

Privacy Implications of the Meta Ray-Ban AI Smart Glasses

in the SWANA Region, and Technical Methods
for Detection

A research and advisory briefing for civil society, journalists, and human rights defenders

Author: Ragheb Ghandour



Executive Summary

Meta's Ray-Ban smart glasses have entered a region that is already a global epicenter of targeted digital surveillance, and they do so in the form of a fashionable, difficult-to-detect, face-worn camera. SMEX developed this briefing based on two bodies of evidence. The DFRWS USA 2026 forensic study of the Ray-Ban Meta ecosystem ^[1], which documents exactly what these glasses and their companion app capture and retain, and the regional human-rights context in which that capture becomes dangerous. We then examine concrete, technology-based methods available for detecting the glasses in the field, and assess which of them are actually effective.

Three findings emerged from this briefing. First, surveillance is among the capabilities present in Meta's smart glasses. The forensic examination recovers device serial numbers, Bluetooth MAC and pairing histories (the unique hardware IDs that tie the glasses to a particular phone), GPS coordinates embedded in video, plaintext AI queries (the questions asked of the assistant and stored as readable, unencrypted text), and on-device PyTorch face-detection models (face-finding software built into the app) ^[1]. Civil-society researchers separately found dormant facial-recognition code ("NameTag") already shipped to roughly 50 million phones ^[23, 25]. Second, captured data leaves the SWANA region by design. In April 2025, Meta enabled cloud AI collection by default^[8], and footage resulting from it was routed to human reviewers in Nairobi, which included intimate material ^[9, 11]. Third, the balance currently favors the recorder as the most reliable method to detect the presence of the glasses, while Bluetooth Low Energy fingerprinting (identifying the glasses by the faint wireless signal they broadcast), works well only when the glasses are switched on and first linked to a phone ^[26]. The recording LED can be permanently disabled by a hardware mod that costs USD 50-100 ^[33], while optical detection performs poorly on this specific device ^[26].

For at-risk communities like women, LGBTQ+ people, journalists, activists, and minorities, the combination of high impact and weak legal recourse makes these glasses a disproportionate threat. The recommendations that close this briefing therefore treat detection as advisory rather than protective, and we lean on enforced no-recording policies, behavioral awareness, and partnership with regional digital-rights organizations.

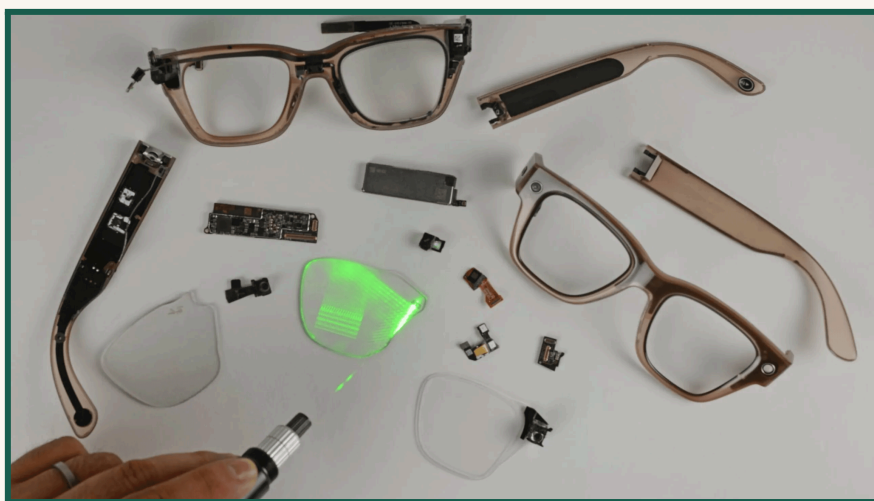


Figure 1 - Meta Ray-Ban Display Teardown ([iFixit](#))

1. The Forensic Foundation (DFRWS USA 2026)

We build this briefing on “Seeing the Evidence: A Forensic Framework for Analyzing Ray-Ban Meta AI Smart Glasses,” authored by Shishir Panta, Ruba Alsmadi, and Ibrahim (Abe) Baggili of the BiT Lab at Louisiana State University and presented at DFRWS USA 2026 ^[1, 2]. The paper establishes a three-layer glasses, companion, cloud forensic model and formalizes how evidence is distributed, correlated, and attributed across those layers. Through privileged filesystem acquisition (extracting the app’s private files using elevated, admin-style access) of the Android companion application and correlation with Meta cloud exports, it documents a rich set of artifacts inside the *com.facebook.stella* sandbox (the private storage area the Meta AI app keeps on the phone).

