

Space & Astronomy | Jan 31, 2026 | 20 min read | By Bryan White

The Bio-Digital Checkpoint: Mobile Fortify and the Automated Governance of Public Space

AI * Ethics * Computing

1. Introduction: The Vertical Border and the dissolution of Sanctuary

In the contemporary landscape of American national security, the traditional conception of the border as a fixed geopolitical line -- a physical demarcation between sovereign states -- has become increasingly obsolete. It has been replaced by what political geographers and criminologists term the "vertical border" or the "ubiquitous border." In this paradigm, the border is not a place one crosses, but a status one carries. It adheres to the body of the non-citizen -- and increasingly the citizen -- manifesting wherever state power intersects with individual movement. The technological realization of this paradigm is "Mobile Fortify," a smartphone-based surveillance application deployed by Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP).

This report provides an exhaustive analysis of Mobile Fortify, tracing its operational mechanics, technical specifications, and profound ethical implications. Emerging from the shadows of bureaucratic obscurity through investigative leaks by 404 Media and Wired, and subsequently critiqued in The Guardian, Mobile Fortify represents a "techno-authoritarian" shift in domestic policing.[1] By tethering the immense data-processing power of the Department of Homeland Security's (DHS) backend architectures to the handheld devices of field agents, the state has effectively deputized the smartphone as a mobile biometric checkpoint.

The deployment of this technology, operational since at least May 2025, signifies a departure from reactive enforcement toward proactive, algorithmic population management.[1] Utilizing advanced facial recognition and contactless fingerprinting technologies provided by NEC Corporation, agents can now capture and verify identities in real-time, often without consent, in spaces previously considered insulated from federal immigration interdiction -- courthouses, schools, and city streets.[1] This report argues that Mobile Fortify is not merely an upgrade in enforcement efficiency but a fundamental restructuring of the relationship between the state and the individual, effectively converting public space into a domain of "e-carceration".[5]

2. The Technical Substrate: NEC Corporation and Biometric Capture

The efficacy and danger of Mobile Fortify lie in its technical sophistication. Unlike earlier iterations of mobile enforcement tools that relied on manual data entry or bulky peripheral scanners, Mobile Fortify leverages the native optical capabilities of standard government-issued smartphones combined with enterprise-grade biometric algorithms.

2.1 The Vendor Ecosystem: NEC Corporation

While initially obscured by DHS, the architecture of Mobile Fortify is built upon the intellectual property of NEC Corporation, a Japanese multinational and a global hegemon in biometric identification.[4] The DHS's 2025 AI Use Case Inventory explicitly identifies NEC as the vendor, linking the app to a broader ecosystem of surveillance contracts valued at millions of dollars.[7]

NEC's involvement is pivotal because of the specific pedigree of its algorithms. The company's flagship facial recognition suite, "NeoFace," has consistently ranked at the top of the National Institute of Standards and Technology (NIST) Face Recognition Vendor Tests (FRVT) for matching accuracy.[8] This algorithm is designed to perform "1:N" (one-to-many) identification, meaning it compares a single probe image against a gallery of millions to find a potential match, rather than simply verifying a claimed identity (1:1 matching).[8]

2.2 Facial Recognition Mechanics: The NeoFace Algorithm

The facial recognition component of Mobile Fortify operates by converting the human face into a mathematical vector.

- * Nodal Point Analysis: The software scans the "probe" image (the photo taken by the agent) to map specific landmarks or "nodal points" on the face -- the distance between the eyes, the width of the nose, the depth of the eye sockets, and the shape of the cheekbones.[8]

- * Vector Template Generation: These measurements are converted into a numerical string, or "faceprint." This template is unique to the algorithm; an NEC template cannot be read by a competitor's system (e.g., Clearview AI or IDEMIA) without conversion.[10]

- * Algorithmic Tolerance: A key selling point of NeoFace is its robustness in "unconstrained" environments. Traditional facial recognition fails when lighting is poor or the subject is not looking directly at the camera (off-pose). NEC claims its algorithm utilizes advanced pattern recognition to compensate for low-resolution images, video surveillance feeds, and partial occlusions.[9] This capability is critical for Mobile Fortify, which is designed for use "in the field" where studio lighting is absent and subjects may be uncooperative.[2]

2.3 Contactless Fingerprint Extraction

Perhaps more revolutionary than facial recognition is the app's "contactless" fingerprinting capability. Traditionally, fingerprinting required physical contact -- ink on paper or a finger pressed against a capacitive glass platen. Mobile Fortify breaks this physical barrier.

