comply with the AFP Security governance framework and accept personal responsibility for information security.

AFP appointees with authority to access a third party database/system must ensure they comply with all terms and conditions allocated to that database/system.

Part A – ICT system access

7. Access conditions

The identity and suitability of individuals to access official material must be confirmed before access is granted.

System users must have the following security clearance levels for the below ICT systems:

ICT System	Security Clearance	Compartment Briefings
AFP Core Systems	BASELINE	
AFPSec	NEGATIVE VETTING 1	
CABNET	NEGATIVE VETTING 1	
AFPTSN	POSITIVE VETTING	s47E(d)

For all other systems the minimum security clearance must be determined by the system risk owner.

System users must:

- have a legitimate requirement and authority to access AFP ICT systems
- only be granted access to ICT systems necessary to perform their official duties
- hold a current security clearance appropriate to the highest classification of information stored on, or accessible through, the ICT system they are authorised to use. Refer to the table above and s. 21 below.
- use their own unique logon identifier (user ID) to access an AFP ICT system and be accountable for all actions associated with their user ID
- not allow another person to use a computer account or password not assigned to them
- not attempt to obtain passwords or access computer accounts not assigned to them unless it is part of their official duties
- protect passwords according to the classification of the ICT system or device to which it allows access, refer to s. 7.4 below.

7.1 Access management

Upon meeting the requirements detailed above, access to AFP ICT systems (excluding PROMIS access by non-AFP appointees, refer to s. 7.2 below) must be approved by a system user's supervisor (coordinator or above) unless system specific arrangements are required or have already been approved.

AFP coordinators or above may approve access to personal information held by other system users.

Team leaders or above may approve access to shared resources such as network folders and email distribution lists. Where appropriate and once a supporting business case has been approved by Technology and Innovation (T&I), executive assistants or business administration officers may also approve access to shared resources.

To ensure appropriate use of AFP systems, AFP managers and coordinators should be aware of and monitor system users' information access and activities on AFP ICT systems. Supervisors must ensure system users hold appropriate security clearances and are briefed on the appropriate protective security procedures for handling information.

7.2 PROMIS access by non-AFP appointees

Access to PROMIS by a non-AFP appointee must be endorsed by an AFP manager. Where ongoing access (past 12 months) is required, the sponsoring AFP manager must confirm the ongoing requirement with the system risk owner.

Memorandums of understanding that relate to the access of AFP information systems must incorporate clauses relating to security reporting, personnel and information security requirements and must be reviewed by Security prior to finalisation.

For further information refer to the AFP National Guideline on access to PROMIS by non-AFP appointees.

7.3 Information access requirements

	Certain Sensitive and Compartmented Information[1]	TOP SECRET	SECRET	CONFIDENTIAL	PROTECTED	UNCLASSIFIED with a DISSEMINATION LIMITING MARKER	UNCLASSIFIED
Positive vetting	✓	✓	✓	✓	✓	✓	✓
Negative vetting level 2	✓	✓	✓	✓	✓	✓	✓
Negative vetting level 1	✗	✗	✓	✓	✓	✓	✓
Baseline	✗	✗	✗	✗	✓	✓	✓
Employment screening	✗	✗	✗	✗	✗	✓	✓

Supervisors must notify the system manager, by emailing T&I (ICT-Support) when a system user requires reduced or modified access permissions, including when:

- transferring to different duties
- changing the nature of duties
- on long-term leave of more than 90 days (e.g. long service, maternity or without pay)
- ending a secondment or attachment to the AFP
- ending membership of a joint task force or similar operational team
- suspended from duty
- ending AFP employment or engagement.

Accounts not used for 90 days must be suspended in accordance with T&I procedures.

7.4 Passwords

Passwords must not be written down and kept with any AFP ICT system or mobile electronic device. Where there is a requirement to physically record a password, it must be:

- stored in a sealed envelope which should, at minimum, also contain:
  - the asset number of the device
  - the names of those authorised to use the device
  - the date the password was changed.
- protectively marked to the maximum security classification of the ICT system or device to which it allows access
- handled and stored in accordance with the:
  - level of sensitivity or classification of the information the password protects
  - Access and storage requirements for information and assets
  - AFP Security Governance Framework.

Where a record is kept electronically, for systems up to and including PROTECTED, it should be kept using s47E(d) s47E(d) software, which is available on AFP core systems.

Passwords used to access AFP systems should not be used to access non-AFP systems.

System users must immediately report any password compromise or suspected password compromise to Security by submitting a security incident report or contact Security for advice. The password must be changed as soon as practicable after the incident.

8. Acceptable and prohibited use

8.1 Acceptable use

System users must only:

- use AFP ICT systems in accordance with this guideline and other AFP governance, including:
  - **the need-to-know policy** – system users must only access information needed to perform their official duties and for which they have an appropriate security clearance
  - **information release** restrictions – system users must only release information obtained from AFP ICT systems to another person in accordance with the AFP National Guideline on information management.

System users requiring access to SECRET and TOP SECRET material may be granted an authorised account for the relevant externally provided ICT system. System users must operate third party systems in accordance with the system risk owner's security requirements.

8.2 Limited personal use

Where an AFP ICT system is approved for limited personal use, system users may use it for limited personal use if they comply with all AFP requirements.

Limited personal use must:

- be in accordance with the business area policies and procedures
- not be excessive in cost, space, time or resources
- not affect the ability of AFP ICT systems to operate efficiently
- not require changes to the ICT system or negatively affect security mechanisms
- not fall outside the boundaries of acceptable use
- comply with:
    - AFP Code of Conduct
    - Better Practice Guide on Workplace Bullying and Workplace Discrimination.

8.3 Prohibited use

System users must not, without lawful excuse or authority, use AFP ICT systems:

- in a way that could adversely impact on AFP core business, operational requirements or reputation
- in a way which breaches Commonwealth policies and/or requirements
- for personal gain, including any personal business interest, unless that business interest is approved secondary employment, noting provisions for the Discussion Fora as per s. 10.5 below
- to create, access, distribute or store inappropriate information
- to access non-AFP ICT systems or data that could endanger the security of AFP ICT systems, including:
    - external web-based email (e.g. Hotmail, Yahoo Mail, Gmail)
    - instant messaging
    - seized or intercepted computer data which has not been appropriately sanitised (e.g. electronic evidence)
    - known malicious software or viruses
    - untrustworthy websites or files
    - unapproved ICT hardware
    - file sharing
    - video conferencing.

Where inappropriate material has been unintentionally accessed by legitimate searches, or the nature of material was not evident from the title or link displayed, system users must:

- immediately exit the inappropriate content
- make a file note or diary entry describing the circumstances
- notify their supervisor
- submit an integrity report in accordance with the AFP National Guideline on integrity reporting.

System users, who are required to access inappropriate material for official reasons, on AFP systems not authorised for this use or are outside of their standard duties, must log a PROMIS case note entry or diary note and advise their supervisor for each instance.

9. Internet usage

All system users accessing the internet for AFP business reasons, whether by AFP core systems or any other connection (e.g. stand-alone computers) must ensure their usage does not fall outside the boundaries of acceptable use, including:

- using, without authorisation, any discreet or covert internet connections, as per the AFP National Guideline for official online activities
- being excessive in cost, space, time or resources
- adversely affecting the efficient operation of AFP ICT systems

- on its own, requiring changes to policies or practices, or alterations to security settings
- access to inappropriate material
- compromising the AFP.

Security may block access to specific websites or website categories that may endanger the security of AFP ICT systems or impact the operational availability of AFP ICT systems. Access to a specific website within a blocked category may be authorised on application to Security by the relevant coordinator. For additional information refer to the internet browsing categories, allowed and blocked.

10. Communications

10.1 Telephones and facsimiles

Fax machines transmit information over the public telephone system and must only be used to transmit UNCLASSIFIED information.

The AFPNET telephone system (including facsimiles, mobile telephones, the teleconferencing system and the Voice over Internet Protocol system) and the public telephone system must only be used to transmit UNCLASSIFIED information.

Telephone messaging systems (SMS, MMS, voice mail, pagers and messaging applications) must only be used to transmit UNCLASSIFIED information.

AFP Secret and Top Secret networks have telephone systems that can be used for conversations up to SECRET and TOP SECRET respectively. Refer to s. 27.1 below.

System users must consider who can overhear a telephone conversation, especially in open plan environments.

Travelling with electronic devices

AFP appointees travelling overseas for official purposes must be mindful of the AFP National Guideline on mobile devices. AFP appointees travelling to a country assessed by Security as high risk should only take electronic devices that have not been used prior and will not be used upon returning to country (burn device).

AFP appointee’s should contact Security in the first instance, by submitting their signed International Travel Approval Form to Security, to confirm if a burn device is required.

Business areas are responsible for the purchase of burn devices.

For more information on travelling overseas with electronic devices, refer to the Travelling internationally with electronic devices guide and the Mobile electronic devices returning from travel FAQs.

10.2 Wireless communication devices

System users must not connect any wireless communication device to any AFP ICT system or network until approval to operate that device has been received from the system risk owner after consultation with Security.

10.3 Email

System users must treat unsolicited emails (spam) as if they contain inappropriate material and must not reply or forward:

- chain emails
- junk email
- games
- non-work related advertising.

System users must:

- not use **personal email accounts** to send or receive official information obtained in the performance of their AFP duties
- comply with the information security articles and FAQs on security classifications of email allowed to organisations**.** Adding an external email address to AFP mailing lists is at the discretion of the mailing list owner.
- only send information (including attachments) classified:
    - FOR OFFICIAL USE ONLY or above to recipients authorised to receive information of that classification.
    - SECRET or TOP SECRET from the AFP Secret or Top Secret networks respectively.
    - Sensitive: Cabinet via CABNET.
- only **automatically forward emails** if it is:
    - appropriate to do so (e.g. the recipient has a 'need to know')
    - restricted to an AFP email address.
- limit **out-of-office email notification** to respond to internal recipients only, as these notifications also respond to spam
- not add AFP email addresses to **external mailing lists** of non-government organisations unless it is required for official purposes, such as registering for a conference
- not use AFP core system passwords when using an AFP email address to register online for official purposes.

System users who are contractors must list their position in the signature block of their AFP email as contractor.

10.4. Social networking

System users:

- should not identify their employment with the AFP in unofficial online social networking (this includes the use of AFP logos and insignia)
- should act responsibly and mitigate risks to their safety
- must not:
    - establish a personal account with an AFP email address
    - compromise the AFP's security, reputation or operational effectiveness
    - use AFP logos or insignia for private purposes
    - breach s. 60A of the *Australian Federal Police Act 1979* (Cth).

System users and their supervisors must ensure:

- the use of social networking via personal devices whilst on duty is reasonable as per s. 8.2 above
- their usage of social networking sites on AFP ICT systems does not fall outside the boundaries of acceptable use, in accordance with s. 8.1 above.

Any use of AFP logos and insignia must be in accordance with the AFP National Guideline on intellectual property, commercialisation, logos and insignia.

For further information refer to the AFP National Guideline on social media (drafting) or contact the Social Media team.

10.5. Discussion Fora use

System users may use the AFP Discussion Fora for general internal interactive discussion on matters of broad interest or relevance. The AFP Discussion Fora facilities must only be used for AFP-related or AFP-approved purposes, including:

- AFP business

- professional, competency and organisational development and technical literacy
- AFP-sanctioned social activities
- activities which benefit or support charitable work or the AFP's role or presence within the community
- other non-official information relevant to the interests and support of the AFP and AFP personnel within the work environment
- the reasonable sale of personal items (via the Employee Forum) that complies with all other AFP governance requirements and does not include commercial sales (e.g. multi-level marketing or connection to a business interest)
- advertising approved secondary employment business, goods and services (via the Blue Pages).

The use of AFP Discussion Fora facilities must be consistent with the AFP Core Values, as per the AFP Commissioner's Order on Professional Standards (CO2).

Reasonable sale of personal items refers to advertising a moderate quantity of items belonging to a system user that a sensible person would:

- not find to be extreme or excessive
- not associate with a conflict of interest
- find in keeping with relevant governance on using information and communications technology, and does not detract from the system user's AFP duties.

Classified information must not be posted on the AFP Discussion Fora.

The AFP reserves the right to moderate any material posted on the Discussion Fora.

The Commissioner or their delegate, as per AFP Commissioners Order on security (CO9) may authorise the removal of any posting it considers inappropriate or out of date.

11. Printer security

System users must:

- not leave sensitive or protectively marked information on printers
- ensure unmanaged printers with wired or wireless connections (including Wi-Fi and Bluetooth) are not connected to any AFP equipment
- ensure all expired printer cartridges and consumables are sanitised prior to disposal
- sanitise printer cartridges and consumables that are relocating to a less secure area.

For information on sanitisation, refer to the How to Sanitise AFPNet Printer.

Secret systems installed outside of a Zone 5 area must not have printers connected, unless authorised in writing by Manager Security (Chief Security Officer) on advice from the Information Technology Security Advisor. In these instances, business areas must establish ongoing and effective procedures for the accountability of each printed document in accordance with Attachment 3 – Classified documents accountability.

System users printing from the AFP Secret Network and AFP Top Secret Network must comply with governance and separate security documentation, available on the systems or from Security.

12. Software

System users must maintain the confidentiality, integrity and copyright of software, whether it has been developed by the AFP or purchased commercially.

System users must not download any software from the internet. **Exceptions** to this include:

- for discreet or covert use; however, all downloads must be done from a reliable source
- applications downloaded from a reliable source to AFP-approved mobile phone or tablet computers.

To purchase software system users must contact the Technology & Innovation portfolio in accordance with the AFP National Guideline on procurement and contracting.

Overt system users who have an approved business requirement to have software downloaded must submit a request to Technology & Innovation (via ICT-Support) with the location of the file and a description of the business requirement. Failure to do so may result in the software not functioning on AFP ICT systems.

For further information contact Security.

13. Removable data storage devices and ICT hardware

Privately owned or unapproved ICT hardware must not be:

- connected to any AFP ICT system or network
- used to process or store official or classified information.

System users must purchase approved RDSDs and all overt ICT hardware through the Technology & Innovation portfolio in accordance with the AFP National Guideline on procurement and contracting.

All leased official hardware that can store information must include provisions to sanitise or destroy the data at the end of its lease. Further information is available on request from Security.

For information regarding the procurement of ICT hardware for discreet or covert use, refer to the AFP National Guideline for official online activities.

Information regarding approved RDSDs is available at the Removal data storage devices FAQs.

13.1. Handling and storage

All overt ICT hardware must be registered, issued, receipted, disposed of and accounted for in accordance with AFP asset management guidance.

System users must:

- when storing official information on an RDSD, only use an approved RDSD
- ensure RDSDs and ICT hardware used for the processing or storage of classified information are:
  - not shared with, or loaned to, anyone who does not have the necessary need-to-know and the required security clearance
  - appropriately sanitised (if previously used), as per s. 23.5 below, before transferring information to another organisation, area or individual.
- ensure approval is granted, and an audit trail recorded, before moving information outside the AFP's secure or authorised work area in accordance with the AFP National Guideline on information management
- be appointed by the system risk owner as an authorised user in order to download data from AFP core systems to CDs or DVDs (downloading data permissions must be administered by the AFP Technology & Innovation function)
- minimise the risk of compromise to information by deleting information on RDSDs when it is no longer required
- ensure the safe custody of any RDSD or ICT hardware under their control until it is formally transferred to another system user or returned to the issuing authority
- ensure passwords and/or security authenticators are kept separate from the respective ICT hardware
- comply with separate specific requirements regarding the use of RDSDs and the removal of information on secret and top secret systems.

For information on the management and control of ICT hardware used for the purposes of covert or discreet activities, refer to the AFP National Guideline for official online activities.

14. Mobile computing

System users must:

- only use AFP issued, owned and configured devices for mobile computing
- only connect remotely to AFP core systems per s. 14.1 below
- only store information classified up to and including PROTECTED on an approved AFP portable device
- not store CABINET or Security-Caveated material, or information classified CONFIDENTIAL or SECRET on a mobile device unless approved by the Manager Security (Chief Security Officer)
- not store TOP SECRET information on a mobile device.

System users using mobile computing devices must only use RDSDs that are approved for the storage of information. These devices must be equipped with approved security controls.

14.1 Remote access

System users must only access ICT systems remotely if:

- it is necessary for system user to perform their duties
- it is via AFP owned, configured and approved ICT systems
- the connections are secured per security controls certified by the ITSA
- there is a two-factor authentication process available
- tokens (hard or soft) are allocated
- through a method risk assessed and approved by Security (i.e. using SatinLOW).

To obtain privileged or remote access to the AFP Secret Network or AFP Top Secret Network systems, system users must receive approval from the network owning agency.

15. Monitoring AFP ICT systems

System users must be aware that the AFP reserves the right to audit and remove any unauthorised material from its ICT systems without notice.

All system users' access to, and activities on, AFP ICT systems are continuously monitored and recorded by Security and Technology & Innovation to:

- ensure compliance with this and other governance
- ensure the integrity of information contained within AFP's ICT systems is maintained
- investigate conduct that may be illegal or adversely affect the AFP or its appointees
- detect inappropriate or excessive personal use
- monitor security.

Use of AFP ICT systems is monitored through an individual's unique logon identifier (User ID) and access rights governed by a password personal to that user.

Requests for audits of ICT systems must be approved by a coordinator or above, or team leader for Professional Standards or Security, and forwarded to Security.

Part B – Security of ICT systems and access

16. Accreditation of AFP ICT systems

All AFP ICT systems must be security assessed and accredited by the AFP's accreditation authority, as per the AFP Commissioner's Order on Security (CO9) and the AFP ICT System Accreditation Plan.

Externally provided ICT systems deployed within the AFP are subject to security assessment and possible accreditation as national security systems.

17. Audit of AFP ICT systems

All AFP ICT systems must have an audit capability to meet the AFP's security requirements.

Prior to the development or implementation of any new AFP ICT system, consultation must take place with Security to ensure the provision of compliant system security monitoring, audit logging and related tools to enable the effective monitoring and reporting of AFP system activities.

Where new ICT systems are unable to be audited by existing security tools, the provision of a suitable audit and monitoring capability must be included in consultation with Security.

Where applicable, all existing AFP ICT systems must perform the level of audit logging and security monitoring as per the Security ICT system audit plan. Where proprietary systems, devices or tools exist to enable the monitoring of these systems, provision for access to these logs must be made available to Security.

System and application security and audit logs should clearly identify which platform, system or application the logs are associated with, particularly in the case of an ICT system having multiple environment instances. All audit logs must be protected in accordance with AFP security standards. Further information is available on request from Security.

18. Data retention

Data on ICT systems must be retained online in accordance with the system risk owner requirements for availability and accessibility of data. Data retention requirements are also subject to the *Archives Act 1983* (Cth).