1.1 What the ecosystem captures and retains

The paper’s artifact taxonomy maps directly onto the surveillance concerns we raise below.

Artifact category	Representative artifacts (per DFRWS Table 4)
Identity	User ID, username, account ID, profile picture; device serial number; Bluetooth MAC addresses; device UUID and pairing history; synced Messenger/Instagram contacts.
Media	Raw, processed, and thumbnail photos and videos; IMU motion-sensor (accelerometer/gyroscope) data; capture timestamps bound to the device serial and pairing ID.
Geolocation	GPS latitude/longitude embedded in video captures (observed for videos, not photos), enabling movement reconstruction.
AI interaction logs	Conversation states, response text, unique session ID codes; user questions and AI responses stored in readable text in a temporary data cache; voice-command details; links from AI visual queries to capture sessions and the device serial.
On-device AI models	PyTorch machine-learning models for Face Detection, Classifier, and Occlusion; the instructions and configuration for the built-in AI assistant.
Anti-forensic persistence	Serial number immutable across all actions; pairing MAC rotates on reset; reminders and cloud transcripts survive local deletion, leaving secondary evidence of the deletion itself.

Two properties matter most for the regional threat model we use. The presence of on-device face-detection models ^[1] shows that the hardware is already provisioned for facial analysis, and this corroborates the separate civil-society discovery of dormant facial-recognition code we discuss in **Section 2**. The anti-forensic results show that a careful user’s deletion, unpairing, or factory reset reduces but does not eliminate the trail ^[1]. In our reading this cuts both ways as it aids accountability for a victim seeking to prove they were recorded, but it also means an activist’s own device can betray sources, locations, and timelines even after a wipe.

On scale, the paper reports over two million units sold by early 2025 ^[1]. That figure has since grown extensively. Ray-Ban's maker EssilorLuxottica reported that sales of AI-glasses have more than tripled in 2025, selling over seven million units that year ^[3], pushing cumulative sales toward roughly 9 million dollars and turning a niche gadget into a population-level capture surface.

2. SWANA Regional Privacy Implications

2.1 A pre-existing surveillance emergency

The SWANA/MENA region is the most heavily documented theatre of commercial-spyware abuse in the world. Citizen Lab's tracking of NSO Group's Pegasus identified suspected operators across Algeria, Bahrain, Egypt, Jordan, Morocco, Saudi Arabia, Tunisia, and the UAE ^[4], and the tool has been tied to the targeting of dissidents and journalists including associates of Jamal Khashoggi ^[5,6]. In "The Great iPwn," Citizen Lab found that operatives used Pegasus to compromise 36 personal phones of Al Jazeera journalists and executives, attributing distinct operator clusters to Saudi Arabia and the UAE ^[7]. Separately, Intellexa/Cytrox's Predator spyware was confirmed against exiled Egyptian targets ^[4]. A mainstream, deniable, face-worn camera does not replace this apparatus. In our assessment, it extends it, normalizing ambient capture by ordinary people that can feed the same repressive machinery.