- * Visual-to-Biometric Conversion: Using the high-resolution camera of the smartphone, the app captures an image of the subject's hand. NEC's "contactless hybrid finger scanner" technology then processes this visual image.[12]

- * Minutiae Extraction: The algorithm inverts the visual data, identifying the ridges (the raised parts of the print) and valleys (the lower parts). It specifically locates "minutiae" -- the points where ridge lines end (ridge endings) or split

(bifurcations).[9]

* Standardization (FBI Appendix F): The app processes this visual data to meet the FBI's "Appendix F" Image Quality Specifications (IQS), which govern the fidelity required for law enforcement comparisons. This involves converting the 3D curvature of the finger seen by the camera into a flattened, 2D grayscale representation equivalent to a rolled ink print.[14]

* Hygiene and Speed: By removing the need for physical contact, the "hygienic" nature of the scan lowers the social and physical friction of the encounter. An agent does not need to touch the subject to "book" them; they merely need to photograph their hands.[12]

2.4 Comparison of Biometric Modalities in Mobile Fortify

The following table summarizes the technical distinctions between the two primary modalities employed by the app:

Feature	Facial Recognition (NeoFace)	Contactless Fingerprinting (NEC Hybrid)
Capture Mechanism	Smartphone Camera (Optical)	Smartphone Camera (Optical Macro)
Algorithm Basis	Nodal Point & Vector Analysis	Ridge Count & Minutiae Relation Method
Data Standard	ISO/IEC 19794-5 (Face)	FBI IQS Appendix F / NIST ITL
Primary Challenge	Lighting, Pose, Occlusion, Bias	Focus, Motion Blur, Scale Calibration
Interaction Type	Passive (can be covert)	Active (requires subject to present hands)
Database Link	HART / TVS / State Dept.	IDENT / NGI (FBI)
Error Vector	Demographic Bias (Race/Gender)	Environmental Noise / Image Quality
Source Citations	[8]	[12]

3. The Data Ecosystem: HART, "Super Query," and Encryption

The smartphone running Mobile Fortify is merely the sensory organ of a much larger organism. The cognitive center of this system is the Homeland Advanced Recognition Technology (HART), the massive biometric database currently replacing the legacy Automated Biometric Identification System (IDENT).

3.1 The HART Backend

HART is hosted in the Amazon Web Services (AWS) GovCloud, representing a modernization of DHS's biometric infrastructure.[16] It serves as the central repository for over 270 million digital identities, aggregating data from border crossings, visa applications, law enforcement encounters, and international data-sharing agreements.[6] When a Mobile Fortify user initiates a scan, the app

transmits the biometric template to HART. This transition from IDENT to HART is not merely administrative; it represents an expansion of capability. HART is designed to be "multimodal," capable of fusing face, finger, iris, and potentially DNA and voice data into a single "digital person" profile.[16]

3.2 The "Super Query" Capability

Upon a successful match -- or even a manual query -- Mobile Fortify enables a function known as the "Super Query." This feature, detailed in DHS use case inventories and coalition letters, allows the agent to pull a cascading array of non-biometric data linked to the identity.[18]

The "Super Query" acts as a meta-search engine across federated government databases. It does not simply return a name; it returns a life.

- * Immigration & Travel: It queries the Automated Targeting System (ATS) and Traveler Verification Service (TVS) to reveal visa status, border crossing history, and travel patterns.[6]

- * Assets & Movement: It connects to databases tracking vehicles, vessels, and aircraft, likely integrating license plate reader (LPR) data to map the subject's physical movements.[19]

- * Social Graphing: The query can retrieve associated addresses, phone numbers, and known associates, effectively mapping the subject's social network.[20]

- * Intelligence Integration: There are indications that the system feeds into and pulls from intelligence reporting systems, potentially flagging individuals based on "derogatory information" or "officer comments" from previous encounters.[17]

3.3 Security Architecture and FIPS 140-2 Compliance

Given the sensitivity of transmitting biometric templates and personally identifiable information (PII) over cellular networks, Mobile Fortify is mandated to adhere to the Federal Information Processing Standard (FIPS) 140-2.[23]