19. Monitoring AFP ICT systems

All activities on AFP ICT systems must be monitored by Security and Technology & Innovation.

All AFP ICT system access grants, modifications and revocations must be recorded (logged) by the Technology & Innovation portfolio for auditing and denial purposes.

20. Access Conditions

20.1 Shared, service and test accounts

Shared, service and test account usage must:

- for shared accounts, be approved by the area coordinator or above and all approval records kept for auditing
- for service and test accounts, be approved by a Technology and Innovation (T&I) coordinator or above and all approval records kept for auditing
- be listed in an auditable format/ICT system and reviewed every 6 months by a member of T&I at the level of coordinator or above
- have an appointed owner to be accountable for actions
- use account names that conform to naming standards so they are easily identifiable
- use passwords as per existing policy, except that:
    - shared test accounts may have a password expiry of up to 6 months
    - service account passwords must be reset every 6 months or when an individual who has privileged access is no longer an authorised user of the shared account.

Shared test accounts must not be:

- used if an individual test account is available
- able to access both production data and test data.

Where shared accounts are required for shared equipment used in meeting rooms, these accounts must not have access to AFP core systems classified information resources, including shared drives, SPOKES, PROMIS and email.

20.2 Privileged access

Privileged access must only be provided to AFP appointees who have both an:

- approved business need to maintain AFP ICT systems
- appropriate security clearance.

Privileged access to T&I managed systems must only be authorised by a T&I coordinator or above. Authorisation must be recorded within a system which allows subsequent auditing.

Privileged access to any ICT system not managed by the T&I portfolio must only be authorised by the system manager or their delegate. Authorisation must be recorded within a system which allows subsequent auditing.

Privileged access accounts must not be used:

- remotely where a two-factor authentication process is not available
- as a primary or daily logon account
- as an automated method to bypass security controls without the approval of the Information Technology Security Advisor (ITSA)
- to access internet sites
- to download/upload files from the internet without the approval of the ITSA
- to send or receive emails externally without the approval of the ITSA.

21. Security classification of AFP ICT systems

All AFP ICT systems are classified by the system risk owner according to the highest level of classified data processed on the system.

Information must only be processed, stored or transmitted on ICT systems that are approved for its security classification. Refer to the below table:

ICT System	Highest Classification Allowed	Other Restrictions
AFP Core Systems	PROTECTED	No security caveats (unless in draft format) No cabinet-related material (unless in draft format)
AFPSec	SECRET	No cabinet-related material
CABNET*	SECRET Sensitive: Cabinet	
AFPTSN	TOP SECRET	No cabinet-related material

*** Note:** In accordance with the Australian Government Cabinet Guideline information classified with the DLM of Sensitive: Cabinet must hold a minimum classification of PROTECTED and **must only be held on a Cabinet system**.

Prior to endorsing applications for system access by system users, supervisors must consider the access conditions and enforce the required security clearance levels, per s. 7 above.

22. Support of ICT systems

The system manager must ensure suitable security controls are implemented for all ICT systems under their control. These controls include:

- physical security
- restricted system access by administrators and system users
- secure transfer of information.

All ICT systems, including cloud based/external provider must be held within accredited facilities, as per the PSPF – Australian Government Physical Security Management Protocol and supporting guidelines:

ICT System	Accredited Zone
AFP Core Systems	Zone 3
AFPSec	Zone 4
CABNET*	Zone 4
AFPTSN	SCIF

The system risk owner must:

- ensure ICT systems are certified by the appropriate authority (contact AFP Security for assistance)
- not establish standalone systems to process or store information classified SECRET or TOP SECRET without written authorisation from the ITSA
- ensure unmanaged ICT systems are not held in a Zone 5 area or SCIF without the approval of the ITSA.

Any exemptions for security controls must be discussed with Security and if necessary approval obtained from the system risk owner.

22.1. Cloud services

The AFP must, where it is fit for purpose, adopt cloud-based services that provide adequate protection of data and delivers value for money.

Prior to any acquisitions or integration of a cloud-based service, business areas must submit a completed security risk assessment to T&I (via ICT-Support).

Cloud-based services must be in accordance with:

- Australian Government Cloud Computing Policy
- Australian Government Information Security Manual (ISM)
- Australian Government Protective Security Policy Framework (PSPF)
- Australian Privacy Principles (Privacy Act).

22.2 Connecting external systems to AFP systems

System users must not allow any external or foreign ICT system to be connected to AFP ICT systems without obtaining prior approval from Security.

22.3. Hacking or searching information security mechanisms

System users must not search security mechanisms of ICT systems (including external websites) without lawful authority.

System users with lawful authority must only probe security mechanisms using ICT systems approved to do so.

System users must not probe security mechanisms of AFP ICT systems without written approval from all of the following:

- ITSA
- system risk owner
- system manager.

22.4 Screen locks

All AFP ICT system access terminals (desktops/laptops) must have automatic screen and session locks enabled.

Where a requirement exists to have an account without a screen lock, it must be configured in accordance with the ‘Shared, service and test accounts’ requirements, as per s. 20.1 above.

23. Security of RDSDs, ICT hardware and software

All controls used for the security of ICT hardware and RDSDs must be approved by Security.

ICT security hardware and software must be assessed by Security prior to their use within the AFP ICT environment.

All RDSDs and ICT hardware containing storage media which has been used to store or process information must only be transferred, exchanged or disposed of in accordance with this section.

23.1 Purchasing ICT security hardware and software

All overt ICT hardware or software to be used within the AFP to provide security functionality must be approved by Security prior to being purchased.

For information regarding the procurement of ICT hardware for discreet or covert use, refer to the AFP National Guideline for official online activities.

23.2 Repair and maintenance

ICT hardware used for processing classified data must always be inspected and/or repaired by a suitably cleared T&I AFP appointee, service agent or supervised un-cleared service agent.

Service agents must be supervised at all times by an appropriately cleared T&I AFP appointee while working on ICT hardware.

System users removing ICT hardware from AFP controlled premises for maintenance or repair must ensure all media is removed or appropriately sanitised prior.

Where it is impracticable to remove or sanitise the media from ICT hardware, system users must seek advice from Security and undertake any actions recommended in accordance with that advice, prior to removing the hardware from AFP premises.

23.3 Removal from AFP premises

ICT security hardware and ICT hardware must not be removed from AFP premises without written approval from the respective coordinator or above.

Note: Approval is not required for the removal of AFP approved and issued mobile computing devices and portable ICT equipment from AFP premises.

Where there is a requirement to process or have access to information outside of AFP controlled facilities, system users must only use AFP owned and managed ICT hardware, unless approved by Security.

System users authorised to remove ICT security hardware or ICT hardware from AFP premises must:

- ensure the appropriate level of physical protection of the hardware at all times whilst outside AFP premises
- comply with the:

- AFP National Guideline on information management
- Attachment 2 – Transferring and transporting classified information
- Australian Government Protective Security Policy Framework
- Australian Government Information Security Manual.

23.4 Transfer

Before re-allocation or transfer of RDSDs or ICT hardware to another system user, workgroup or team, any media containing information classified up to and including PROTECTED must be sanitised by a method approved by Security.

Any media containing, or which previously contained, information classified CONFIDENTIAL or above, must:

- not be transferred
- be destroyed by a method approved by Security.

23.5 Sanitisation

To remove all information from RDSDs or unserviceable storage devices system users must follow the approved sanitisation procedures.

For information on sanitising, refer to the media sanitisation section of the Information Security Manual.

Where RDSDs cannot be sanitised or when there is no requirement to keep them, system users must contact T&I (ICT-Support) to arrange sanitisation and/or destruction of the equipment.

23.6 Disposal/part exchange

ICT hardware used for processing information classified up to and including PROTECTED must not be offered for disposal or part exchange outside the AFP unless the hard disks or storage media have been either:

- replaced
- securely sanitised or destroyed by a method approved by Security.

ICT hardware used for processing information classified as CONFIDENTIAL, SECRET or TOP SECRET must not be offered for disposal or part exchange outside the AFP unless the hard disks have been either:

- replaced
- securely destroyed by a method approved by Security.

Part C - Zone 5 areas and SCIFs

24. Access to ICT systems in a Zone 5 area or SCIF

24.1 New user accounts

When a new user account for a Top Secret ICT system is required, the following procedure applies:

- An AFPTSN application form, available via AFP Corporate Forms and Templates (Part 1), and from local vaults (Part 2) must be completed and supplied to T&I (ICT-Support), along with a copy of an iAspire TSE completion certificate.
- The ICT system administrator must ensure all details are correct prior to forwarding Part 2 of the request forms to the host agency for account creation.
- The relevant Top Secret Control Officer (TSCO) should provide the user with:
    - all relevant security documentation
    - a verbal brief outlining the user's responsibilities.

24.2 Account closure

When a user account is no longer required, the following procedure applies:

- the user must notify their TSCO and the Communications Security Officer (COMSO) of the date and reason to close the account
- the TSCO must notify the system administrator to suspend the account
- COMSO must:
    - administer compartment debriefings as required
    - notify the system administrator to finalise the user's account form.
- the system administrator must close the account and retain all parts of the account for auditing purposes.

25. ICT Equipment

25.1 Information communications and technology (ICT) equipment

All ICT equipment other than AFP approved laptops and mobile devices must be held within accredited facilities, as per the PSPF – Australian Government Physical Security Management Protocol and supporting guidelines.

25.2 Repairs to ICT equipment

AFP ICT equipment classified SECRET (located in a Zone 5 area or SCIF) or TOP SECRET (located in a SCIF) must only be installed, repaired or configured by appropriately qualified, authorised and security cleared AFP appointees.

AFP ICT equipment classified up to PROTECTED and located in a Zone 5 area or SCIF may be repaired or configured by T&I personnel who:

- possess a Negative Vetting 1 security clearance
- remain under the supervision of an appropriately cleared and briefed AFP appointee of the area or the TSCO.

For visitor control procedures, refer to the National Guideline on physical security (drafting).

The installation, repair and configuration of third party ICT equipment (not AFP Secret Network or AFP Top Secret Network systems) located in a Zone 5 area or SCIF must comply with the owning agency's System Security Plan requirements which are provided at the time of installation by the owning agency (can be obtained from Security).

26. Information Management

AFP managers must adequately provide for the protection of classified material in security plans relating to their activities. All information held by the AFP must be:

- classified in accordance with the Better Practice Guide on applying protective marking and the Business Impact Levels
- stored in accordance with the access and storage requirements for information and assets
- transferred and transported in accordance with Attachment 2 of this guideline
- recorded in a classified documents register (refer to Attachment 3 –classified document accountability) where classed as accountable material
- managed in accordance with the AFP National Guideline on information management
- for registry files, accurately recorded in PROMIS and returned to the Records Management Unit when no longer required. AFP appointees transferring areas must ensure the files are transferred correctly and PROMIS updated to reflect the new file holder.

Sensitive compartmented information (SCI) must only be stored, handled, discussed and/or processed (electronic or otherwise) in a facility accredited by the Australian Signals Directorate Defence Intelligence Security to be a SCIF.

Information classified TOP SECRET must be processed electronically in a SCIF, but may be stored, handled and discussed in a Zone 5.

26.1 Classified documents accountability

Classified Documents Registers (CDRs) must be used to record the receipt, storage, physical transmission, disposal and destruction of all accountable material.

Where a business area handles documents of different classifications, a separate CDR must be maintained for Sensitive: Cabinet, TOP SECRET and codeword documents. Documents marked with security caveats do not require a separate CDR.

While it is not a requirement, information classified PROTECTED may be recorded in a CDR to maintain strict control over the classified material.

26.2 CDR responsibilities

CDR supervising member (CDRSM)

Line managers responsible for business areas that handle accountable material must appoint a CDRSM(s).

Prior to being appointed as a CDRSM, individuals must:

- be an AFP appointee
- hold a current AFP security clearance (without restrictions) to the level of the documents being handled
- have received training from the COMSO in the maintenance of a CDR
- demonstrate a high order understanding and commitment to safeguard and account for the material held.

The CDRSM for TOP SECRET and codeword documents should be the relevant Top Secret Control Officer. The CDRSM of a Zone 5 area or a SCIF must conduct a monthly audit of a progressive 10% sample of the complete CDR document holdings.

The CDRSM must be recorded on the opening page of the CDR.

CDR maintaining member (CDRMM)

All AFP appointees who notate classified documents in their area's CDRs are the CDRMMs and must be recorded on the opening page of the CDR.

CDRMMs are responsible for:

- recording documents within the CDR and the daily maintenance of the register
- ensuring safe-hand receipts for transmitted documents are returned, as per Attachment 3 of this guideline
- notifying Security of lost documents by submitting a security incident report.

CDRMMs must:

- properly receipt, account for and record the disposal, transfer or removal of each separate copy of the item, by use of a CDR
- only use the AFP approved form of CDR (AFP Form 819), which can be obtained from the Communications Security Team (no electronic CDR form is endorsed for use in AFP)
- appropriately classify a CDR – CDRs must be classified on their content, not on the documents they record. If care is taken not to identify nationally classified material in the document title, it should rarely be necessary to classify the register above FOR OFFICIAL USE ONLY
- store CDRs separately from the material it records and also in accordance with the requirements for its own classification
- use, transfer, retain, archive, close and dispose of a CDR in accordance with Attachment 3 of this guideline.

Communications Intelligence Security Officer (COMSO)

The COMSO must:

- manage the issue of all CDRs
- maintain a master record of all open and closed registers
- annually conduct a 100% audit of CDRs (calendar year).

For the appropriate use and management of a CDR see Attachment 3 of this guideline.

26.3 Sensitive compartmented information

Sensitive compartmented information (SCI) must only be stored, handled, discussed and/or processed (electronic or otherwise) in a facility accredited by the Australian Signals Directorate Defence Intelligence Security to be a SCIF. SCIFs comprise those facilities listed at access and storage requirements for information and assets.

AFP appointees must not be provided with access to SCI unless:

- the position they occupy is listed on the AFP designated security assessment position register and they have a need to know
- they have received the appropriate compartment brief from the relevant agency, as below
- they have signed the corresponding briefing acknowledgement forms
- the information is received within a SCIF
- they have undertaken a SCIF familiarisation tour conducted by the relevant Top Secret Control Officer or the COMSO.

Compartment briefs

Supervisors of AFP personnel requiring compartment briefs must arrange the briefings through the Communications Intelligence Security Officer (COMSO). AFP personnel must not directly approach external agencies to arrange their own briefings.

When access to a compartment is no longer required, AFP appointees must arrange for the COMSO to formally debrief them. AFP appointees who supervise or otherwise work with other AFP personnel must ensure those AFP personnel who no longer require access to a compartment are formally debriefed by the COMSO.

26.4 Communications intelligence material

AFP appointees who handle communications intelligence (COMINT) material must ensure that:

- they comply with:
    - the AFP National Guideline on information management
    - all COMINT security instructions held in the Australian Signals Intelligence Security Regulations and Orders (ASSROs). A copy can be found on the Australian Intelligence Community Network (AICNet).
- they have been given the necessary briefings
- records are maintained for the handling, printing, movement and destruction of all COMINT material within the AFP via the appropriate classified documents register
- the printing of material is strictly controlled and all copies must be:
    - accounted for in a CDR
    - destroyed (using an 'A' Class Shredder) after 14 days. If material is required for a longer period, approval must be sought from the originating author, business unit or agency.
- they do not reproduce COMINT material unless approved by the originating author, business unit or agency

- any compromise or suspected compromise of COMINT material must be reported immediately to the COMSO and a security incident report sent to Security as soon as practicable after the incident or suspicion
- all records are available for audit by the COMSO at any time.

AFP appointees who supervise or otherwise work with other AFP personnel who handle COMINT material must ensure that those AFP personnel comply with the COMINT material requirements as detailed above.

Any compromise or suspected compromise of COMINT material must be reported by the COMSO to the Department of Defence.

26.5 Transmission of classified material

Codeword material and information classified TOP SECRET must:

- never be stored or transmitted on standalone computers or networks other than the AFP Top Secret Network (AFPTSN)
- be stored within a SCIF in accordance with the access and storage requirements for information and assets
- not be removed from a SCIF or AFP premises unless:
    - the material is stored in a Security Construction and Equipment Committee endorsed container in accordance with the access and storage requirements for information and assets
    - written approval for the movement is received from the originating author, agency or business unit
    - the Top Secret Control Officer has approved the movement
    - movement is recorded in the relevant CDR
    - the classified information is managed in accordance with the AFP Information handling guides, and safely transfer in accordance with Attachment 2 of this guideline.

26.6 Waste management

Regardless of its protective marking, any document no longer required within a Zone 5 area or SCIF must be shredded using an approved Class A shredder. The destruction must be:

- conducted by two AFP appointees who hold the necessary security clearance and briefings
- notated in the relevant CDR as destroyed (the destruction member and witness must sign the register)
- in accordance with this guideline and the AFP National Guideline on information management.

All printer cartridges must be sanitised prior to removing them from the machine in accordance with the procedures detailed in the information handling guides and the Australian Government Information Security Manual. Sanitised cartridges must be provided to the COMSO for destruction.

General waste must be kept in bins separate to those used for classified documents.

27. Communications security risk management

27.1 Phone and multifunction devices

The AFP deploys a suite of secure phone, fax and multifunction devices inside Zone 4, Zone 5 and locally designated sensitive areas. These communication systems provide secure communications within the AFP and with external agencies.

When communicating classified material via telephone, AFP appointees must use the appropriate phone systems as listed in the table below:

Phone system	Classification
Avaya VoIP phones	UNCLASSIFIED
AFPSec VoIP	up to and including SECRET

AFPTSN VoIP	up to and including TOP SECRET

AFP appointees who supervise or otherwise work with other AFP personnel must ensure those AFP personnel use the appropriate phone systems as listed in the table above when communicating classified material.

Handsets with ‘push to talk’ switches installed must not be modified or otherwise tampered with which would render the capability ineffective.

In all areas where SECRET ICT systems are located and fitted with VoIP phones, mobile phones and other VoIP systems of lower classifications may be used if appropriate standard operating procedures to prevent data spills exist and are adhered to.

27.2 Infrared data association communication devices

All infrared data association devices, such as remote control handsets, which form part of the operational fixtures of a Zone 5 area or SCIF, must only be installed after both:

- certification by technical surveillance counter measures
- receipt of a written security waiver from the Manager Security (Chief Security Officer).

27.3 Controlled cryptographic (encryption) items

All controlled cryptographic items are the responsibility of the Security portfolio and must only be purchased and maintained by Security in accordance with Australian Signals Directorate (ASD) guidelines.

To protect against interception and/or unauthorised reading of misrouted data, system users must only use ASD approved encryption devices when using AFP voice and data communication devices to transmit information classified CONFIDENTIAL or above.

For information on ASD approved devices contact Security.