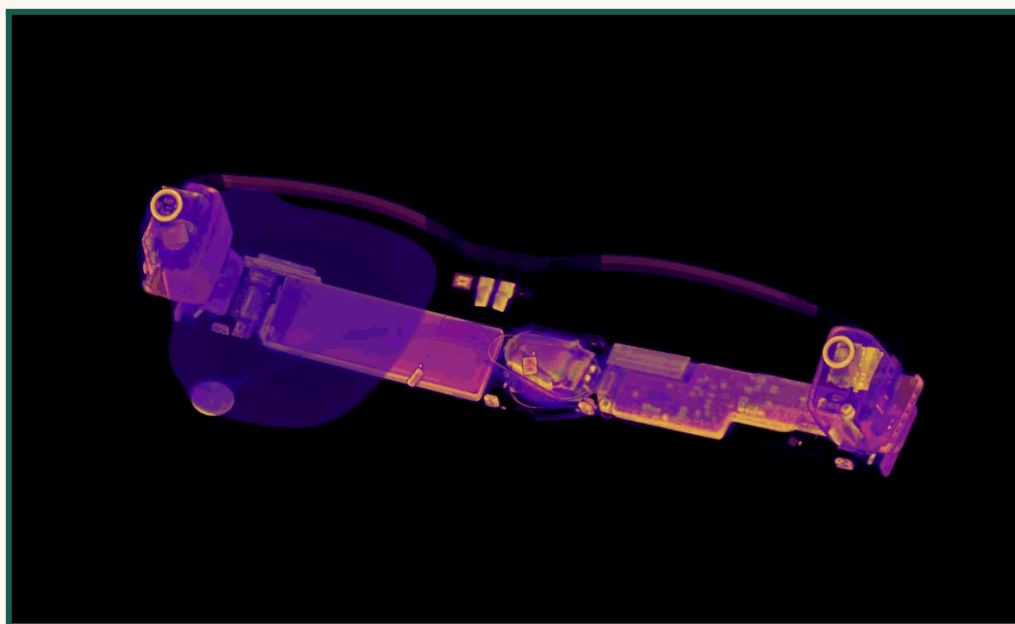


Figure 2 - RayBan Meta Sunglasses electronic components scan - [Voyager Lumafield](#)

2.2 Data leaves the region, by design and by default

Meta's April 2025 policy change made "Meta AI with camera" enabled by default and began storing voice interactions in the cloud by default, with no opt-out, retained for up to a year ^[8]. A joint Swedish press investigation then revealed that footage was being reviewed by human annotators at a Meta subcontractor in Nairobi, Kenya, and that

footage included deeply sensitive and intimate material ^[9, 10]. Meta terminated the contract around May 2026, and Kenya's data-protection regulator opened a probe ^[11, 12]. For the SWANA users we advise, and for the non-consenting bystanders they film, this means covertly captured images can be transferred, cloud-processed, and human-reviewed thousands of kilometers away, entirely outside any regional legal protection.

2.3 Data-protection law exists on paper but offers thin recourse

Most states in the region now have data-protection statutes, including Saudi Arabia's Personal Data Protection Law (PDPL) and the UAE's PDPL, alongside separate data-protection regimes in the DIFC and ADGM, the UAE's financial free zones. Other examples include Egypt's Law No. 151 of 2020, whose executive regulations were issued in November 2025; Bahrain's Law No. 30 of 2018; and Morocco's Law No. 09-08. ^[13, 14, 15] In practice, we observe three structural gaps that neutralize these laws in the smart-glasses scenario: broad national-security exemptions that shield state surveillance; nascent or unpublished cross-border-transfer regimes, meaning that transfers to Meta's US and EU servers face little scrutiny ^[15]; and the near-total absence of a practical remedy for a bystander recorded without consent by a private individual using a foreign company's product ^[16].

2.4 Vulnerable populations face amplified, sometimes life-threatening risks

Human Rights Watch documented security forces in Egypt, Iraq, and Jordan entrapping LGBTQI+ people through fake dating-app profiles, leading to arbitrary arrest, torture, and sexual assault, with illegitimately obtained digital photos used as prosecution evidence ^[17, 18, 19]. In this context we regard covert facial capture and identification via glasses as potentially catastrophic.

The covert filming of women is the single most-documented real-world abuse of these glasses. In May 2025, Spanish authorities arrested a man in Barcelona who used the Ray-Ban Meta glasses to secretly record roughly 329 videos of women ^[20], and a 2026 BBC investigation found numerous accounts of filming women without consent, in one case exposing a victim's phone number to over a million viewers ^[21, 32]. The device has earned the nickname of "pervert glasses" ^[33]. In the SWANA region particularly and in other honor-based-violence contexts, a single covert image of a woman can be weaponized for extortion or family violence. In addition, several Gulf states already criminalize photographing individuals without consent, which underscores the gravity attached to non-consensual imaging ^[22].