- * Encryption Standards: FIPS 140-2 validation requires that the cryptographic modules used by the app meet strict federal benchmarks. This likely involves AES-256 (Advanced Encryption Standard) for data at rest (cached on the phone) and TLS 1.2/1.3 (Transport Layer Security) for data in transit to the AWS GovCloud.[25]

- * Module Validation: The "crypto-module" within the Samsung or Apple devices used by ICE must be certified. If the module is not in "FIPS mode" or uses non-compliant algorithms (like standard Diffie-Hellman without specific curve parameters), the device is technically non-compliant.[25]

- * The Privacy Paradox: While these encryption standards protect the data from external hackers (confidentiality), they do not protect the subject from the state (privacy). The rigorous application of FIPS 140-2 ensures that the government's surveillance network is secure for the government, ensuring the integrity of the data used to prosecute and deport, but offering no solace to the individual whose data is non-consensually harvested.

4. Operational Deployment: The "Roving Patrol" Model

The operational doctrine of Mobile Fortify is one of "forward deployment." By liberating biometric verification from the fixed infrastructure of the booking station, ICE has enabled a tactical shift toward "roving patrols" in the U.S. interior.[1]

4.1 The Chicago and Illinois Context

The practical application of this doctrine is vividly illustrated in the lawsuit filed by the State of Illinois and the City of Chicago in January 2026. The complaint describes a "lawless organized bombardment" of Chicago neighborhoods, where federal agents armed with Mobile Fortify conduct aggressive street stops.[1]

* Sensitive Locations: Agents have been documented operating near schools, medical facilities, and courthouses -- zones typically treated as "sensitive locations" where enforcement is deprioritized to avoid disrupting essential services.[1]

* The "Check" as Intimidation: The mere presence of the app changes the dynamic of a stop. An agent no longer needs to bring a suspect to a station to verify their identity. They can do it on the sidewalk. This capability is allegedly being used to scan "random people of color," utilizing the app as a tool of racial filtering rather than targeted enforcement.[1]

4.2 The "Consent" Fallacy

A critical ethical and legal failure of Mobile Fortify is the absence of meaningful consent. Internal DHS documents obtained by 404 Media state unequivocally: "ICE does not provide the opportunity for individuals to decline or consent to the collection and use of biometric data/photograph collection".[2]

This policy creates a coercive environment. When an armed federal agent "aims a phone" at a subject, the power asymmetry renders the concept of "opting out" theoretical at best.[1] The speed of the technology -- capturing a face in milliseconds -- means the data is often collected before the subject can verbally object or physically turn away. This "drive-by" biometrics capability transforms the human face into a constantly readable license plate.

4.3 Data Retention: The Forever Lineup

Perhaps the most egregious operational detail is the retention policy. According to the Guardian, every photograph or fingerprint taken by Mobile Fortify -- regardless of whether it matches a suspect or is completely innocent -- is stored in the Automated Targeting System (ATS) for 15 years.[1] This practice effectively builds a "forever lineup." An innocent individual scanned during a protest or a random stop is entered into the criminal/immigration intelligence ecosystem for a decade and a half. Their biometrics become available for future "1:N" searches, increasing their exposure to potential false positives in subsequent investigations.

5. Algorithmic Bias and the Crisis of Accuracy

The reliance on facial recognition for "definitive" status determinations presumes a level of technological infallibility that does not exist. The deployment of Mobile

Fortify rests on a foundation of algorithms that have been proven, repeatedly, to harbor significant demographic biases.

5.1 The "Gender Shades" Reality

The landmark "Gender Shades" study by Joy Buolamwini and Timnit Gebru provides the empirical baseline for understanding the risks of Mobile Fortify. The study audited commercial facial analysis algorithms and found that error rates were not distributed equally across the population.[1]

* The Intersectional Gap: While algorithms from major tech companies achieved near-perfect accuracy (0.0% - 0.8% error rates) on light-skinned males, they failed catastrophically on darker-skinned females, with error rates reaching as high as 34.7%.[1]

* The Training Data Problem: This disparity is a result of "data bias." The algorithms are trained on datasets that are overwhelmingly male and light-skinned (e.g., the IJB-A benchmark was 79.6% light-skinned).[1] The algorithm effectively "learns" the features of white men with high fidelity but treats the features of Black women as noise or anomalies.