27.4 Cryptographic systems/equipment

Cryptographic (encryption) software or devices must not be installed on, or connected to, AFP ICT systems unless the installation is approved and coordinated by Security.

Unless specifically authorised by Security, system users must not install encryption software products (freeware, shareware or commercial) on any AFP ICT system.

Encryption devices and cryptographic key material must be managed by Security in accordance with Australian Communications-Electronic Security Instructions.

System users must afford cryptographic key material and associated equipment the level of physical protection commensurate with its security classification in accordance with instructions from Security.

Should an encryption device fail, where a backup link does not exist, system users must suspend the communication link pending the installation of a replacement device, unless otherwise authorised by the system risk owner after consultation with Security.

28. Security incidents

Any breaches of this guideline must be reported to AFP Security via a security incident report form.

In addition to breaching the professional standards of the AFP, inappropriate departures from the provisions of this instrument may also constitute a breach of AFP’s security and be dealt with under the security incident management practices, as per the AFP Commissioner’s Order on Security (CO9).

To enable the Manager Security (Chief Security Officer) to notify system risk owners of any data spill, security incidents involving AFP and third party ICT systems must be notified in accordance with security reporting requirements, refer to Part C of the AFP National Guideline on personnel security. Failure to comply with system security requirements may result in either the temporary suspension or permanent withdrawal of services by the system risk owner.

Note: the cost of data spills may be passed back to the business unit responsible. To limit the cost incurred to the business area the incident must be reported to Security as soon as practicable after the incident occurs.

29. Further advice

Queries about the content of this document should be referred to Security Reporting & Referrals.

30. Resources

Legislation

- *Archives Act 1983* (Cth)
- *Australian Federal Police Act 1979* (Cth)
- *Privacy Act 1988* (Cth) (including the Australian Privacy Principles).

AFP governance instruments

- AFP Commissioner's Order on Professional Standards (CO2)
- AFP Commissioner's Order on Security (CO9)
- AFP National Guideline for official online activities
- AFP National Guideline on access to PROMIS by non-AFP appointees
- AFP National Guideline on Complaint Management
- AFP National Guideline on information management
- AFP National Guideline on intellectual property, commercialisation, logos and insignia
- AFP National Guideline on integrity reporting
- AFP National Guideline on mobile devices
- AFP National Guideline on personnel security
- AFP National Guideline on physical security
- AFP National Guideline on procurement and contracting
- AFP National Guideline on social media (drafting)
- Better Practice Guide on applying protective marking
- Better Practice Guide on Workplace Bullying and Workplace Discrimination.

Other sources

- Access and storage requirements for information and assets
- AFP asset management guidance
- AFP Corporate Forms and Templates
- AFP Discussion Fora
- AFP Information handling guides
- AFP Security Governance Framework
- AFP Security Glossary of Terms
- AFP System risk owners
- Australian Communications-Electronic Security Instructions (Security)
- Australian Government Business Impact Levels
- Australian Government Cabinet Guideline
- Australian Government Cloud Computing Policy
- Australian Government Information Security Manual
- Australian Government Protective Security Policy Framework
- How to Sanitise AFPNet Printer
- Information handling guides
- International Travel Approval Form
- Internet Browsing Categories, allowed and blocked

- Mobile electronic devices returning from travel FAQs
- Protective Security Policy Framework (PSPF): Security zones and risk mitigation control measures
- PSPF – Australian Government Physical Security Management Protocol
- Removable data storage devices FAQ
- Security classifications of email allowed to organisations
- Security ICT system audit plan (Information Security)
- Security incident report
- Travelling internationally with electronic devices guide
- Documentation which can be obtained from the Communications Intelligence Security Officer:

    - Australian Signals Directorate (ASD) guidelines (Security).
    - ASIO Technical Note
    - ASIO Protective Security Circulars
    - Australian Signals Intelligence Security Regulations and Orders (ASSROs) – can be obtained from the Australian Intelligence Community Network (AICNet)
    - Department of Foreign Affairs and Trade Special Security Orders and Standing Instructions.

31. Attachments

Attachment 1 – Prohibited items

The items listed in the table below are prohibited from:

- audio secure rooms
- locally designated sensitive areas
- Sensitive Compartmented Information Facilities (SCIF)
- speech privacy rooms
- Zone 5 areas.

ITEM	DESCRIPTION
1	Mobile device
2	iPad/iPod
3	Device with Bluetooth or GPS connectivity
4	Camera or Film
5	Memory stick or card
6	Recording device
7	Activity fitness tracker
8	Smart watch
9	Bag, Briefcase or Document Holder

Attachment 2 – Transferring and transporting classified information

Attachment 2 – Transferring and transporting classified information

Attachment 3 – Classified documents accountability

1. Classified Document Register entries

Where multiple copies of the same document are received or made, each individual copy of the document requires registration as a separate entry in a Classified Document Register (CDR).

All CDR working entries must be made in black or blue (non-erasable) ink with the exception of:

- temporary disposal entries, which may be made in pencil
- deletions, which must be made in red (non-erasable) ink
- entry dates as detailed below.

Entries may be abbreviated to enable more detailed information to be recorded.

Date of entries

For each new day, the date the entries are made in the CDR must be written in red on the next available blank line which is not serial numbered.

Documents must be entered in the CDR as soon as they have been received or printed and prior to their distribution or removal from AFP facilities.

Covering letters

Where a document is accompanied by a covering letter of a classification not requiring registration, care should be taken to ensure the parent document is marked as being registered; not the covering letter.

Where more than one document of a classification requiring registration is sent under the same covering letter, each separate document must be registered.

Receipt details

RECEIPT OR ORIGIN DETAIL							
Serial No. (a)	Type of Document (b)	Sender or Originator (c)	Reference Number (d)	Date of Origin (e)	Title (or Subject) (f)	Classification (g)	Copy Number (h)

Table 1 - CDR receipt page

The CDR receipt page reproduced at Table 1 must be completed as follows:

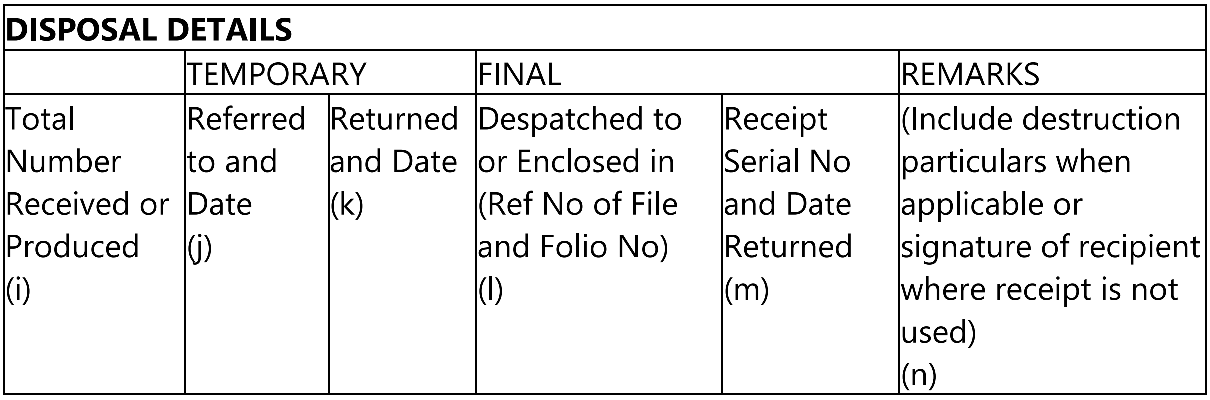
- Allocated serial numbers in column (a) must be marked on the respective document as part of the registration process. Serial numbers must be sequential from the first CDR entry on the first page to the last CDR entry on the last page.
- Document types in (b) should stipulate whether it is a letter, intelligence report, photograph, compact disc, etc.
- Entries in columns (a) to (i) (refer to Tables 1 above and 2 below) must be completed immediately after documents are received or printed from an ICT system.
- Every copy of each document must be recorded as separate entries so that subsequent disposal can be clearly tracked.
- in column (g) abbreviations for protective markings are sufficient.
- where documents are copy numbered (h), the number must be recorded as ‘copy # of #’; otherwise place a hyphen in this column.

When classified documents are received in envelopes marked ‘Personal for…’, ‘Exclusive for…’ or as ‘Eyes only’ for a person or nominated position, the CDR maintaining member (CDRMM) must deliver by hand or safehand the unopened envelope to the intended recipient. On delivery, the addressee must be asked to:

- inspect the package to ensure it has not been tampered with or otherwise compromised
- open the item and ensure the CDRMM is appropriately cleared and briefed to handle the document
- pass the contents to the CDRMM (if appropriately cleared) or to another appropriately cleared person for registration and filing.

Once registered and filed, the documents must be referred back to the intended recipient for any other action required.

Disposal details



DISPOSAL DETAILS					
	TEMPORARY		FINAL		REMARKS
Total Number Received or Produced (i)	Referred to and Date (j)	Returned and Date (k)	Despatched to or Enclosed in (Ref No of File and Folio No) (l)	Receipt Serial No and Date Returned (m)	(Include destruction particulars when applicable or signature of recipient where receipt is not used) (n)

Table 2 - CDR disposal page

The CDR disposal page reproduced at Table 2 must be completed as follows:

- where more than one copy of a document is either produced or received, indicate in column (i) how many (e.g. where 3 copies of a document are received or produced, the number '3' must be placed in column (i) for each of the 3 required entries)
- the CDRMM must check columns (j) and (k) to ensure that documents are not on temporary disposal for more than 48 hours and that when complete, the entry is closed and final disposal completed
- final disposal for all entries to a file (show folio number) is shown in column (l)
- final disposal for all entries to an addressee is shown in column (m)
- entries for documents that have been retained locally remain open and are accountable until they are closed by destruction or further disposal of the related document or material
- entries relating to the receipt of amendments should be endorsed in column (n) as 'incorporated into CDR serial.......', then deleted by red entry
- column (m) must be completed immediately after the receipt form is returned for incoming items or raised for outgoing items
- column (n) must contain all detail of a document's destruction, including the full details of any witnesses to the destruction. Other comments applicable to the chain of custody of the document should also be entered
- where a recipient signs for a document in the CDR, their AFP number (or other relevant identification number), name, date and signature must be recorded in column (n).

Safe-hand receipt forms

All CDR-related receipt forms must be returned:

- within Australia: within 14 days of the date of receipt
- overseas: within 30 days of the date of receipt.

CDRMMs must actively monitor the return of receipts. Where documents have not been received by the intended recipient, the sender must commence tracing the path of the documents to identify their current location.

If tracing action fails to locate the documents, Security-Reporting-and-Referrals must be notified via a security incident report as per the AFP National Guideline on personnel security.

Destroying registered documents

When classified documents require destruction, the following procedure must be applied:

1. The destruction must be conducted by a CDRMM.

2. Prior to any destruction occurring, each document to be shredded must be positively identified by both the CDRMM and a witness, by cross-checking the details on the document with the details recorded in columns (a) to (h) of the CDR.
3. TOP SECRET documents must be shredded within the relevant sensitive compartmented information facility (SCIF).
4. All parts of each document must be destroyed using a Class A shredder.
5. Once the documents have been destroyed, the CDRMM must close the relevant CDR entries by conducting the actions detailed below.

When non-paper documents (i.e. CDs, DVDs, etc.) require destruction, the Communications Intelligence Security Officer (COMSO) must be consulted to determine the appropriate method of destruction.

Shredding particles must be collected in a clear plastic bag attached to the shredder. Once an appropriate AFP appointee of the area (i.e. who has the necessary security clearance and briefings) has checked that all of the shredding is 1mm cross-cut, it may be disposed of as UNCLASSIFIED waste. To make it easier to check for large pieces, other forms of paper waste or non-paper waste must not be mixed with the shredded material.

Closing a CDR entry

When there is no longer a need to retain a document within the originating business area, it can be:

- disseminated in accordance with Commonwealth law and the AFP National Guideline on information management
- archived if required per the *Archives Act 1983* (Cth) and the AFP National Guideline on information management
- destroyed by shredding in a Class A shredder.

In each case, the applicable CDR entry must be closed by ruling a red line straight across both the Receipt Details page and Disposal Details page along the middle broken line. Where a document is disposed of by transfer to another person using a safe-hand receipt, the entry may only be closed on return of the receipt form.

Where a document has been shredded, the destroying CDRMM and witness must clearly write their names and AFP numbers, and date and sign the entry in column (n).

Archiving registered documents

TOP SECRET documents must not be submitted to the AFP's Records Management Unit.

Registered documents that need to be archived should be delivered by safe-hand, as per Attachment 2 of this guideline, to the nearest regional AFP Records Management office. The AFP's Records Management office responsible for archiving must sign for each document, and **note** the file in which the documents are contained.

Audits

If an item recorded in a CDR cannot be located during an audit, the Security Reporting requirements must be followed.

The details/results of audits/musters must be recorded separately to the material held against the CDR and vice versa. The record must include the:

- date of the audit
- serial numbers checked
- method used for the audit (e.g. all documents in a file (insert file numbers), sequential CDR serial numbers, etc.)
- anomalies identified and corrective action taken.

2. Closing and retention of CDRs

A CDR remains active until all entries have been closed. Once all entries awaiting destruction, disposal or transfer to another CDR have been completed, the CDR may be closed.

The CDR must be retained by the business area for 5 years after the date it was closed.

In the event that a team or function is disbanded or re-organised, the return and transfer of all accountable material held by that team or portfolio is the responsibility of both the outgoing CDRMM and responsible line manager. Once all accountable material has been returned or disposed of, the CDR must be returned to the Information Security-Communications Security Team/COMSO.

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 11:42 AM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47B invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 11:18 PM
To: s47E(d)
Subject: Please activate your Clearview account

Hi s47E(d)

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single biggest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Mondav. 2 December 2019 2:46 PM
To: s47E(d)
Subject: Verify your email for Clearview

Hi s47E(d)

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/ImNyYWlnLm1hbm5AYWZwLmdvdi5hdSI.EMYogA.sR0hWHJs3lwNLOB39UhXXm-cjW0

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 2 December 2019 2:46 PM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER
Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

From: Hoan T s47G @clearview.ai>
Sent: Tuesday, 3 December 2019 2:13 PM
To: s47E(d)
Subject: Connecting re: Clearview

Hi s47E(d)

I'm one of the founders of Clearview - and also incidentally from Australia, but now living in the USA

How have you found the app so far? I would love to connect and learn more about how it can be used for the AFP.

Let me know what time is good to chat!

Best Regards
Han

From: s47G @clearview.ai>
Sent: Tuesday, 3 December 2019 2:46 PM
To: s47E(d)
Subject: Re: Connecting re: Clearview [SEC=UNOFFICIAL]

Great chatting s47E(d)

Just let me know the names/emails of any colleague you want to give the app too

Let's stay in touch!

> On Dec 2, 2019, at 11:18 PM, s47E(d) @afp.gov.au> wrote:
>
> UNOFFICIAL
> Hi Han,
>
> Thanks for reaching out. We've only just started using it and so far it has been valuable.
>
> I'm available anytime.
>
> Rgds
>
> s47E(d)
>
> COVERT ONLINE ENGAGEMENT
> AUSTRALIAN CENTRE TO COUNTER CHILD EXPLOITATION AUSTRALIAN FEDERAL
> POLICE
>
> Tel + s47E(d) www.afp.gov.au
> UNOFFICIAL
>
> -----Original Message-----
From: Hoan T s47G @clearview.ai>
> Sent: Tuesday, 3 December 2019 2:13 PM
> To s47E(d) @afp.gov.au>
> Subject: Connecting re: Clearview
>
> Hi s47E(d)
>
> I'm one of the founders of Clearview - and also incidentally from
> Australia, but now living in the USA
>
> How have you found the app so far? I would love to connect and learn more about how it can be used for the AFP.
>
> Let me know what time is good to chat!
>
> Best Regards
> Han
>
> ***
> WARNING

>
> This email message and any attached files may contain information that
> is confidential and subject of legal privilege intended only for
> use by the individual or entity to whom they are addressed.   If you
> are not the intended recipient or the person responsible for
> delivering the message to the intended recipient be advised that you
> have received this message in error and that any use, copying,
> circulation, forwarding, printing or publication of this message or
> attached files is strictly forbidden, as is the disclosure of the
> information contained therein. If you have received this message in
> error, please notify the sender immediately and delete it from your
> inbox.
>
> AFP Web site: http://www.afp.gov.au
> **

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 5 December 2019 12:27 AM
To: s47E(d)
Subject: Please activate your Clearview account

Hi s47E(d)

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

emember: your password must be 8 characters and contain a number.

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single biggest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 4 December 2019 11:55 AM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47E(d) invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Tuesday, 17 December 2019 1:13 AM
To: s47E(d)
Subject: Your Clearview account is still waiting

Hi s47E(d)

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

s47E(d)

From:	help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent:	Thursday, 9 January 2020 6:40 PM
To:	s47E(d)
Subject:	How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s47E(d) s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesdav. 4 December 2019 11:52 AM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

[redacted] s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 18 December 2019 1:14 AM
To: [redacted] s47E(d)
Subject: Take a selfie with Clearview

Hi [redacted] s47E(d)

Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has **unlimited** searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are **always** private and **never** stored in our proprietary database, which is totally separate from the photos you search.

You can get Clearview on your iPhone or Android cell phone by clicking "Get Mobile App" on the left-hand side of the screen when you're logged in to Clearview on desktop.

To log in to Clearview on desktop just click the button below:

Log in

You can also upload a photo of yourself to Clearview on your desktop computer.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

[redacted] s47E(d)

s47E(d)

From: Jessica G s47G @clearview.ai>
Sent: Thursday, 19 December 2019 1:07 PM
To: s47E(d)
Subject: cv
Attachments: Clearview_Search_Tips.pdf; Success Stories.pdf

Good evening. You should have an email from Team Clearview with your account activation link. I encourage you to test the tech on computer/laptop (log in thru https://app.clearview.ai/app/login) and the mobile app. Also attached is general info and sample success stories and a doc with some tips on how to best use photos. If you would find a video demo call helpful just let me know. Finally – if there are any other officers/agents that would like an account just send me names and emails.

Please do not hesitate to contact me with any questions.

- Jess

Jessica Medeiros Garrison
205.568.4371
s47G @clearview.ai

s47E(d)

Clearview Search Tips

Potential Causes of Reduced Accuracy for Clearview Facial Recognition Technology

Clearview is an investigative software application that uses state-of-the-art facial- recognition technology to match a face in a user-uploaded image to a face in publicly available images. It is designed to be used in ways that ultimately reduce crime, fraud, and risk in order to make communities safer. Clearview's technology is designed with the utmost attention to accurate and unbiased match-generation.