At last, for the people we support who are already targeted by Pegasus and Predator, a covert camera in a meeting or at a protest adds a deniable capture channel that can identify sources and map networks ^[4, 7].

2.5 Facial recognition is imminent, not hypothetical anymore

The Harvard I-XRAY proof-of-concept (October 2024) was able to pair commercial Ray-Ban Meta glasses with a face-search engine and language models to identify strangers and pull names, addresses, and phone numbers in under a minute. Then, in June 2026, EFF's Threat Lab researchers discovered dormant facial-recognition code, internally called "NameTag," already shipped through the Meta AI companion app to roughly 50 million phones ^[23, 25]. The pipeline used face detection, conversion of each face into a faceprint of 2,048 numbers (a numeric code that stands in for a person's face), and matching against a stored database. An EFF technologist was able to activate it in debug mode, judged it nearly ready, and warned it would turn wearers into a distributed surveillance network ^[23, 24].

This maps precisely onto the on-device face-detection models recovered in the DFRWS forensic study ^[1], and in our reading, the forensic evidence and the civil-society evidence corroborate each other.

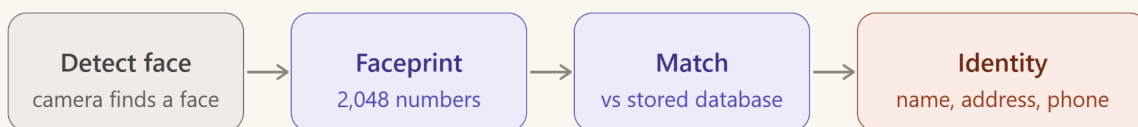


Figure 4 - Demonstrated on strangers in under a minute (Harvard I-XRAY). shipped dormant as "NameTag"

2.6 Availability and regional posture

Ray-Ban Meta glasses are now widely sold across the Gulf, and even formally launched in the UAE launch in 2025, even if the rollout was reportedly delayed due to strict regional photography and cybersecurity laws ^[22]. We found no comprehensive regional ban, but photography law in several states nominally criminalizes non-consensual imaging but is rarely enforceable in practice against tourists or users ^[22].

2.7 Regional digital-rights defenders

SMEX runs regional legal databases and convenes the MENA Alliance for Digital Rights (MADR) ^[16]; Access Now and its MENA policy team and Digital Security Helpline provide advocacy and direct technical support ^[18]; 7amleh focuses on Palestinian digital rights; and Masaar in Egypt works on digital rights, cybersecurity, and legal reform. Other regional and international organizations such as Citizen Lab, Amnesty International's Security Lab, and EFF, whose forensic and code-analysis work underpins much of the evidence we rely on above ^[4, 7, 23].

3. Technical Methods to Make Smart Glasses Detectable

No single method reliably detects a pair of glasses that is already paired and passively recording. We summarize the practical options below, then examine each in turn.

Method	How it works	Reliability
BLE fingerprinting	Scan for Meta's BLE advertising: company ID 0x01AB, service UUID 0xFD5F. Tools: banrays, Nearby Glasses, Glasses Radar, nRF52840/Ubertooth sniffers.	Best available, but mostly at power-on/pairing; defeated by MAC randomization once connected.
WiFi sync detection	Detects the direct WiFi burst when media transfers from glasses to phone.	Only during sync; defeated by recording now and syncing later.
Optical / IR retroreflection	"Cat-eye" reflection from the camera lens under IR/visible light; commercial camera finders.	Unreliable on this device; hands-on testing found weak, inconsistent reflection.
Recording LED	The white capture indicator on the frame.	Easy to miss; permanently defeated by a 50-100 USD hardware mod.
SDR facility monitoring	Passive software-defined-radio sensors scanning BLE, WiFi, cellular, Zigbee to classify and locate wearables.	Effective but enterprise-grade; not portable for an individual.