5.2 NEC and the Real-World Performance Gap

While NEC claims superior accuracy for its NeoFace algorithm, these claims are often based on NIST benchmarks conducted on static, high-quality mugshots. Operational reality is different. "In the wild" facial recognition -- performed via a handheld phone, on a moving street, with variable lighting -- introduces noise that exacerbates underlying biases.

* Environmental Degradation: Shadows, glare, and off-angle poses (yaw, pitch, roll) degrade the "nodal point" map. When the algorithm is already less sensitive to darker skin tones (due to lower contrast and poor training representation), these environmental factors cause error rates to spike further for people of color.[11]

5.3 Case Study: Nijeer Parks and the False Positive

The danger of algorithmic reliance is not hypothetical. The case of Nijeer Parks serves as a warning for the Mobile Fortify era.

* The Incident: Parks, a Black man, was identified by a facial recognition system as a shoplifting suspect.

* The Consequence: Despite being 30 miles away at the time of the crime, he was arrested and jailed for 10 days.[1] The police and prosecutors treated the algorithmic match as "probable cause," ignoring the lack of physical evidence linking him to the scene.

* The Precedent: Parks' case illustrates "automation bias" -- the psychological tendency of humans to trust automated systems over their own judgment or contradictory evidence. When Mobile Fortify alerts an ICE agent to a "match," the agent is conditioned to accept the machine's verdict as truth.

5.4 Case Study: The Oregon Misidentification

Investigative reporting by 404 Media uncovered a specific failure of Mobile Fortify that confirms these fears. During an immigration raid in Oregon, agents used the app to scan a detained woman. The system failed to identify her correctly; instead, it returned two different names, both incorrect.[1] This incident fundamentally undermines ICE's assertion that the app provides a "definitive" determination of status. If agents had relied solely on the app, they would have been pursuing two "phantom" identities, potentially detaining the woman under a false name or harassing the innocent individuals whose names were erroneously returned.

6. Theoretical Frameworks: E-Carceration and Techno-Authoritarianism

To understand Mobile Fortify solely as a law enforcement tool is to miss its broader sociological significance. It represents a shift in the philosophy of governance, moving from physical confinement to digital control.

6.1 From Decarceration to E-Carceration

Legal scholar Chaz Arnett provides a critical framework for this transition in his work "From Decarceration to E-Carceration." Arnett argues that while modern penal reforms often aim to reduce the number of people in physical prisons ("decarceration"), they often replace physical bars with digital shackles.[5]

* The Digital Prison: Mobile Fortify is an instrument of this "e-carceration." It allows the state to extend the "carceral net" over entire communities. An undocumented immigrant -- or a citizen targeted by error -- living under the threat of Mobile Fortify is effectively in a prison without walls. Their movements are tracked ("Super Query"), their identity is constantly audited, and their freedom is contingent on the algorithmic verification of the state.[5]

* Net-Widening: Far from reducing the footprint of the state, technologies like Mobile Fortify "widen the net." They bring more people under surveillance than could ever be physically detained. The cost of scanning a thousand people is negligible compared to the cost of jailing them, encouraging mass-scale monitoring.[5]

6.2 The Techno-Authoritarian Nightmare

The Guardian characterizes Mobile Fortify as a "techno-authoritarian nightmare".[1] This critique draws on the inversion of democratic transparency.

* The Transparency Inversion: In a democracy, the government is supposed to be transparent (public records, open proceedings) while the citizen retains privacy. Mobile Fortify inverts this: the government's algorithms and databases (HART/ATS) are black boxes, protected by "law enforcement sensitivity" and proprietary trade secrets [31], while the citizen is rendered transparent. The state sees everything; the citizen sees nothing.[1]

* The Panopticon Effect: This asymmetry creates a Panopticon effect. The citizen does not need to be scanned every day to feel the pressure of the system. The possibility that any agent with a phone could scan them at any moment enforces a disciplining power, chilling dissent, political organization, and free movement.[1]

6.3 Social Stratification and Marginalization

Arnett further argues that this surveillance is not applied universally but is a tool of "social stratification." It disproportionately targets "historically subordinated groups".[5] Mobile Fortify is not being deployed in affluent, predominantly white suburbs to check for visa overstays. It is deployed in Chicago neighborhoods, at protests, and near border zones. It reinforces racial hierarchies by subjecting specific populations to a level of biometric scrutiny that the dominant culture does not experience.[5]

7. Legal and Constitutional Crises

The deployment of Mobile Fortify has precipitated a collision between 21st-century technology and 18th-century constitutional law.