The following factors can inhib t facial recognition technology from making accurate facial matches. All of these factors concern characteristics of the image that is input by the user (the "probe image") and in some way obscure or disrupt algorithmic analysis of the features of the person the user is attempting to identify (the "search subject"). Searches which are affected by one or more of these factors are more likely to result in search results which do not facilitate accurate identification of image subjects, although accurate results are still sometimes possible when searching images that are affected by these factors. The human operators of Clearview's search technology must follow Clearview's user guidelines and use their law enforcement training to determine the accuracy of all search results.

The most common confounding factors include:

1) Low-Resolution Probe Images

Probe images must have sufficiently high resolution in the facial area of the search subject to allow the facial recognition algorithm to identify and match specific features. Low resolution images, with high pixelation in the face region of the subject, cannot consistently support accurate facial matching. Low resolution probe images may result from the inherent limitations on the resolution of the camera which took the source image, motion blur, or may result from other conditions such as the distance between the search subject and the camera which took the probe image.

2) Image and Video “Noise” in Probe Image

Just as inherent low resolution can prevent inaccurate matches, “noisy” imagery containing motion blurs and atmospheric interference will result in pixelated and/or blurred facial features for the search subject which frustrates the operation of the facial feature identification and matching algorithm.

3) Poor Lighting Conditions in Probe Images

The facial area of the search subject must be sufficiently well-lit in the probe image to allow the facial recognition algorithm to identify and match specific features. Probe images which do not contain a sufficiently well-lit facial area will not produce accurate search results because the facial features are not sufficiently visible for algorithmic identification.

4) High Camera Pitch Angle Probe Images

Many cameras, such as roof and ceiling-mounted security cameras, and cameras on airborne platforms, produce images which look down on the search subject from a high “pitch”, or transverse, angle. When used as a probe images, cameras that are at a high pitch/transverse angle to the search subject’s face will produce accurate matches at significantly lower rates, because many facial features are not visible from a high transverse angle, and because transposing features to match them with photos taken at a low transverse angle is difficult to accomplish algorithmically.

5) Monitor Screen Artifacts in Probe Images

Some users display an image of the search subject on an LCD monitor and then take a photo of that image with their mobile device, using this photo as the probe image in a search in the mobile app version of Clearview. This often results in artifacts, including visible resolution cells, in the probe image, which prevents accurate algorithmic detection and matching of facial features. To prevent this problem, users should not resort to the “photo of a screen” technique, and should instead directly upload images from their computers to the web browser version of Clearview.

6) Ancillary/Background Features in Probe Image

Probe images that contain conspicuous background objects and patterns that overlap with the facial area of the search subject can result in inaccuracies in the search results returned by Clearview. This problem can be mitigated in some cases by cropping background objects out of the image.

7) Hats, Glasses and Other Face-Covering Objects

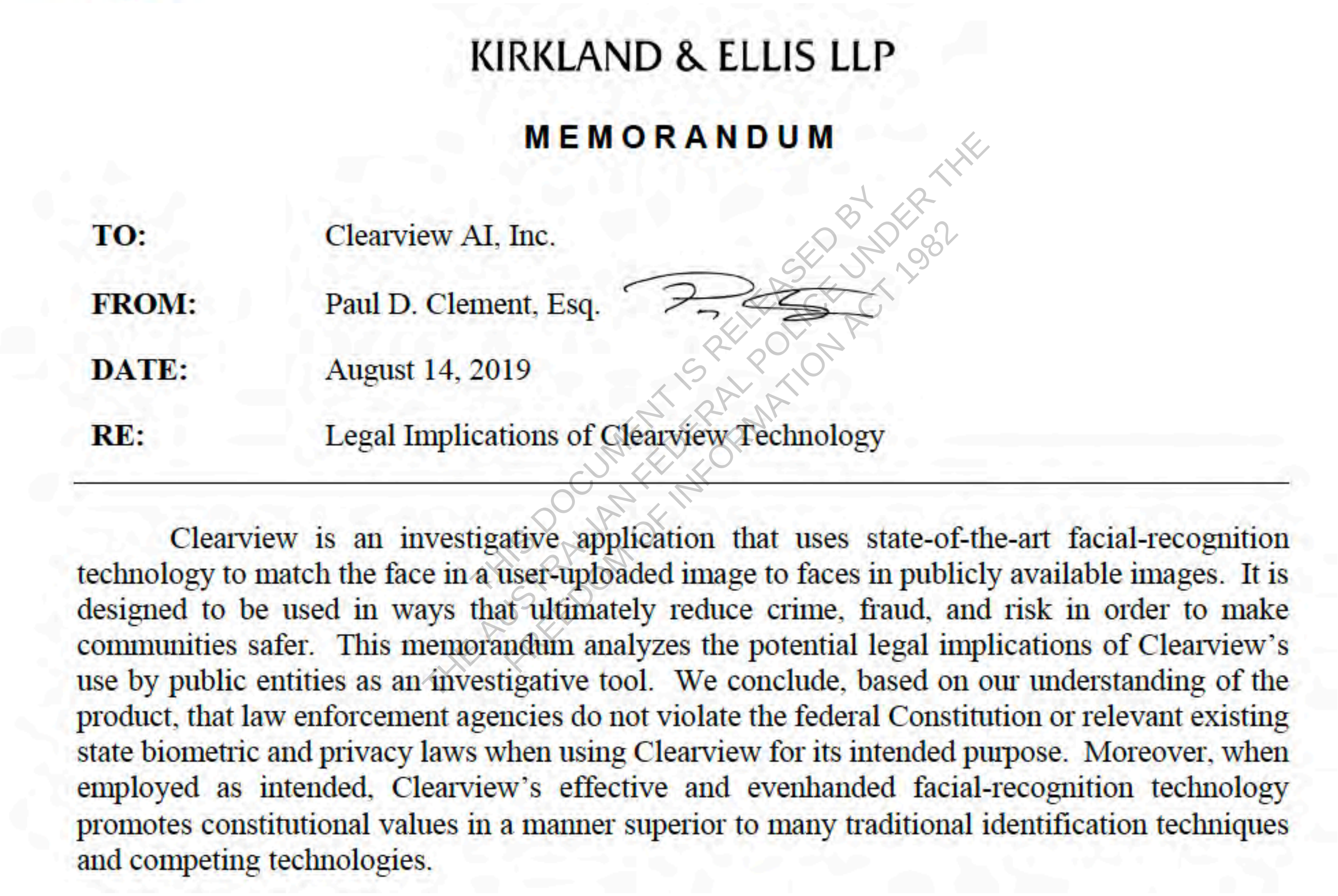
Objects, most commonly items of clothing like hats or sunglasses, which partially or totally obscure the face of the search subject will reduce the likelihood of an accurate match.

Users searching images that are affected by one or more of these factors should exercise additional scrutiny and caution when analyzing the search results, and should expect lower rates of successful identification when using probe images that are characterized by one or more of these factors.

What is Clearview? Clearview's mission is to drastically reduce crime, fraud and risk in order to make communities safer and commerce secure.

Clearview provides law enforcement a revolutionary facial search engine. From a single image it can instantly and accurately return photos matching that face from the Internet and other publicly available sources.

Paul Clement Legal Implications Briefing
Counsel to Clearview



KIRKLAND & ELLIS LLP

MEMORANDUM

TO: Clearview AI, Inc.

FROM: Paul D. Clement, Esq.

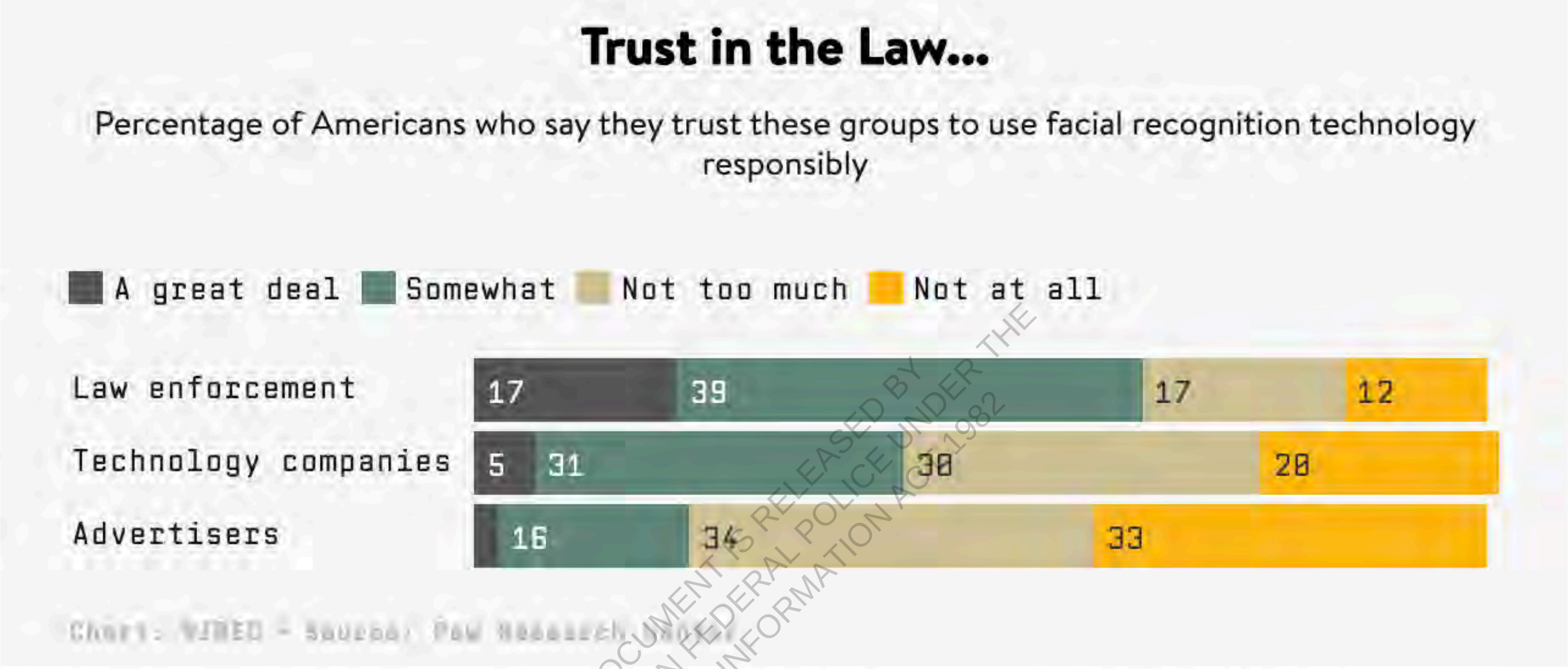
DATE: August 14, 2019

RE: Legal Implications of Clearview Technology

Clearview is an investigative application that uses state-of-the-art facial-recognition technology to match the face in a user-uploaded image to faces in publicly available images. It is designed to be used in ways that ultimately reduce crime, fraud, and risk in order to make communities safer. This memorandum analyzes the potential legal implications of Clearview's use by public entities as an investigative tool. We conclude, based on our understanding of the product, that law enforcement agencies do not violate the federal Constitution or relevant existing state biometric and privacy laws when using Clearview for its intended purpose. Moreover, when employed as intended, Clearview's effective and evenhanded facial-recognition technology promotes constitutional values in a manner superior to many traditional identification techniques and competing technologies.

**Entire Memo - Attachment "A"*

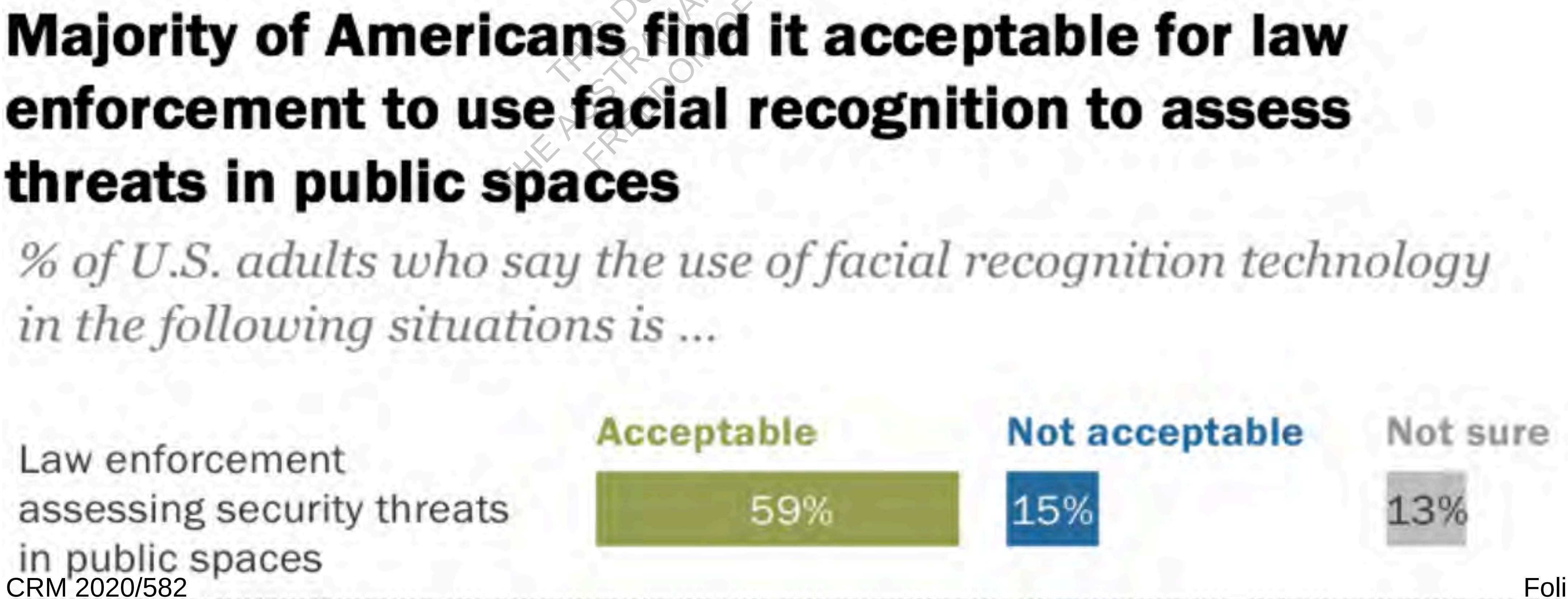
(Pew, 9/19)



Trust in the Law...

Percentage of Americans who say they trust these groups to use facial recognition technology responsibly

Chart: WIRED • Source: Pew Research Center



Majority of Americans find it acceptable for law enforcement to use facial recognition to assess threats in public spaces

% of U.S. adults who say the use of facial recognition technology in the following situations is ...

Accuracy Test Report

In October 2019, the undersigned Panel conducted an independent accuracy test of Clearview AI...For the purposes of this analysis, the Panel used the same basic methodology used by the American Civil Liberties Union (ACLU) in its July 2018 accuracy test of Amazon's Rekognition technology.

The ACLU's approach entailed comparing photographs of all 535 members of the U.S. House of Representatives and Senate against a database of 25,000 arrest photos. The test resulted in 28 members of Congress being incorrectly matched to arrestees from the photo database.

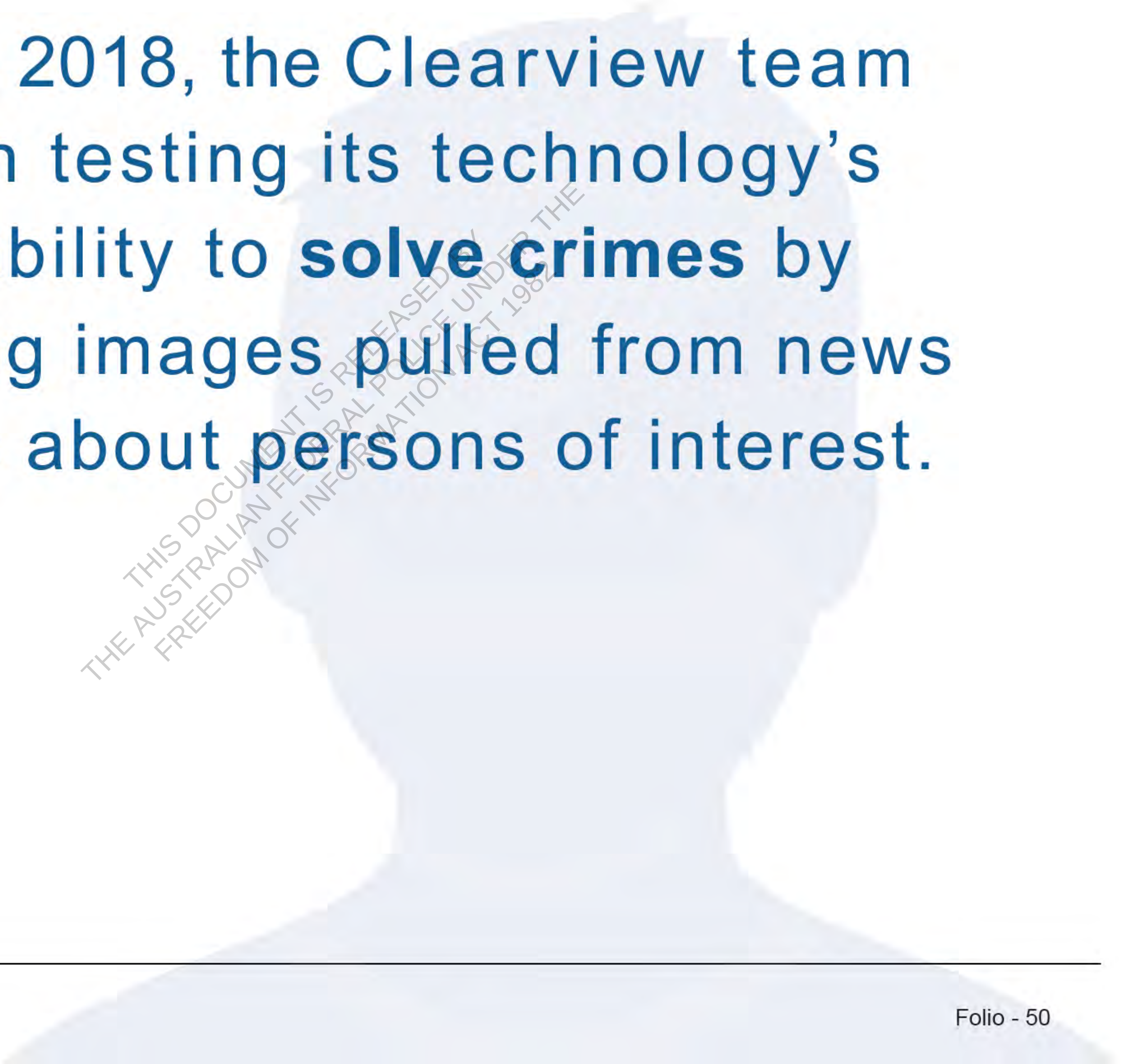
With those important concerns in mind, the Panel conducted the same test of Clearview. **Along with analyzing all 535 members of Congress, the Panel also analyzed all 119 members of the California State Legislature and 180 members of the Texas State Legislature, for good measure.**

The test compared the headshots from all three legislative bodies against Clearview's proprietary database of 2.8 billion images (112,000 times the size of the database used by the ACLU). The Panel determined that Clearview rated 100% accurate, producing instant and accurate matches for every one of the 834 federal and state legislators in the test cohort.