3.1 Bluetooth Low Energy fingerprinting (currently the most viable)

Ray-Ban Meta glasses broadcast BLE advertising packets (small wireless announcement messages that nearby devices can see) carrying Meta's assigned company ID **0x01AB** and service UUID **0xFD5F** (fixed identifiers baked into that signal, a signature); a verified capture, taken as the glasses power on, shows a distinctive data pattern, **020102102716e4** ^[26]. Open-source and app tools exploit this. NullPxl's banrays, a wearable built on a cheap hobbyist microcontroller (ESP32) that sounds an alert on a Meta match ^[26], the Nearby Glasses Android app, which also matches broadcast names and ID codes with a configurable signal-strength cut-off (an RSSI threshold, which roughly maps to distance) ^[27, 28], and Glasses Radar, which matches the full manufacturer-data template and requires several consistent sightings to cut false positives ^[29]. The critical limitation we flag for field use is that detection is reliable only at pairing, at power-on, and less consistently when the glasses leave the charging case ^[26]. Once connected and actively recording, the glasses largely stop advertising, and following the live connection would require capturing the very first connection-request message (**CONNECT_REQ**) with a specialist radio-capture gadget such as an nRF52840

or Ubertooth sniffer ^[26]. MAC randomization, where the glasses periodically change hardware ID to avoid being tracked, defeats detection based on the manufacturer's ID prefix, the shared company ID produces false alarms from Meta VR headsets, and Apple's iOS blocks apps from scanning for these signals in the background, so we know of no reliable background detector on iPhones ^[27, 29].

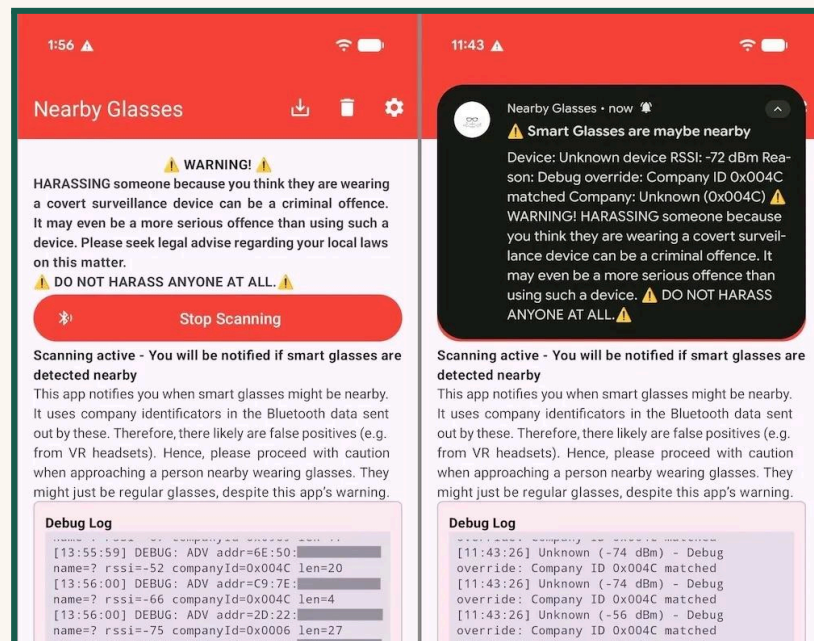


Figure 3 - The Nearby Glasses app alerts users to Meta or Snap smart glasses in their vicinity by tracking the Bluetooth signals these devices broadcast. [Source](#)

3.2 WiFi detection

Full-resolution media transfer runs over a temporary direct WiFi link between the glasses and a phone, not over Bluetooth, which handles only audio and commands ^[29]. This produces a detectable traffic burst, but only during sync, not during capture. A user who records now and syncs later at home defeats live WiFi monitoring entirely.

3.3 Optical and infrared retroreflection

Camera lenses bounce light straight back toward its source, known as the “cat-eye” effect (the bright glint you see reflected off a lens) that underlies commercial hidden-camera finders ^[31]. On the Ray-Ban Meta glasses specifically, hands-on testing found that this glint was weak and inconsistent even at a close range of under 850 nm and 940 nm light, insufficient to distinguish the glasses from ordinary reflective eyewear ^[26]. We therefore treat optical detection as currently unreliable for this device.