7.1 The Tenth Amendment and State Sovereignty

The lawsuit filed by Illinois and Chicago challenges the federal government's intrusion into state affairs.

- * The Argument: The plaintiffs argue that the "occupation" of Chicago by federal agents wielding Mobile Fortify violates the Tenth Amendment, which reserves powers not delegated to the federal government to the states.[1]

- * Impeding State Functions: By creating a climate of fear, federal agents are allegedly impeding the state's ability to provide essential services -- education, health, safety. If parents are afraid to take their children to school because agents are scanning faces at the bus stop, the federal government is actively dismantling the state's educational mandate.[1]

7.2 The Fourth Amendment: Search and Seizure

The most direct constitutional challenge lies in the Fourth Amendment. Is a facial scan a "search"?

- * Warrantless Biometrics: The "Biometric Scanning Policy" challenged in the lawsuit involves capturing biometrics without a warrant or probable cause.[1] While the Supreme Court has not definitively ruled on mobile facial recognition in public, the non-consensual capture of intimate biometric data -- which reveals identity, movement, and potentially health data -- arguably constitutes an unreasonable search.

- * The "Definitive" Determination: DHS's position that a Mobile Fortify match is "definitive" raises Due Process concerns.[1] If a machine's probability score can override a birth certificate, the citizen is stripped of their right to present evidence and confront their accuser. The accuser is an algorithm, and the evidence is a proprietary source code that the defendant is not allowed to see.

7.3 The Legislative Vacuum

A recurring theme in the critique of Mobile Fortify is the lack of legislative authorization. The ACLU notes that Congress never explicitly authorized DHS to use facial recognition for widespread interior enforcement.[1] The agency is operating

in a "legislative vacuum," repurposing authorities granted for border security (like the TVS system for airports) and applying them to domestic policing without debate or oversight.[2]

8. Comparative Analysis: Mobile Fortify vs. Electronic Monitoring

To understand the specific niche of Mobile Fortify, it is useful to compare it with other "e-carceration" tools, specifically the SmartLINK app and traditional ankle monitors.

| Feature | | Mobile Fortify | | SmartLINK (ICE) | | Ankle Monitor (GPS) |

| Target Audience | | General Public / Suspected Undocumented | | Individuals in Removal Proceedings (ATD) | | High-Risk Parolees / Detainees |

| Trigger Mechanism | | Agent-Initiated (Random/Targeted Stop) | | Schedule-Initiated (Check-in) | | Continuous (Always On) |

| Biometric Capture | | Face & Fingerprint (Live Scan) | | Face & Voice (Self-Report) | | GPS Location (Passive) |

| Surveillance Logic | | Identification (Who is this?) | | Compliance (Are you where you said?) | | Restriction (Stay in zone) |

| Data Scope | | "Super Query" (All linked gov data) | | Location & biometric verification | | Location history |

| Consent | | Non-Consensual / Coercive | | "Voluntary" alternative to detention | | Mandated by court |

| Ethical Risk | | Random stops, racial profiling, "forever lineup" | | Privacy invasion, false check-in failures | | Physical discomfort, stigma, battery anxiety |

Analysis: While SmartLINK and ankle monitors are tools of supervision for people already in the system, Mobile Fortify is a tool of acquisition. It is the dragnet used to pull people into the system. It represents the front-end of the e-carceration pipeline, whereas SmartLINK represents the maintenance phase.[27]

9. Conclusion: The Fork in the Road

The emergence of Mobile Fortify marks a critical juncture in the history of American civil liberties. We stand at a fork in the road.

One path leads to the normalization of the "biometric checkpoint society".[2] In this future, the vertical border is omnipresent. The distinction between citizen and suspect dissolves, replaced by a universal status of "scannable entity." Anonymity in public space is extinguished, and the government possesses a real-time, algorithmic map of the population, curated by vendors like NEC and hosted on the servers of Amazon. In this world, the "Super Query" becomes the ultimate arbiter of truth, capable of overriding physical documentation and human testimony.