Conducted Independently By:

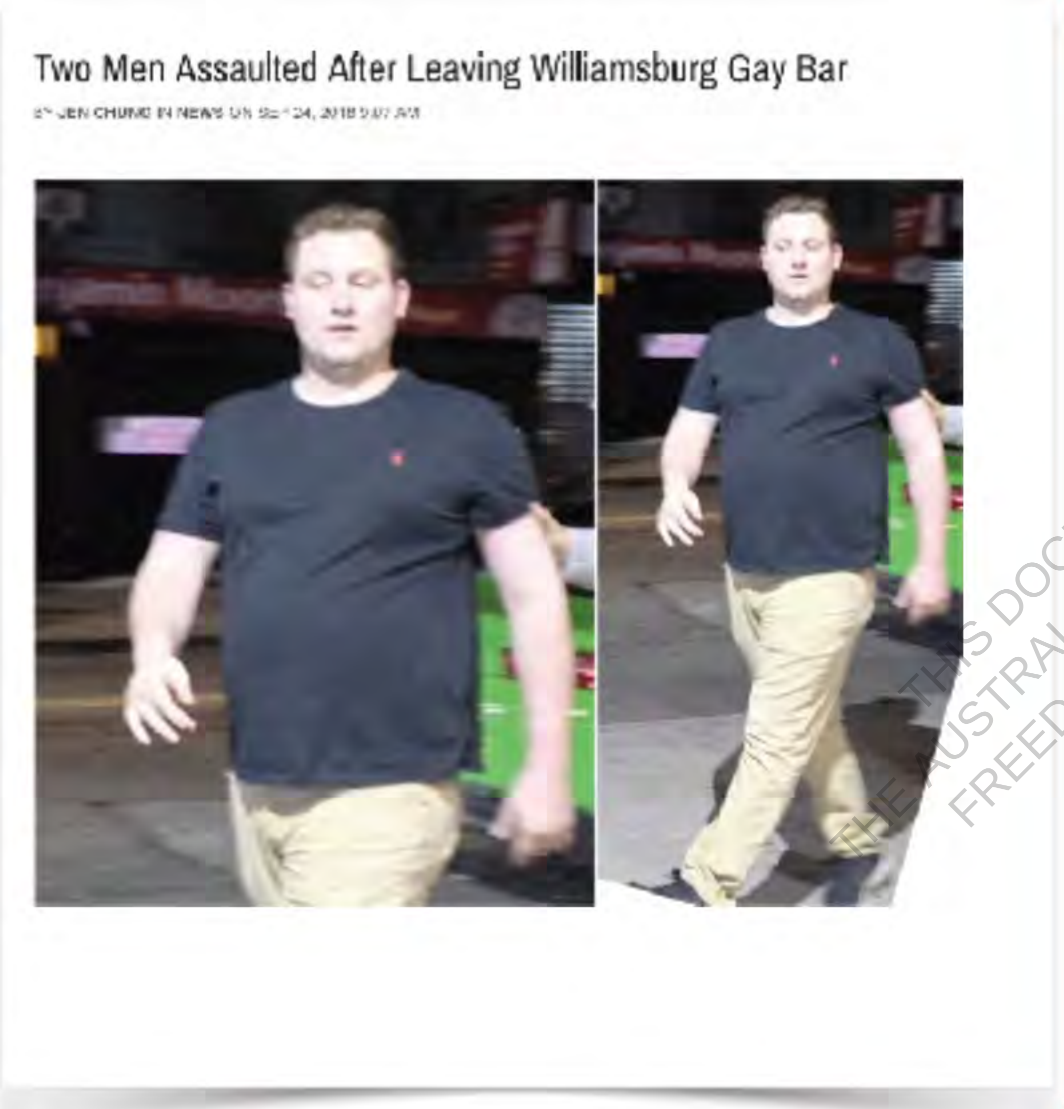
Hon. Jonathan Lippman　Nicholas Cassimatis, PhD　Aaron M. Renn

- **Judge Lippman** served as Chief Judge of the State of New York from 2009 to 2015....
- **Nicholas Cassimatis** is former Chief of Samsung's North American AI Research
- **Aaron Renn** is a Senior Fellow at the Manhattan Institute



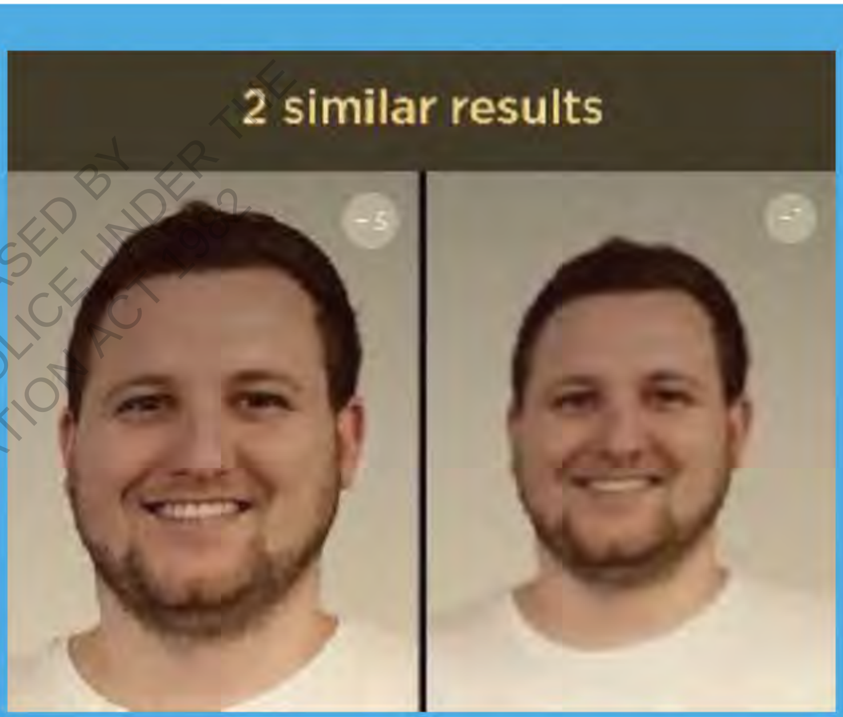
In late 2018, the Clearview team began testing its technology’s capability to **solve crimes** by scanning images pulled from news reports about persons of interest.

On September 24, 2018, **The Gothamist** published a photo of a man who assaulted two individuals outside a bar in Brooklyn, NY.



Two Men Assaulted After Leaving Williamsburg Gay Bar

BY JEN CHUNG IN NEWS ON SEP 24, 2018 9:07 AM



2 similar results

Using Clearview, we instantly identified the assailant and sent the tip to the police, who confirmed his identity.

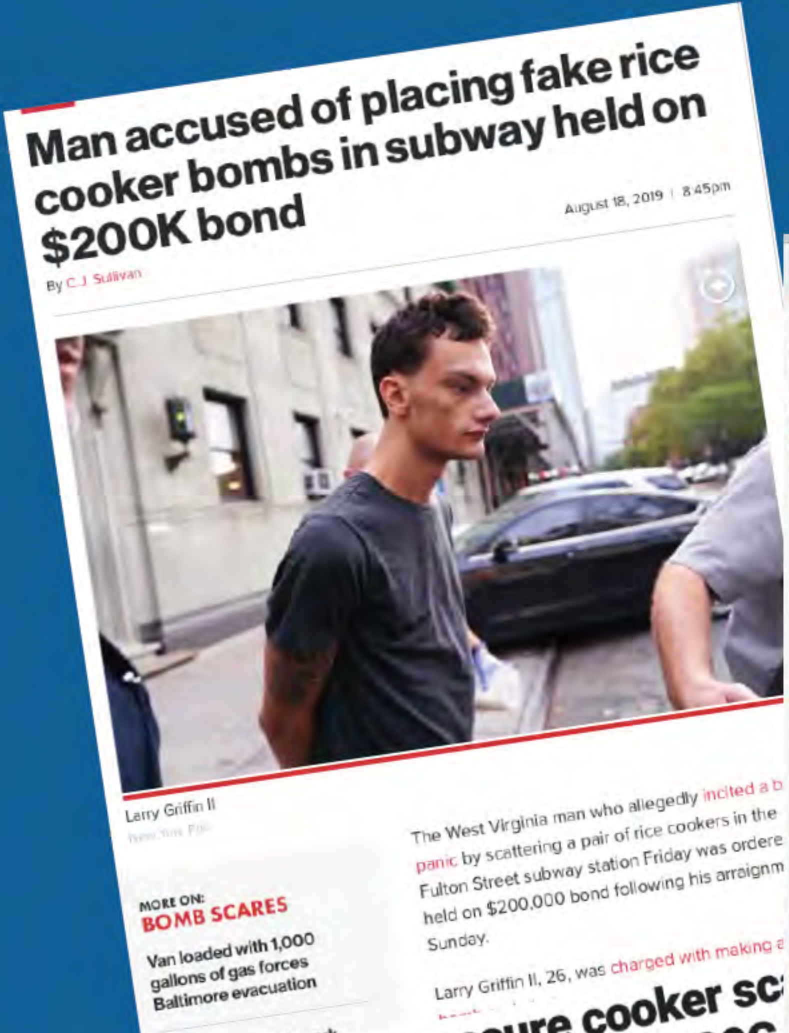
Clearview begins to launch pilot programs with law enforcement.

Detectives begin breaking unsolved cases involving **pedophiles, credit-card fraud, sexual harassment, ATM theft and hate-crimes.**

Here are some of their stories…

NYC Bomb Scare

https://www.youtube.com/watch?v=JqA9cCpJUO4
Click here ⇧ to see News Coverage



Man accused of placing fake rice cooker bombs in subway held on $200K bond

By C.J. Sullivan August 18, 2019 | 8:45pm

Larry Griffin II

MORE ON: BOMB SCARES

Van loaded with 1,000 gallons of gas forces Baltimore evacuation

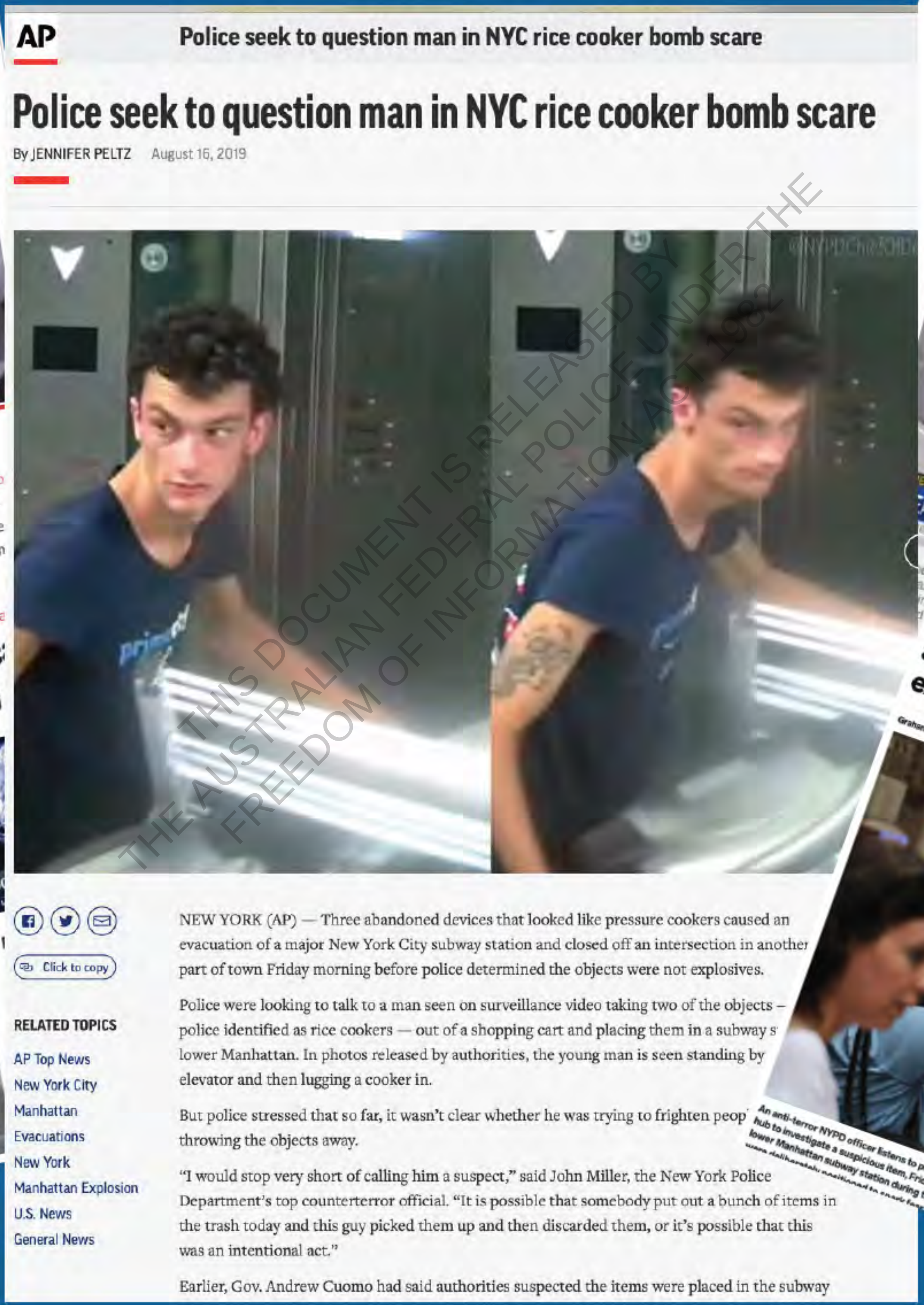
Panic erupts at Newark

The West Virginia man who allegedly incited a b panic by scattering a pair of rice cookers in the Fulton Street subway station Friday was ordere held on $200,000 bond following his arraignm Sunday.

Larry Griffin II, 26, was charged with making a

New York City pressure cooker sc suspect has bail set at $200G

By Nicole Darrah | Fox News



AP Police seek to question man in NYC rice cooker bomb scare

Police seek to question man in NYC rice cooker bomb scare

By JENNIFER PELTZ August 16, 2019

Click to copy

RELATED TOPICS
- AP Top News
- New York City
- Manhattan
- Evacuations
- New York
- Manhattan Explosion
- U.S. News
- General News

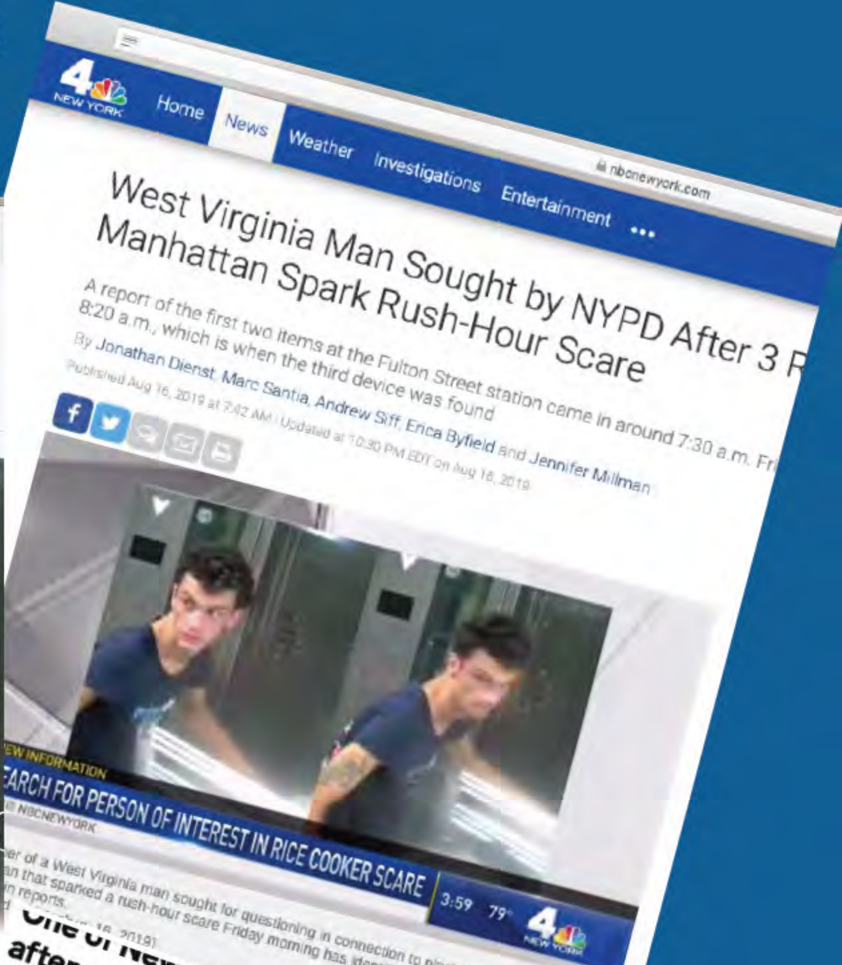
NEW YORK (AP) — Three abandoned devices that looked like pressure cookers caused an evacuation of a major New York City subway station and closed off an intersection in another part of town Friday morning before police determined the objects were not explosives.

Police were looking to talk to a man seen on surveillance video taking two of the objects – police identified as rice cookers — out of a shopping cart and placing them in a subway s lower Manhattan. In photos released by authorities, the young man is seen standing by elevator and then lugging a cooker in.

But police stressed that so far, it wasn't clear whether he was trying to frighten peop throwing the objects away.

"I would stop very short of calling him a suspect," said John Miller, the New York Police Department's top counterterror official. "It is possible that somebody put out a bunch of items in the trash today and this guy picked them up and then discarded them, or it's possible that this was an intentional act."