3.4 The recording LED and its defeat

A small white LED is meant to signal capture, but it is widely criticized as too easy to miss, and covering it with tape triggers a software lockout. A hardware mod that costs between USD 50-100 that drills out or desolders the LED permanently defeats the indicator without disabling the camera, and no factory reset can undo it ^[33]. Meta responded in July 2026 with a firmware update (a change to the software built into the glasses) that disables the camera if the light is blocked or removed, and pledged marketplace takedowns ^[33]. That is a company claim pending independent testing, a

physically removed component is genuinely hard for firmware to detect, and coverage did not confirm model coverage, so we do not treat the LED as a detection signal.

3.5 Professional SDR monitoring

For high-value environments, software-defined-radio sensor platforms (radio receivers tuned by software, able to listen across many wireless bands at once) passively and continuously scan cellular, Bluetooth, WiFi, and Zigbee (a short-range wireless standard common in smart-home devices) to detect, classify, and locate AI wearables. The approach can scale to a whole building ^[30]. This tooling is enterprise-grade rather than something an individual journalist can carry. We note that institutional recognition of the threat is growing, and some organizations are already banning the glasses on their premises.

4. Connecting the Two Axes

The forensic model and the field-detection problem are, in our view, two views of the same system. The identifiers a forensic examiner recovers after the fact, the Bluetooth MAC, the pairing IDs, and the **0x01AB / 0xFD5F** advertising signature, are exactly the signals a real-time detector tries to catch ^[1, 26]. Both are undermined by the same design choices: MAC randomization, advertising only at power-on and pairing, and cloud-side storage of the actual content. Likewise, the on-device face-detection model documented forensically is the same capability found staged as **NameTag** ^[1, 23]. The device's architecture thus makes it simultaneously data-rich after seizure and hard to catch in the moment.

What changes the risk calculus in SWANA, in our assessment, is consequence and recourse. In the region we work in, the same phenomenon can trigger more severe consequences on a legal level: LGBTQ+ individuals may be prosecuted, dissidents can be identified, and honor-based violence can even take place within several communities while the recourse for the victims is weaker. Broad security exemptions, thin enforcement, no practical privacy measures for bystanders, and data physically beyond the reach of local regulators all make the situation in the SWANA region even more challenging ^[15, 16, 17]. Severe consequence combined with minimal recourse is what makes the device disproportionately dangerous in our region.

5. Recommendations

For at-risk individuals

1. Treat a BLE-scanning app (like Nearby Glasses or Glasses Radar on Android) as an early-warning aid only, understanding that it mostly catches power-on and pairing, produces VR-headset false positives, and cannot run in the background on iOS ^[27, 29].
2. Rely primarily on behavioral cues, like a person orienting their face toward you, an unusual tap or pause on a temple, and the small white LED light, keeping in mind that the LED light can easily be tampered with and turned off ^[33].
3. In sensitive meetings and interviews, enforce a device-free, no-wearable rule and physically collect eyewear. This is the only reliable control.

For organizations and newsrooms

1. In genuinely sensitive facilities, deploy SDR-based radio-frequency monitoring (the software-tuned radio receivers described above) and adopt written wearable-camera bans ^[30].
2. Seek the support of organizations working with surveillance in the region such as SMEX, Access Now, 7amleh, and Citizen Lab for forensic support and threat modeling ^[4, 16, 18].

Thresholds that should change the advice

1. If Meta activates **NameTag** facial recognition or ships an always-on capture mode, escalate from detection to prohibition and public advocacy for regional import or use restrictions ^[23].
2. If a firmware update changes the BLE advertising fingerprint, re-validate every detection app before trusting it ^[26].
3. If independent testing confirms Meta's July 2026 anti-tamper LED firmware across all models, the LED regains limited value as a signal; but until then, we assume it can be defeated ^[33].