The alternative path, championed by the plaintiffs in Illinois and civil liberties advocates, demands a reassertion of democratic control over technology. It requires legislative "firewalls" that prevent the importation of border enforcement tools into domestic policing. It demands the "abolition" of tools that automate racial bias and the strict prohibition of non-consensual biometric capture.[1]

As the algorithms of Mobile Fortify continue to learn, process, and store the faces of the American public, the window for choosing this second path is rapidly closing. The app is not merely a piece of software; it is a constitution-level event, rewriting the compact between the government and the governed in lines of code.

Appendix A: Summary of Key Legal and Technical Documents

- * DHS 2025 AI Use Case Inventory: Identified NEC Corporation as the vendor for Mobile Fortify.[6]
- * State of Illinois v. DHS (Case: 26-cv-321): Lawsuit alleging 10th Amendment and APA violations due to "roving patrols" and biometric scanning.[1]
- * "Gender Shades" (Buolamwini & Gebru, 2018): Academic study establishing the 34.7% error rate for darker-skinned females in facial analysis systems.[1]
- * 404 Media / Wired Reports: Investigative journalism by Joseph Cox uncovering the leaked user manuals, the "Super Query" functionality, and the Oregon misidentification incident.[1]
- * DHS Privacy Impact Assessment (HART): Detailed the transition from IDENT to HART and the scale of the 270-million-person database.[16]

Works Cited

- * ICE's surveillance app is a techno-authoritarian nightmare ..., accessed January 30, 2026, <https://www.theguardian.com/commentisfree/2026/jan/30/ice-surveillance-app-mobile-fortify-authoritarian>
- * How ICE is using facial recognition in Minnesota, accessed January 30, 2026, <https://www.theguardian.com/technology/2026/jan/27/ice-facial-recognition-minnesota>
- * Bitwarden Raises Prices, Microsoft Hands Over Encryption Keys, ICE's Numerous Privacy Concerns, and more!, accessed January 30, 2026, <https://www.privacyguides.org/livestreams/2026/01/23/bitwarden-raises-prices-microsoft-hands-over-encryption-keys-ices-numerous>
- * ICE facial recognition app Mobile Fortify powered by NEC - Biometric Update, accessed January 30, 2026, <https://www.biometricupdate.com/202601/ice-facial-recognition-app-mobile-fortify-powered-by-nec>
- * "From Decarceration to E-Carceration" by Chaz Arnett, accessed January 30, 2026, <https://larc.cardozo.yu.edu/clr/vol41/iss2/5/>
- * Mobile Fortify - Wikipedia, accessed January 30, 2026, https://en.wikipedia.org/wiki/Mobile_Fortify
- * DHS Reveals Tech Giant Behind ICE's Controversial Face-Scanning App, accessed January 30, 2026, <https://www.gadgetreview.com/dhs-reveals-tech-giant-behind-ices-controversial-face-scanning-app>
- * Smart Access - NEC Corporation of America, accessed January 30, 2026, https://www.necam.com/en_US/necns/access/index.html
- * Fingerprint Identification: Biometric Authentication - NEC Corporation, accessed January 30, 2026, <https://www.nec.com/en/global/solutions/biometrics/fingerprint/index.html>