Earlier, Gov. Andrew Cuomo had said authorities suspected the items were placed in the subway



4 NEW YORK Home News Weather Investigations Entertainment ••• nbcnewyork.com

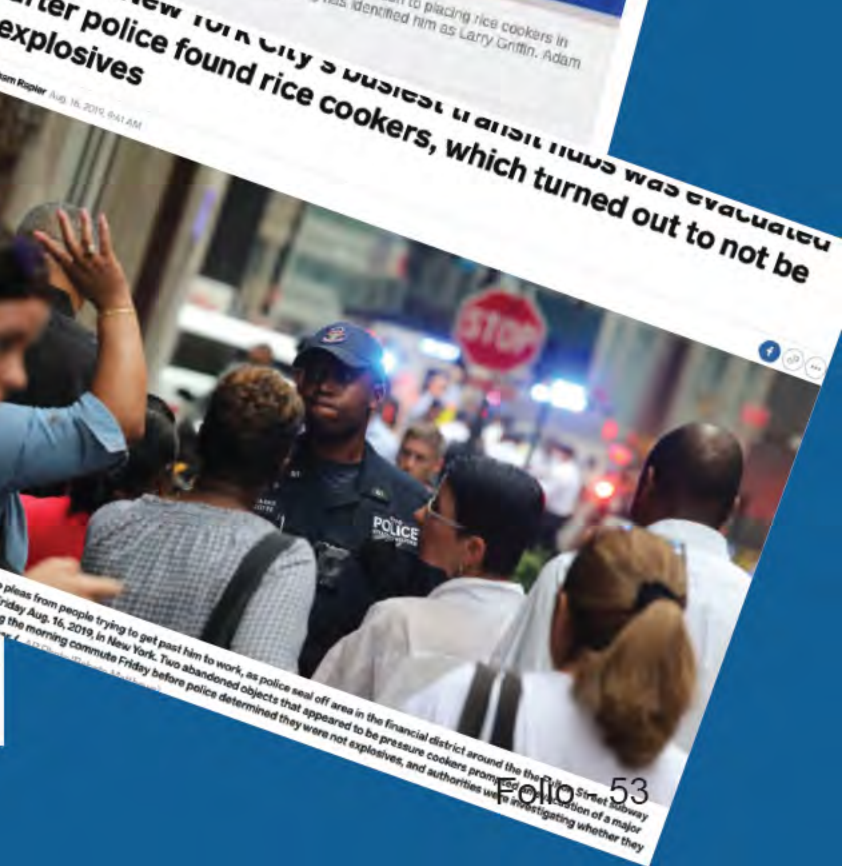
West Virginia Man Sought by NYPD After 3 R Manhattan Spark Rush-Hour Scare

A report of the first two items at the Fulton Street station came in around 7:30 a.m. Fri 8:20 a.m., which is when the third device was found

By Jonathan Dienst, Marc Santia, Andrew Siff, Erica Byfield and Jennifer Millman

Published Aug 16, 2019 at 7:42 AM | Updated at 10:30 PM EDT on Aug 16, 2019

er of a West Virginia man sought for questioning in connection to placing rice cookers in an that sparked a rush-hour scare Friday morning has identified him as Larry Griffin. Adam in reports.



One of New York City's busiest transit hubs was evacuated after police found rice cookers, which turned out to not be explosives

Graham Rapier Aug. 16, 2019, 8:41 AM

An anti-terror NYPD officer listens to pleas from people trying to get past him to work, as police seal off area in the financial district around the the Fulton Street subway hub to investigate a suspicious item, Friday Aug. 16, 2019, in New York. Two abandoned objects that appeared to be pressure cookers prompted evacuation of a major lower Manhattan subway station during the morning commute Friday before police determined they were not explosives, and authorities were investigating whether they were deliberately positioned to spark fear (AP Photo/Bebeto Matthews)

Financial Fraud

Felony charges include:

- Obtaining Property by False Pretense
- Credit Card Theft
- Identity Theft
- Second Degree Sex Exploitation of Minor x 12

Vineland Police: Fraud suspect pretended to be car salesman

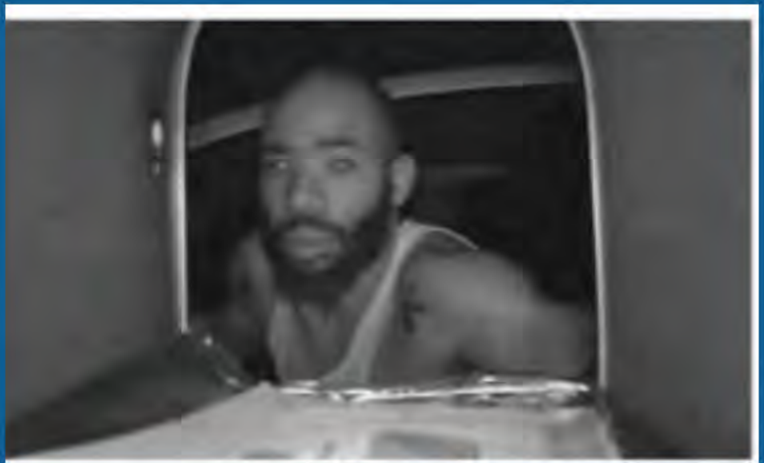
VINELAND – Police announced the arrest of a man who allegedly committed fraud by selling rented cars as his own. James Mero was arrested on Nov. 15. At the time of his arrest, according to reports, he was found in possession of numerous documents that lead investigators to believe there are additional victims in the South Jersey area…Mero would rent vehicles from a local car rental agency and attempt to sell them to residents, accepting down payments and deposits from the victims. Mero also allegedly took potential victims to car dealerships after hours on Sundays, claiming to be a salesperson.

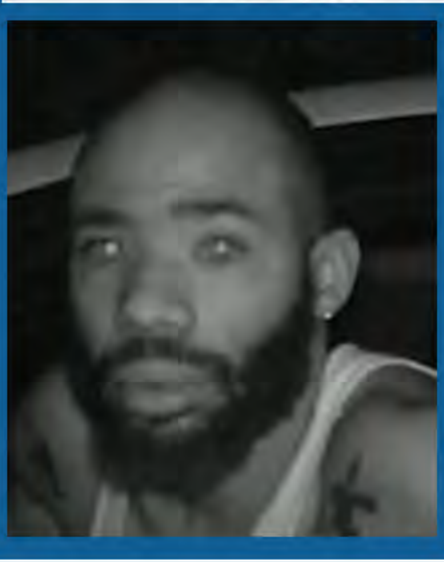
Det. Sgt. Robert Powell
Raleigh Police Department
Financial Crimes Unit

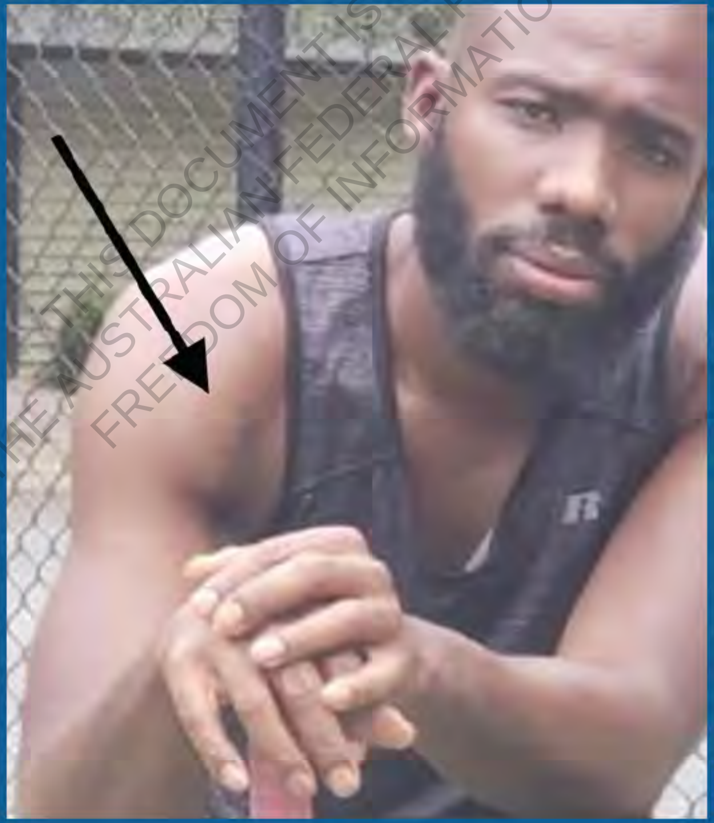
James Mero was identified using Clearview when a BOLO was disseminated using a photo from one of the victims. Mero had been released from federal prison in November 2018, serving time for fraud, and made his way to Raleigh. Total Loss Exposure was $191,536.46 with 15 known victims. On June 3, 2019, US Marshal TFO Brian Lindsey and the US Marshals located and arrested James Mero in Henderson, NC. Mero was wanted on an outstanding federal probation warrant and several financial crimes warrants. The interview with Mero also elicited incriminating statements as well as his consent to examine his cell phone. Initial review of the cell phone found not only incriminating information to his fraudulent activity but child pornography.

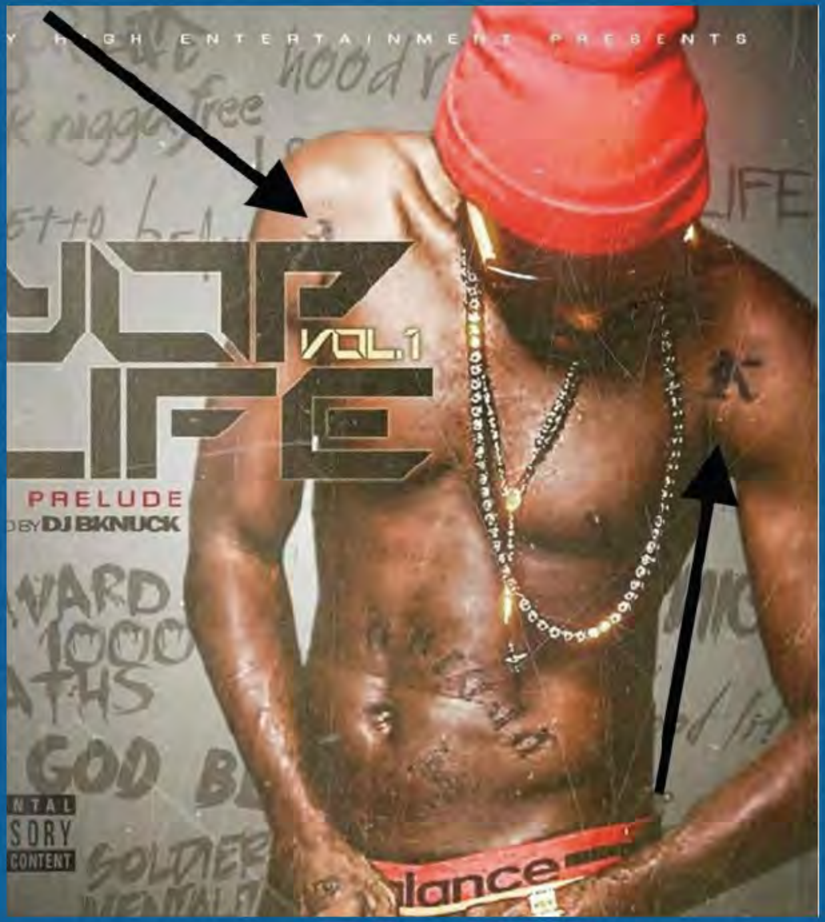
Mailbox Theft

Mail theft is a big problem in the Atlanta area. Detective Scott Harrell received a request for assistance in identifying a mailbox theft suspect. One potential victim, in a heavily hit area, installed a camera in his mailbox. When the suspect opened the mailbox, he did not get out of the car to retrieve the mail but just leaned into the mailbox. This allowed the camera to capture a full frontal facial image. The detective ran the image through Clearview. This produced positive identification based on definitive tattoos on the suspect's shoulder. Clearview returned a 10 year old mugshot and social media photos that corroborated the other evidence on file.

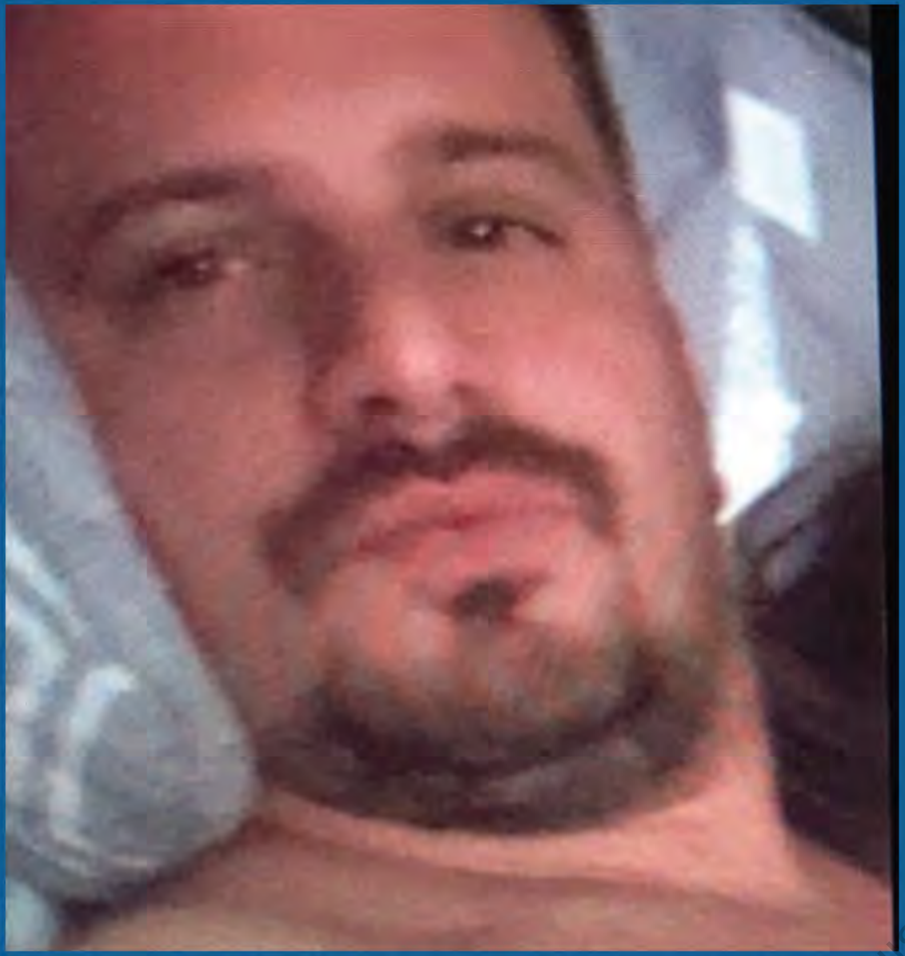


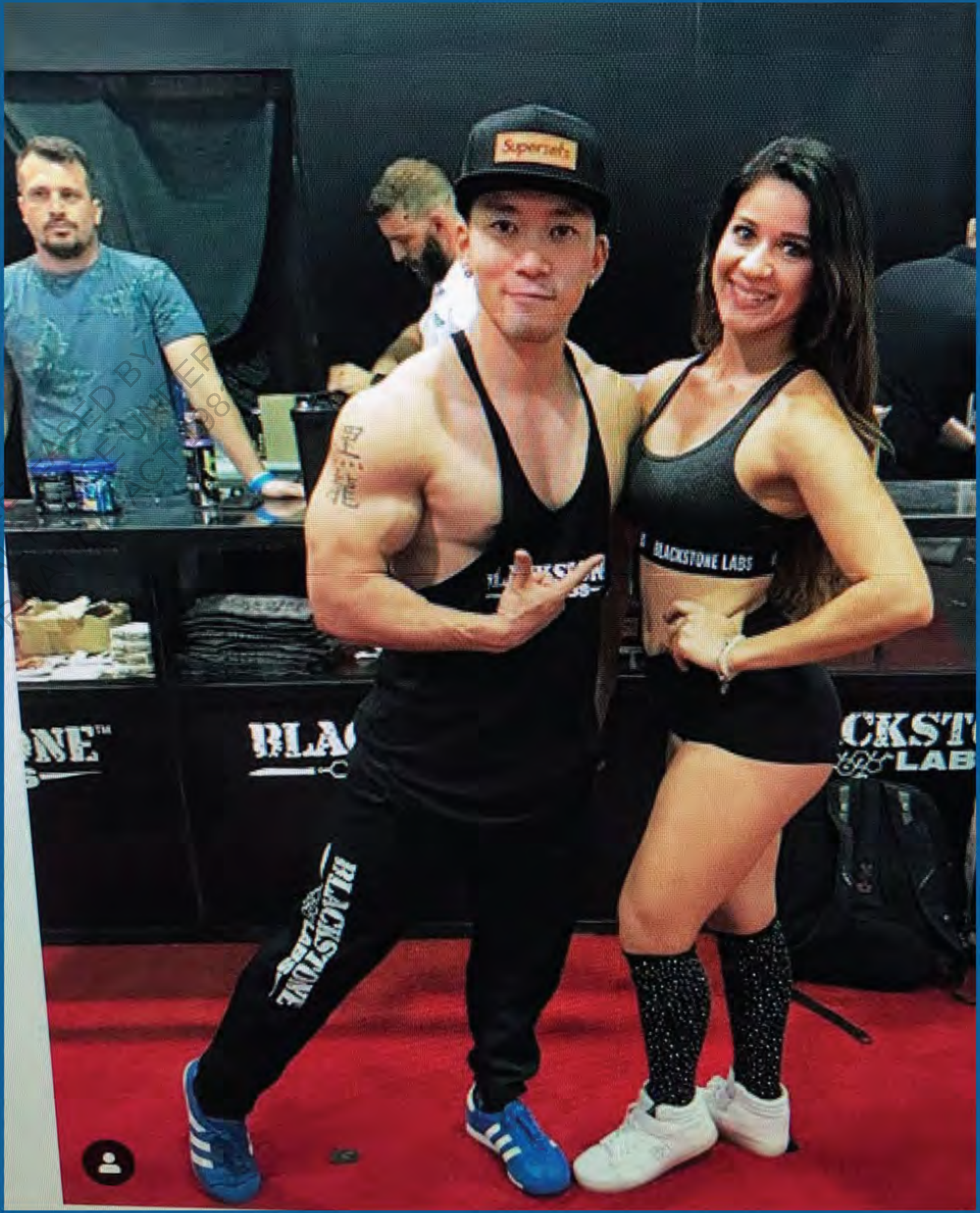






Crimes Against Children

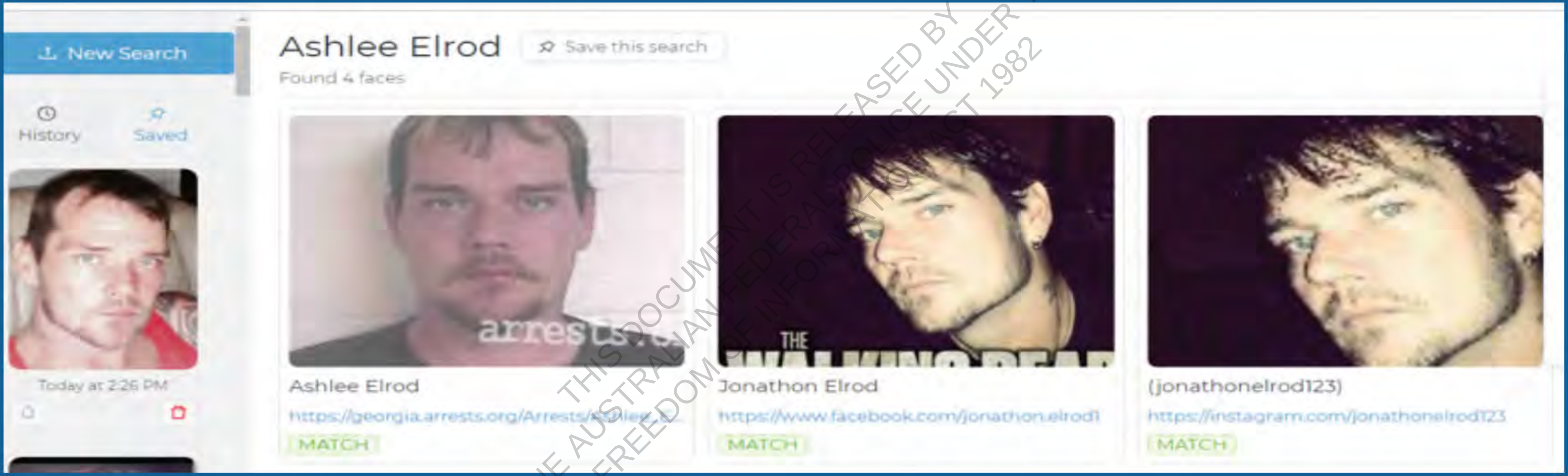




Las Vegas, Nevada – A federal Child Exploitation Investigations Unit had been investigating a major child pornography/exploitation case in Las Vegas. They were reviewing a series of 14 photographs. Two photos included the image of a John Doe in the background. Agents searched the face against available criminal databases and found nothing. A subsequent search of the image through Clearview enabled the investigators to quickly identify the man. This was a major break in this case.