6. Limitations

- Detection is adversarial and currently favors the recorder. We treat every countermeasure as advisory, not protective, because no consumer-grade method reliably detects glasses that are already paired and passively recording ^[26].
- Meta's July 2026 anti-tamper claim is unverified, is uncertain across model generations, and a physically removed LED is hard for firmware to detect ^[33].
- Optical/IR detection specifically fails on this device in hands-on testing, despite working on some other hidden cameras ^[26, 31].
- Some artifact specifics and the author list rely on the DFRWS abstract and indexed snippets; we verify names and details against the final published paper before relying on them ^[1, 2].
- Several detection tools are early-stage projects whose own creators document reliability problems; we independently validate stronger vendor claims ^[26, 27, 29].
- The regulatory picture is fast-moving; we refresh figures and enforcement counts at publication time ^[13, 15].

References

- [1] Panta, S., Alsmadi, R., & Baggili, I., "Seeing the Evidence: A Forensic Framework for Analyzing Ray-Ban Meta AI Smart Glasses." DFRWS USA 2026 (BiT Lab, Louisiana State University).
<https://dfrws.org/presentation/seeing-the-evidence-a-forensic-framework-for-analyzing-ray-ban-meta-ai-smart-glasses/>
- [2] Panta, S., Alsmadi, R., & Baggili, I., "Seeing the Evidence" (preprint listing). ResearchGate, 2026.
https://www.researchgate.net/publication/404038076_Seeing_the_Evidence_A_Forensic_Framework_for_Analyzing_Ray-Ban_Meta_AI_Smart_Glasses
- [3] CNBC, "Ray-Ban maker EssilorLuxottica says it more than tripled Meta AI glasses sales in 2025." February 11, 2026. <https://www.cnbc.com/2026/02/11/ray-ban-maker-essilorluxottica-triples-sales-of-meta-ai-glasses.html>
- [4] The Citizen Lab, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." University of Toronto, 2018.
<https://citizenlab.ca/research/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>
- [5] Arab Center Washington DC, "The Full Story behind the NSO Hack: The Israeli-Military-Allied Surveillance Industry and Transnational Repression." <https://arabcenterdc.org/resource/the-full-story-behind-the-nso-hack-the-israeli-military-allied-surveillance-industry-and-transnational-repression/>
- [6] Forbidden Stories, "Pegasus: The new global weapon for silencing journalists." The Pegasus Project, 2021.
<https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/>
- [7] The Citizen Lab, "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage Zero-Click Exploit." Report No. 135, December 2020.
<https://citizenlab.ca/research/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/>
- [8] Slashdot, "Meta Now Forces AI Data Collection Through Ray-Ban Smart Glasses." May 1, 2025.
<https://tech.slashdot.org/story/25/05/01/1445212/meta-now-forces-ai-data-collection-through-ray-ban-smart-glasses>
- [9] Help Net Security, "Workers reviewing Meta Ray-Ban footage encounter users' intimate moments." March 5, 2026. <https://www.helpnetsecurity.com/2026/03/05/meta-ray-ban-smart-glasses-privacy-risks/>
- [10] AppleInsider, "What privacy? Meta's smart glasses are filming unwitting naked people." March 3, 2026.
<https://appleinsider.com/articles/26/03/03/what-privacy-as-expected-meta-ray-bans-are-a-privacy-disaster>
- [11] Political.org, "Meta Terminates Kenya Contract After Workers Viewed Intimate Footage Captured by Ray-Ban Smart Glasses." May 2, 2026.
<https://political.org/2026/05/02/meta-terminates-kenya-contract-after-workers-viewed-intimate-footage-captured-by-ray-ban-smart-glasses/>
- [12] Malay Mail, "I spy with my Ray-Bans: Kenya eyes Meta glasses over alleged data snooping." April 1, 2026.
<https://www.malaymail.com/news/tech-gadgets/2026/04/01/i-spy-with-my-ray-bans-kenya-eyes-meta-glasses-over-alleged-data-snooping/214584>
- [13] Clyde & Co, "Egypt regulatory update on data privacy." January 2026.
<https://www.clydeco.com/en/insights/2026/01/egypt-regulatory-update-on-data-privacy>
- [14] Privacy International, "State of Privacy Morocco." <https://www.privacyinternational.org/state-privacy/1007/state-privacy-morocco>
- [15] Kayrouz & Associates, "Cross-Border Data Transfers Under UAE Law in 2026." <https://www.kayrouzandassociates.com/insights/cross-border-data-transfers-under-uae-law-in-2026>
- [16] SMEX, "A Snapshot of Digital Rights Coverage in the MENA Region." <https://smex.org/a-snapshot-of-digital-rights-coverage-in-the-mena-region/>
- [17] Human Rights Watch, "Middle East, North Africa: Digital Targeting of LGBT People." February 21, 2023.
<https://www.hrw.org/news/2023/02/21/middle-east-north-africa-digital-targeting-lgbt-people>
- [18] Access Now, "In Egypt, expressing your sexuality online makes you a target for human rights abuse." <https://www.accessnow.org/egypt-expressing-sexuality-online-makes-target-human-rights-abuse-stop/>
- [19] Star Observer, "Egyptian Police Using Grindr To Target Gay Men." <https://www.starobserver.com.au/news/egyptian-police-using-grindr-to-target-gay-men/222760>
- [20] OECD.AI Policy Observatory, "Barcelona AI-Enabled Smart Glasses Privacy Violation Incident." Incident 2025-05-30-e5f6. <https://oecd.ai/en/incidents/2025-05-30-e5f6>