- * NeoFace Reveal - NEC Corporation of America, accessed January 30, 2026,
https://www.necam.com/en_US/docs/NeoFaceReveal_SalesSheet_NECNSS.pdf
- * Understanding bias in facial recognition technologies - The Alan Turing Institute, accessed January 30, 2026,
https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf
- * NEC Contactless Hybrid Finger Scanner - NEC Corporation - Asmag.com, accessed January 30, 2026,
https://www.asmag.com/suppliers/productcontent.aspx?co=nec_corp&id=26660
- * hs100 10 | PDF | Art - Scribd, accessed January 30, 2026,
<https://www.scribd.com/document/82332875/hs100-10>
- * NEC NEOSCAN 45 Mobile Fingerprint Device - Biometric Solutions, accessed January 30, 2026, <https://www.mosaglobal.com/NEC-2-Finger-Mobile-Capture-Device-p/neo45.htm>
- * NeoScan 45 - NEC Corporation, accessed January 30, 2026,
https://www.nec.com/en/global/solutions/safety/pdf/NeoScan_45_Brochure.pdf
- * Privacy Impact Assessment Homeland Advanced Recognition Technology System (HART), accessed January 30, 2026,
https://www.dhs.gov/sites/default/files/2024-08/24_0826_priv_pia-obim-004a-HART-update.pdf
- * Homeland Advanced Recognition Technology (HART): DHS is Building a Massive Database of Personal Information - The National Immigration Law Center, accessed January 30, 2026,
<https://www.nilc.org/wp-content/uploads/2021/12/HART-factsheet-2021-11-10.pdf>
- * Coalition warns DHS that ICE's Mobile Fortify facial recognition app poses serious civil liberties risks, accessed January 30, 2026,
<https://cadeproject.org/updates/coalition-warns-dhs-that-ices-mobile-fortify-facial-recognition-app-poses-serious-civil-liberties-risks>
- * Use Cases - Homeland Security, accessed January 30, 2026,
https://www.dhs.gov/sites/default/files/2026-01/2025_0128_ocio-dhs-ai-use-case-inventory.xlsx
- * Letter to ICE on Mobile Facial Recognition Tech - Senator Edward Markey of Massachusetts, accessed January 30, 2026,
<https://www.markey.senate.gov/download/letter-to-ice-on-mobile-facial-recognition-tech/>
- * Homeland Security - U.S. Customs and Border Protection, accessed January 30, 2026,
https://www.cbp.gov/sites/default/files/2024-08/pta_-_cbp_tvs-internal.pdf
- * 1 November 25, 2025 Chief Privacy Officer Roman Jankowski Department of Homeland Security 2707 Martin Luther King Jr. AVE SE Was - Epic.org, accessed January 30, 2026,
<https://epic.org/wp-content/uploads/2025/11/Coalition-Letter-on-ICE-Mobile-Fortify-FRT-Nov2025.pdf>
- * FIPS 140-2 Encryption: Standards and Use Cases | Digi International, accessed January 30, 2026,
<https://www.digi.com/blog/post/the-fips-140-2-standard-and-use-cases>
- * General Rules of Behavior for Users of DHS Systems and IT Resources that Access, Store, Receive, or Transmit Sensitive Information - ICE, accessed January 30, 2026,
<https://www.ice.gov/doclib/sevis/pdf/behavior-rules.pdf>

* FIPS 140-2 Security Policy - CSRC, accessed January 30, 2026,
<https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1985.pdf>

* OIG - 12 - 88 DHS Needs To Address Portable Device Security Risks - GovInfo,
accessed January 30, 2026,
<https://www.govinfo.gov/content/pkg/GOVPUB-HS-PURL-gpo48840/pdf/GOVPUB-HS-PURL-gpo48840.pdf>

* Face Recognition and the 'Trump Terror': A Marriage Made in Hell | ACLU, accessed
January 30, 2026, <https://www.aclu.org/news/privacy-technology/ice-face-recognition>

* Parks v. McCormac | American Civil Liberties Union, accessed January 30, 2026,
<https://www.aclu.org/cases/parks-v-mccormac>

* How Face Recognition Technology Landed One Innocent Man in New Jersey Jail for Ten
Days, accessed January 30, 2026,
<https://www.aclu-nj.org/news/how-face-recognition-technology-landed-one-innocent-man-new-jersey-jail-ten-days/>

* Is E-Carceration a Problem? Confronting the Shortcomings of Technological Criminal
Justice Reforms, accessed January 30, 2026,
<https://crim.jotwell.com/is-e-carceration-a-problem-confronting-the-shortcomings-of-technological-criminal-justice-reforms/>

* Department of Homeland Security intensifies surveillance in immigration raids,
sweeping in citizens | PBS News, accessed January 30, 2026,
[https://www.pbs.org/newshour/politics/departments-of-homeland-security-intensifies-surveillance-in-immigration-raids-sweeping-in-](https://www.pbs.org/newshour/politics/departments-of-homeland-security-intensifies-surveillance-in-immigration-raids-sweeping-in-citizens/)

* Rights Organizations Demand Halt to Mobile Fortify, ICE's Handheld Face
Recognition Program | Electronic Frontier Foundation, accessed January 30, 2026,
<https://www.eff.org/deeplinks/2025/11/rights-organizations-demand-halt-mobile-fortify-ices-handheld-face-recognition>