Crimes Against Children

Birmingham, Alabama – the images below were used in identifying a John Doe suspect in a child enticement case.



Today at 2:26 PM

Ashlee Elrod

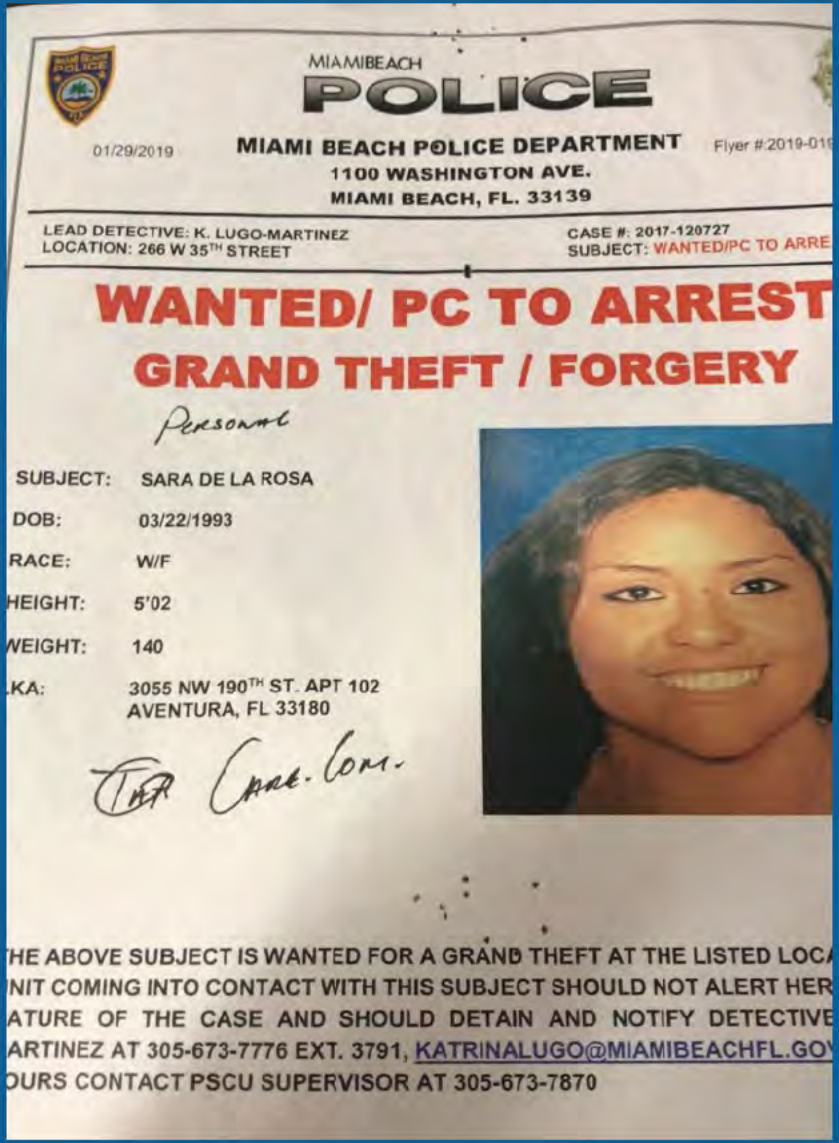
Found 4 faces

Ashlee Elrod
https://georgia.arrests.org/Arrests/Ashlee_E...
MATCH

Jonathon Elrod
https://www.facebook.com/jonathon.elrod1
MATCH

(jonathonelrod123)
https://instagram.com/jonathonelrod123
MATCH

Grand Theft / Forgery



MIAMIBEACH
POLICE

01/29/2019

MIAMI BEACH POLICE DEPARTMENT
1100 WASHINGTON AVE.
MIAMI BEACH, FL. 33139

Flyer #:2019-01

LEAD DETECTIVE: K. LUGO-MARTINEZ
LOCATION: 266 W 35TH STREET

CASE #: 2017-120727
SUBJECT: WANTED/PC TO ARRE

WANTED/ PC TO ARREST
GRAND THEFT / FORGERY

Personal

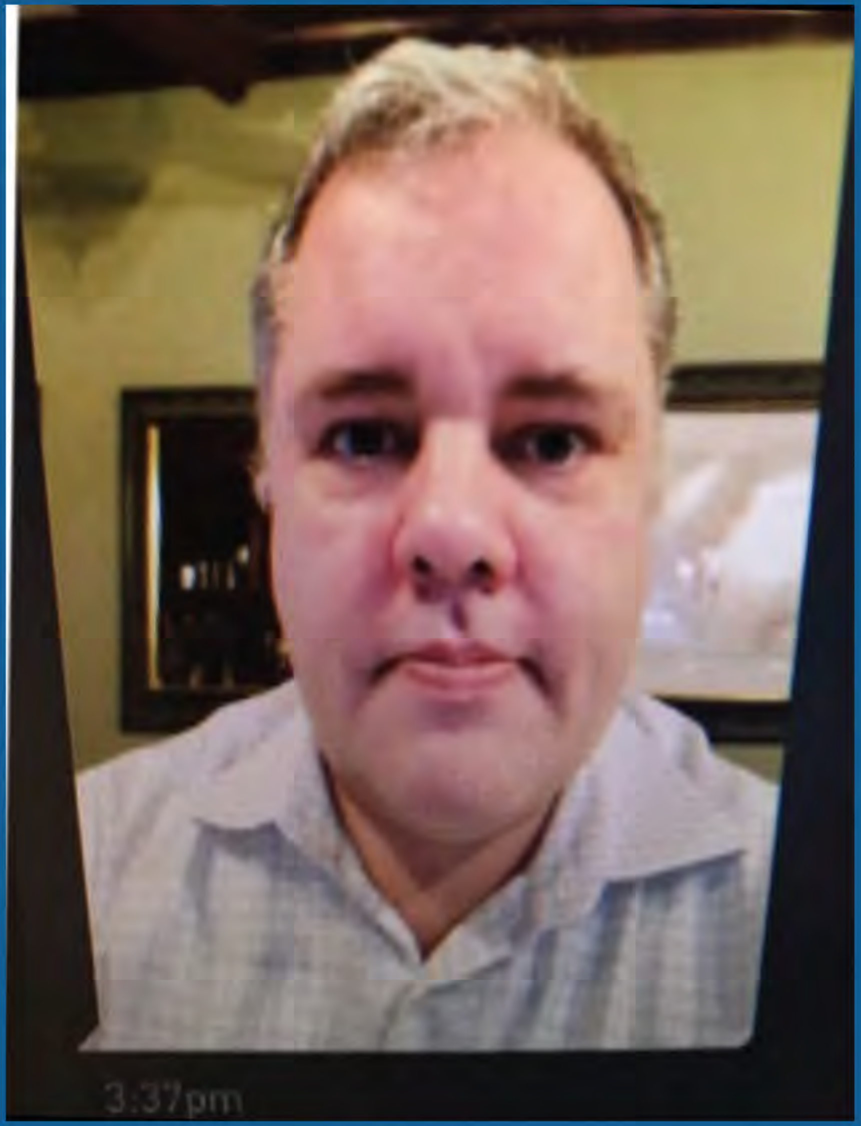
SUBJECT: SARA DE LA ROSA
DOB: 03/22/1993
RACE: W/F
HEIGHT: 5'02
WEIGHT: 140
KA: 3055 NW 190TH ST. APT 102
AVENTURA, FL 33180

HE ABOVE SUBJECT IS WANTED FOR A GRAND THEFT AT THE LISTED LOCA
NIT COMING INTO CONTACT WITH THIS SUBJECT SHOULD NOT ALERT HER
ATURE OF THE CASE AND SHOULD DETAIN AND NOTIFY DETECTIVE
ARTINEZ AT 305-673-7776 EXT. 3791, KATRINALUGO@MIAMIBEACHFL.GOV
OURS CONTACT PSCU SUPERVISOR AT 305-673-7870

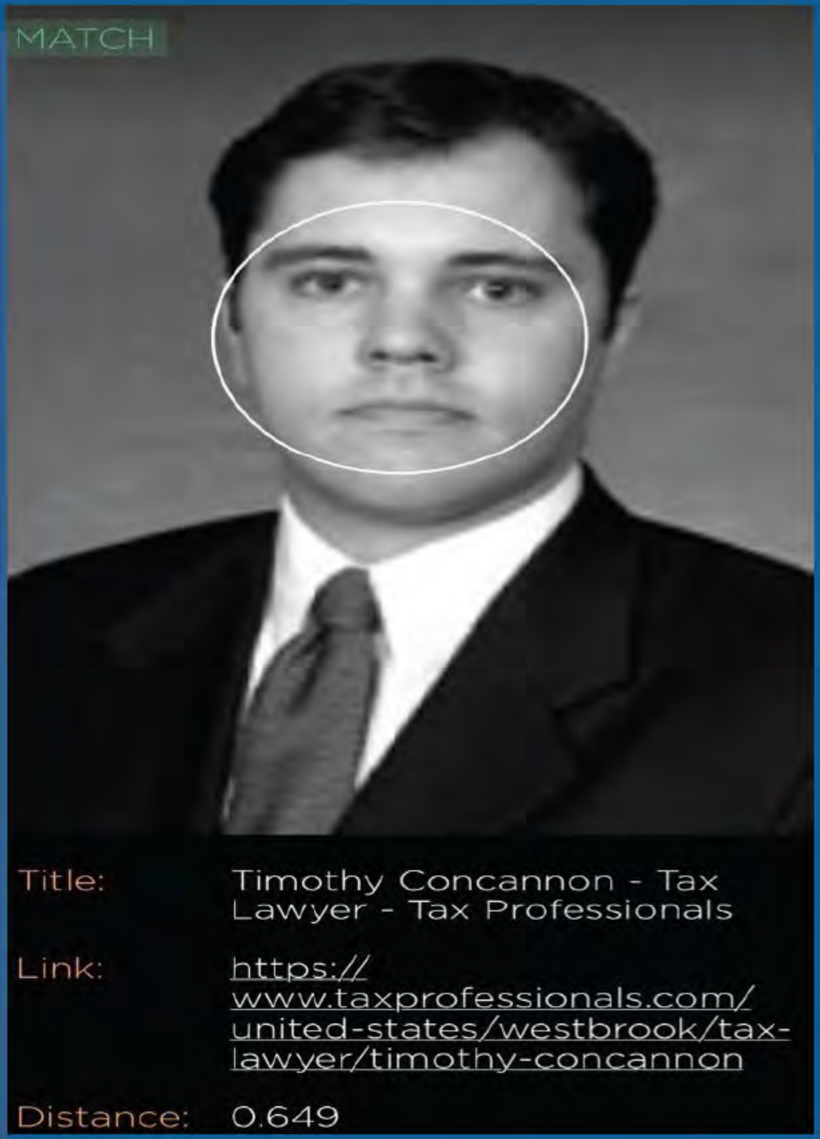
This female suspect alluded law enforcement for several years and was wanted for 17 counts of forgery. Using Clearview, the Sergeant received intelligence that led to her identification and the fact that she was returning from a trip to the Bahamas courtesy of the return ticket she had posted in a photo. The investigator notified TSA, customs and the airline. The suspect was arrested at the gate. Criminal prosecution is pending.

Sergeant Balceiro's unit assists multiple departments with identifying suspects of crimes ranging from drugs, prostitution and theft. In his words, "Great product! Every investigator should have this as a tool". - Sergeant Juan Balceiro, Crime Suppression Unit, Miami Beach Police Department

Pedophile



- Law enforcement was unable to identify this suspect in a NY child pedophile investigation.
- Using Clearview, they matched the facial image to a tax professional through a public website.
- After follow-up investigation, he was arrested six days later.



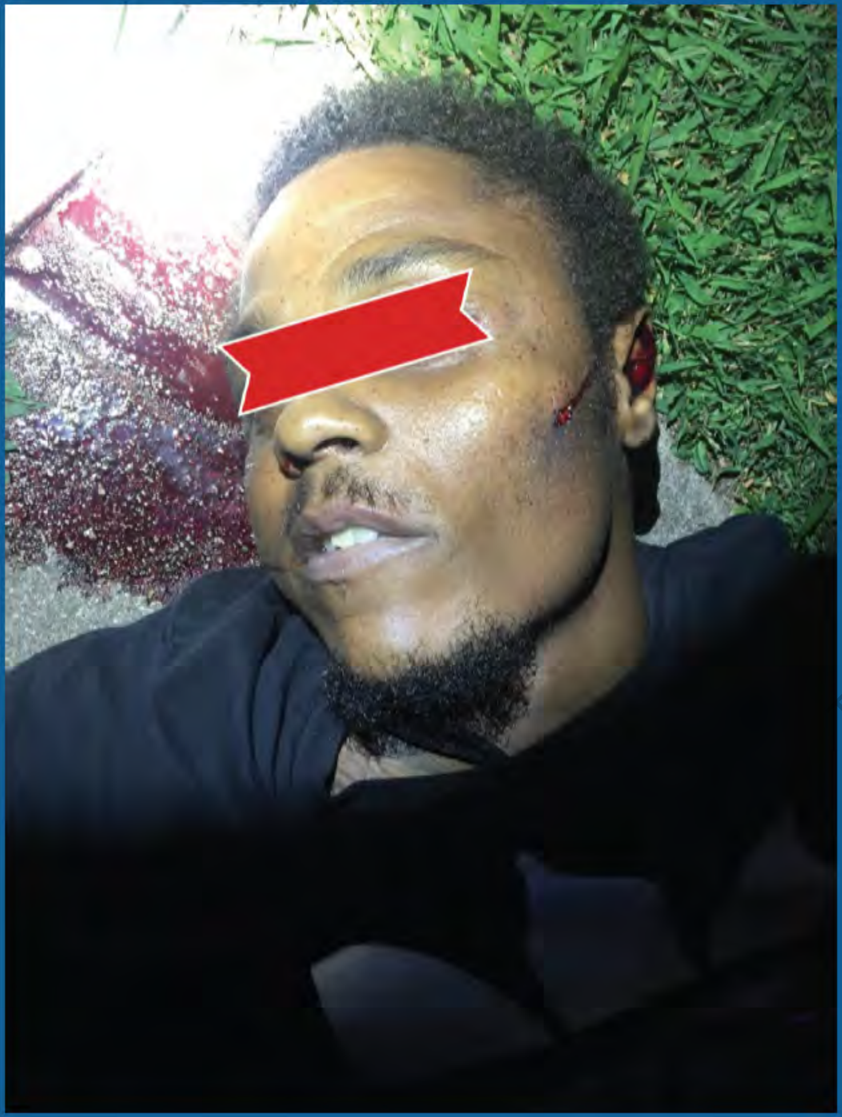
Title: Timothy Concannon - Tax Lawyer - Tax Professionals

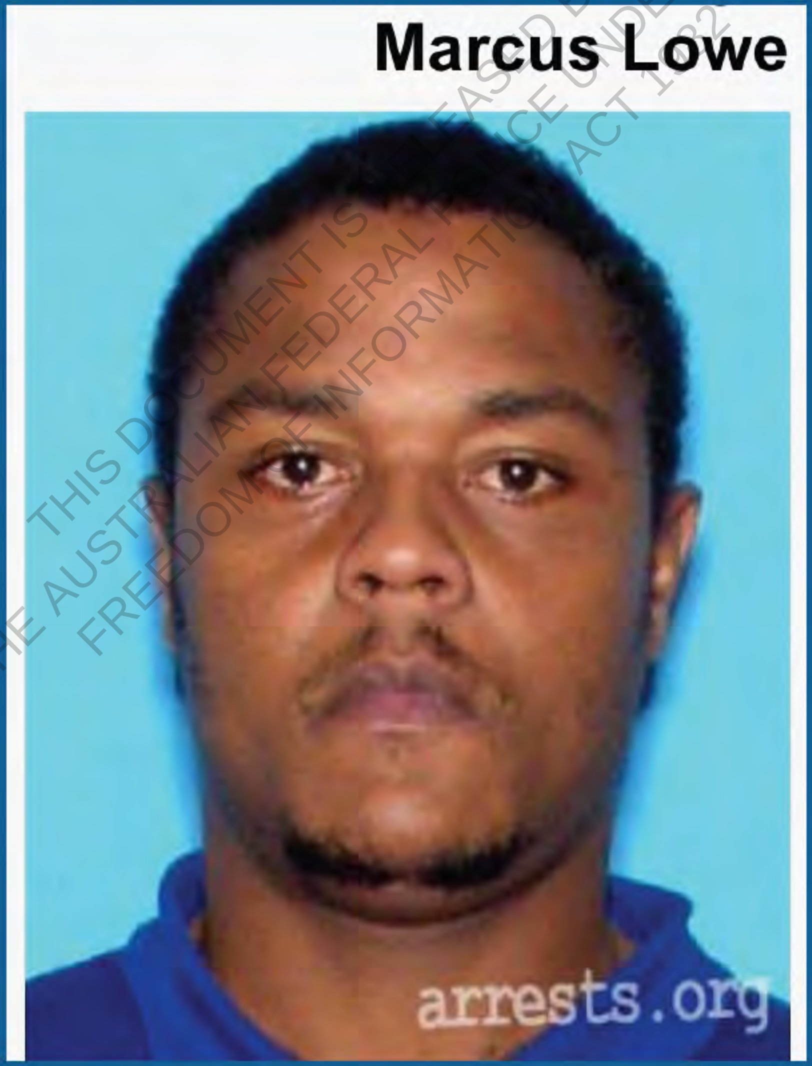
Link: https://www.taxprofessionals.com/united-states/westbrook/tax-lawyer/timothy-concannon