- [21] National Law Review, "BBC Investigation Finds Men Use Smart-Glasses to Secretly Film Women." 2026.
<https://natlawreview.com/article/smart-glasses-and-privacy-wearable-surveillance-and-disclosure-issues>
- [22] ITP.net, "Before You Buy Meta Glasses in the UAE: Must-Know Photography Laws." 2025.
<https://www.itp.net/news/before-you-buy-meta-glasses-in-the-uae-must-know-photography-laws>
- [23] Eastern Herald, "Meta Quietly Put Facial Recognition in Its Smart Glasses App. Then Someone Found It." June 28, 2026.
<https://easternherald.com/2026/06/28/meta-smart-glasses-nametag-facial-recognition-privacy-covert-recording/>
- [24] Electronic Frontier Foundation, "Cooper Quintin" (staff profile). <https://www.eff.org/about/staff/cooper-quintin>
- [25] Tech Times, "Meta Smart Glasses Facial Recognition Code Is Already on Millions of Phones, Wired Finds." June 5, 2026.
<https://www.techtimes.com/articles/317870/20260605/meta-smart-glasses-facial-recognition-code-already-millions-phones-wired-finds.htm>
- [26] NullPxl, "banrays: Glasses to detect smart-glasses that have cameras." GitHub.
<https://github.com/NullPxl/banrays>
- [27] Jeanrenaud, Y., "yj_nearbyglasses: attempting to detect smart glasses nearby and warn you" (Nearby Glasses). GitHub. https://github.com/yjeanrenaud/yj_nearbyglasses
- [28] Cybernews, "Creator of Nearby Glasses app is fighting back clones promising to detect pervert glasses." <https://cybernews.com/security/nearby-smartglasses-detection-app-impostors-warning/>
- [29] Glasses Radar, "How to Detect Ray-Ban Meta Smart Glasses Near You (2026 Guide)." <https://www.glassesradar.app/guide/how-to-detect-ray-ban-meta>
- [30] Hackaday, "Making Glasses That Detect Smartglasses." December 9, 2025.
<https://hackaday.com/2025/12/09/making-glasses-that-detect-smartglasses/>
- [31] Patterson, C., "Can You Find Hidden Cameras? A Review of Products and Techniques." LinkedIn.
<https://www.linkedin.com/pulse/can-you-find-hidden-cameras-review-products-charles-patterson>
- [32] CBC Radio, The Current, "Meta's smart glasses make it easy to secretly film people. It's mostly women bearing the fallout." <https://www.cbc.ca/radio/thecurrent/meta-glasses-covert-recording-9.7139927>
- [33] TheStreet, "Meta sent a warning to its glasses pranksters." 2026.
<https://www.thestreet.com/technology/meta-warns-glasses-instagram-ban-policy-pervert>