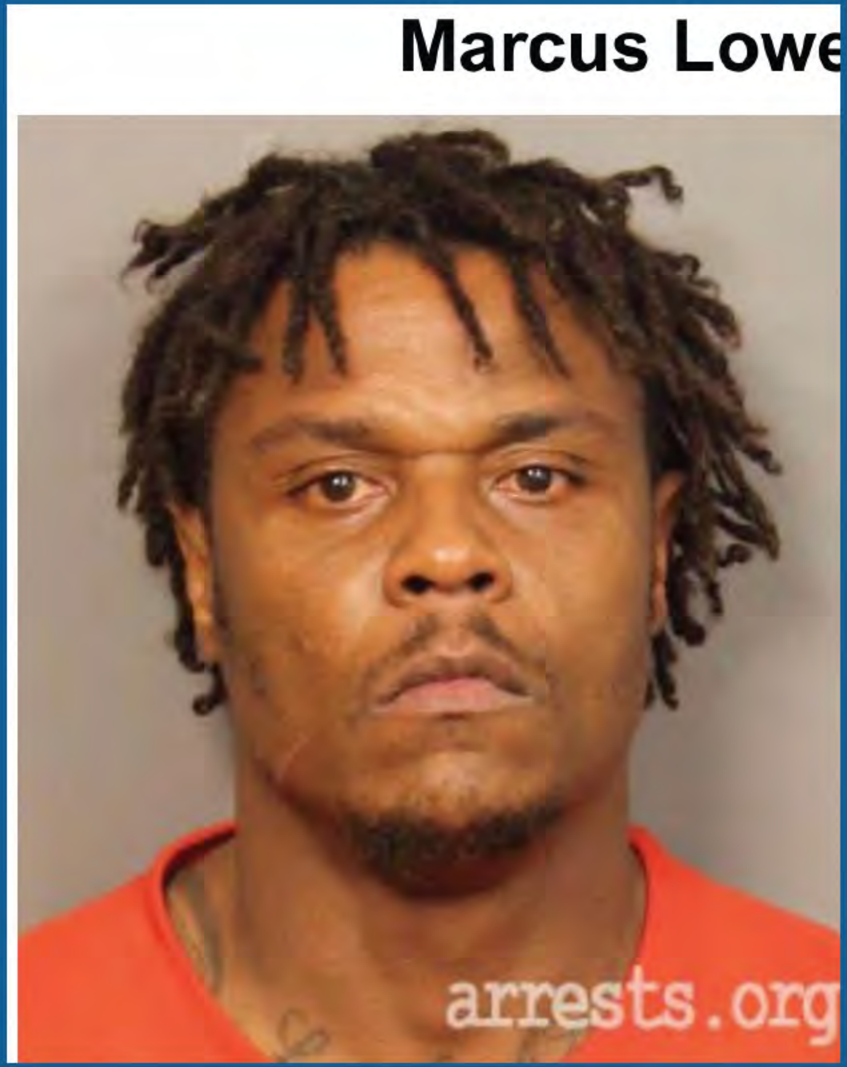
Distance: 0.649

Deceased John Doe

This John Doe victim was found shot on a sidewalk. The officer used the Clearview app to receive information leading immediately to his identity.

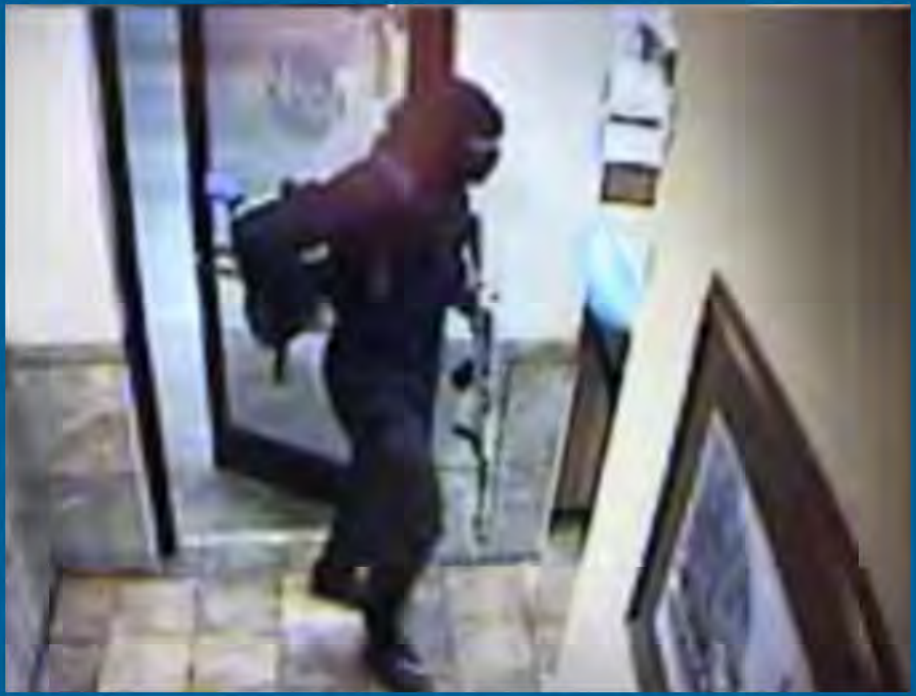


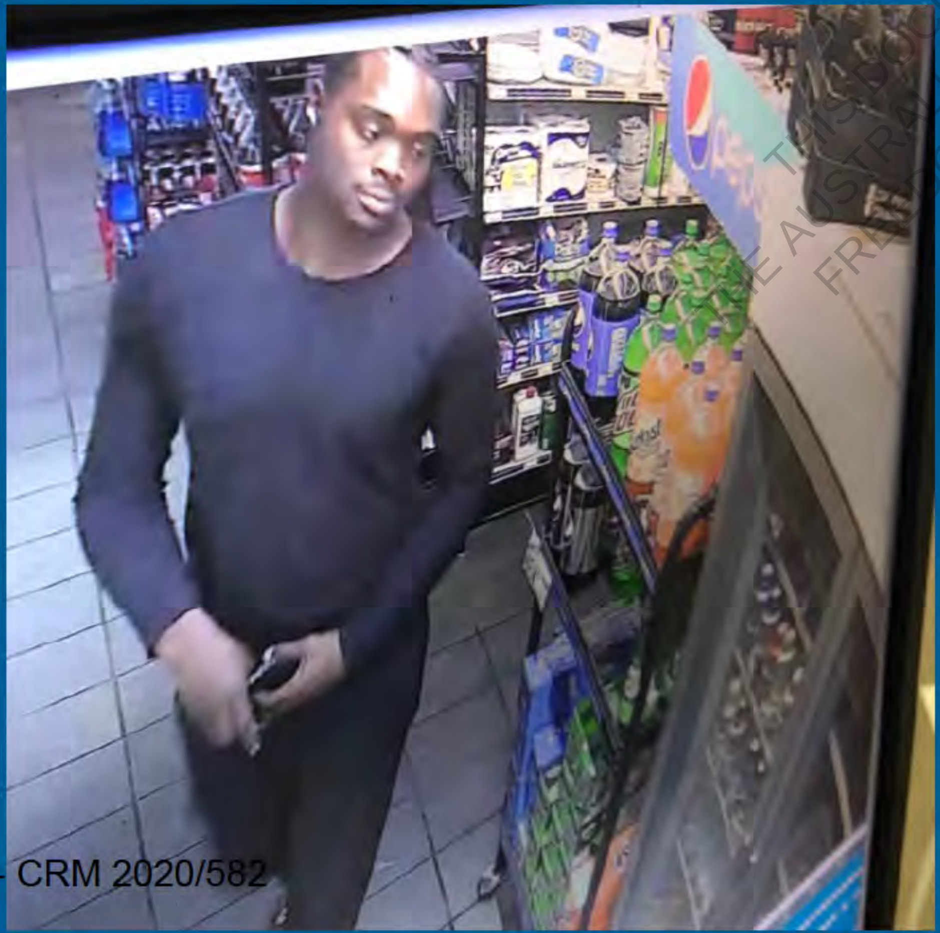


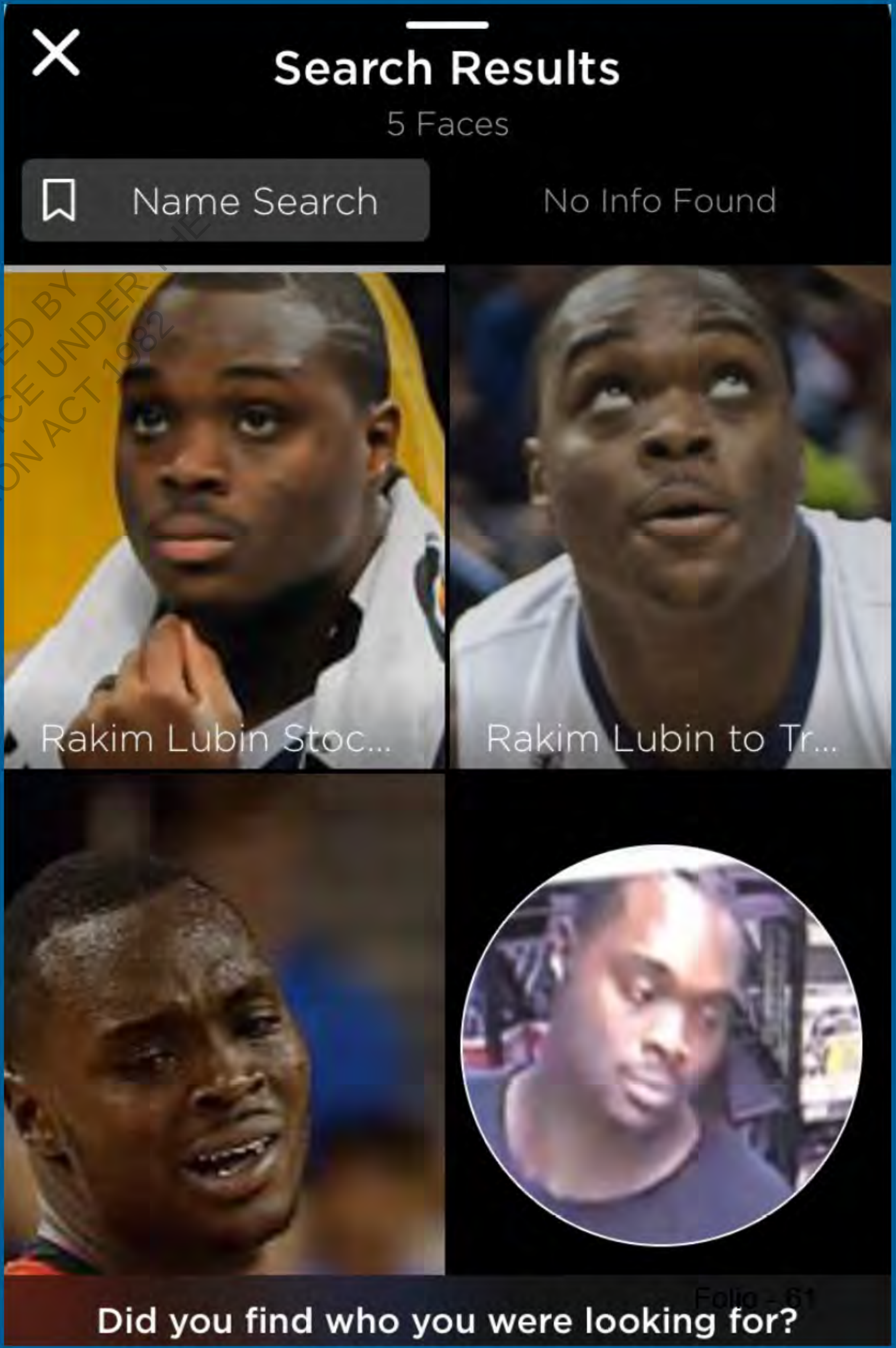


Robbery

Jacks Fast Food Robbed by masked gunman. When the suspect was arrested, he was still in possession of the Regions Bank bag the money was placed in during the robbery.







Search Results

5 Faces

Name Search

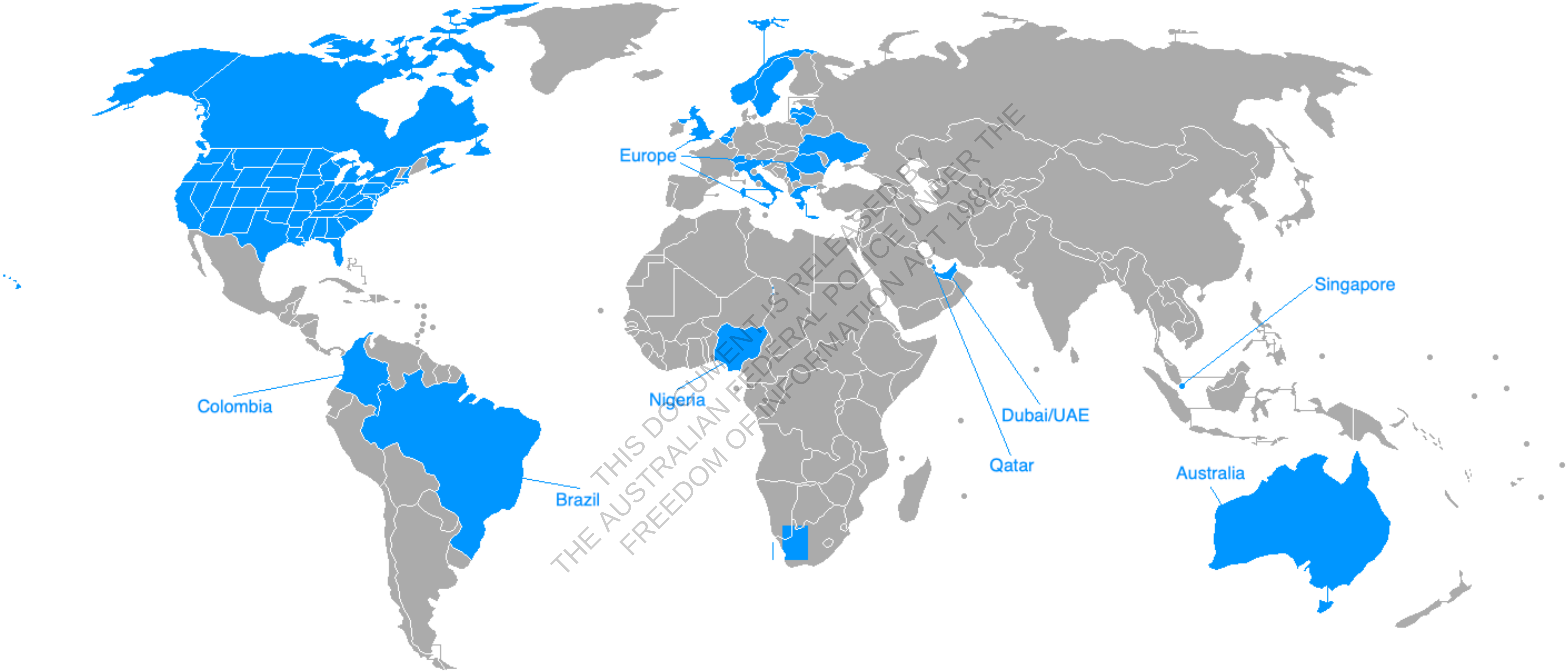
No Info Found

Rakim Lubin Stoc...

Rakim Lubin to Tr...

Did you find who you were looking for?

RAPID INTERNATIONAL EXPANSION



Clearview Ai

Stop Searching. Start Solving.

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 2 January 2020 10:14 AM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER
Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 9 December 2019 9:01 AM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47E(d) invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 9 December 2019 10:36 AM
To: s47E(d)
Subject: Please activate your Clearview account

Hi s47E(d)

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

What's Clearview?

Clearview is like **Google Search for faces**. Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single biggest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s47E(d)

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 9 December 2019 11:02 AM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER
Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 9 December 2019 11:02 AM
To: s47E(d)
Subject: Verify your email for Clearview

Hi s47E(d)

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/Im5pY29sZS53YXRraW5zQGFmcC5nb3YuYXUi.EM8ujw.cGPF5ahClGV-W-chZrhuPWcdNPs

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email

s47E(d) s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 4 December 2019 11:52 AM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER
Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Friday, 6 December 2019 9:55 AM
To: s47E(d)
Subject: You have been invited to Clearview

Follow Up Flag: Follow up
Flag Status: Flagged

Hi s47E(d)

s47E(d) invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 9 December 2019 11:36 AM
To: s47E(d)
Subject: Please activate your Clearview account

Hi s47E(d)

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single biggest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 9 December 2019 3:29 PM
To: s47E(d)
Subject: How to use Clearview

Hi s47E(d)

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.

2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.

3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER
Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.
Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.
Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.
Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Monday, 9 December 2019 3:29 PM
To: s47E(d)
Subject: Verify your email for Clearview

Hi s47E(d)

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/ImFseXNzYS5zdGFubGV5QGFmcC5nb3YuYXUi.EM9fCA.gH6ZxfXmIK69FrOafooRuNQh4g8

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email

s22(1)(a)(ii)

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> **On Behalf Of** Team Clearview
Sent: Wednesday, 18 December 2019 4:33 PM
To s47E(d) @afp.gov.au>
Subject: You have been invited to Clearview

Hi s47E(d)

s47E(d) invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

[redacted] s47E(d)
PERFORMING THE DUTIES OF SUPERINTENDENT CRIMES AGAINST CHILDREN
CRIME PROGRAM
Tel [redacted] s47E(d)
www.afp.gov.au

AFP
AUSTRALIAN FEDERAL POLICE

POLICING FOR
A SAFER AUSTRALIA

Sensitive

[redacted] s22(1)(a)(ii)

[redacted]

s22(1)(a)(ii)

Sensitive

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Friday, 6 December 2019 9:55 AM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47E(d) invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 4 December 2019 1:30 PM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47E(d) invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Tuesday, 21 January 2020 1:45 PM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47B invited you to Clearview!

To try it out for free please click the button below:

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s47E(d)

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Tuesday, 21 January 2020 12:50 PM
To: s47E(d)
Subject: You have been invited to Clearview

Hi s47E(d)

s47E(d) invited you to Clearview!

To try it out for free please click the button below:

What's Clearview?

Clearview is like **Google Search for faces.** Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources.

Our technology combines the **most accurate** facial identification software worldwide with the **single largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview