Issue #8

INTEL WATCH

January 2026

Watching the watchers. Guarding the guardians.

THE WATCHER

Monthly

DEFENDING HUMAN RIGHTS, PROTECTING CIVIC SPACE

DO YOU KNOW WHO'S WATCHING YOU? WE'RE HERE TO HELP YOU FIND OUT

INTELWATCH ADVOCACY:
#UGANDA NOT ALONE

Executive summary

Uganda stands at a critical juncture. In the aftermath of a patently rigged election – where the will of the Ugandan people was disregarded – the Ugandan government has intensified a violent crackdown on the political opposition and civil society organizations. Arbitrary arrests, targeted killings, and systematic repression are not isolated incidents - they are the lived reality for human rights defenders, activists, opposition leaders, and ordinary citizens who dare to dissent. This crisis is not merely an Ugandan issue - it is emblematic of a global trend in which democracy is being dismantled, and fundamental freedoms are under siege.

In light of this reality, The Resistance Bureau in partnership with IntelWatch hosted a #UgandaNotAlone X Space in order to show public solidarity with those on the front lines in Uganda. The event was designed to keep sustained international attention on the Ugandan crisis, push for meaningful accountability, and pressure the African Union and other relevant regional bodies to treat constitutional and electoral coups with the same sense of urgency as military takeovers and featured the Secretary General of the National Unity Platform (NUP) and other leading voices for democratic change in Uganda and the broader region.

Listen again to the X space discussion or for the first time on here

Together, we can amplify the demand for justice and show Ugandans that they are not alone in this struggle for freedom and dignity. Reshare the discussion, join the movement on all social media platforms under the hashtag #UgandaNotAlone to show your support and call for global action and solidarity with the people of Uganda.

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE UPDATES

WHEN RATS ATTACK: THE NEW FACE OF BANKING FRAUD TARGETING SOUTH AFRICANS

IMAGE SOURCE: IT WEB

Remote Access Trojan (RAT) scams are surging as one of South Africa's most dangerous banking frauds, enabling criminals to remotely control victims' phones/computers in real-time via malicious apps/links disguised as urgent fixes from banks, networks, or services—capturing PINs, OTPs, and executing transactions undetected, mimicking legitimate user activity. TymeBank's Bonolo Sebolai highlights red flags like urgency pressure, software install requests, or stay-on-line logins (banks never ask for PINs/OTPs), urging app store downloads only and direct bank verification; Check Point's Ian Janse van Rensburg notes RATs' stealth (no slowdowns), targeting networks/finances, recommending endpoint protection, MFA, and monitoring. Banks counter with real-time behavioral analysis and adaptive controls to minimize friction while thwarting threats, as awareness and layered defenses remain key against evolving sophistication- IT Web

OFFLINE AND SILENCED: AFRICA'S QUIET RISE OF INTERNET REPRESSION

IMAGE SOURCE: INFRASTRUCTURE NEWS

Africa experienced a record 21 internet shutdowns across 15 countries in 2024 per Access Now and #KeepItOn—its worst year on record, part of a global surge to 296 disruptions in 54 nations—often timed with elections, protests, or unrest in places like Sudan, eastern DRC, Senegal (February 2024 election protests), Ethiopia, Kenya, and Equatorial Guinea, stifling dissent under pretexts of national security. Governments increasingly enact cybercrime laws in Kenya and Zambia (2025) to enable ongoing monitoring and content control, while platform gatekeepers like Meta and X face criticism for opaque moderation amplifying outrage; meanwhile, telecoms comply with shutdowns under license threats despite African Commission Resolution 580 (2024) condemning them, as youth-driven digital innovation clashes with repression harming economies, rights, and democracy -
Infrastructure News

INTEL WATCH

Watching the watchers. Guarding the guardians.

RANSOMWARE IN AFRICA

IMAGE SOURCE: AFRICA PRESS

Ransomware, a malicious software encrypting or locking victims' data until ransom payment, ranks among Africa's top cyber threats per Interpol 2024, with high detections in South Africa (12,281) and Egypt (17,849), surging 37% globally per Verizon 2025 amid cybersecurity gaps, phishing, weak passwords, and unmonitored networks; 71% of hit South African firms paid ransoms (Sophos Q1 2025), facing downtime losses, reputational harm, and double extortion leaks, targeting critical sectors like power and healthcare. Africa's under-resourced defenses exacerbate risks, demanding governance accountability via backups, endpoint protection, intrusion detection, staff training, incident plans, business continuity/disaster recovery testing, external experts, and cyber-insurance, as payments guarantee nothing and enable repeat attacks - Africa Press

CYBER RISKS TOP CONCERNS FOR AFRICAN BUSINESSES IN 2026 REPORT

IMAGE SOURCE: ECOFIN AGENCY

The Africa Risk in Focus 2026 report by the Internal Audit Foundation, surveying over 1,000 chief audit executives across 39 countries, identifies cyber incidents (data breaches, malware, ransomware) as the top risk for African businesses at 62%—with 60% prioritizing it for internal audits—driven by AI-enhanced sophistication, rapid digital growth, and $10 billion losses in 2023 amid regulatory gaps and low awareness. Concern peaks in East Africa (65%), Southern/North Africa (64%), lower in Central (32%) and West Africa (53%), while business resilience (49%), surging digital disruption (44%, up from 10%), financial/liquidity risk (43% vs. global 31%), and fraud (43%) follow, reflecting tech interdependence, forex volatility, and infrastructure vulnerabilities across sectors - Ecofin Agency

INTEL WATCH

Watching the watchers. Guarding the guardians.

META'S SMART GLASSES HAVE REAL-TIME FACIAL RECOGNITION CAPABILITIES

IMAGE SOURCE: WEB PRO NEWS

Harvard students AnhPhu Nguyen and Caine Ardayfio developed I-XRAY, repurposing Meta's $300 Ray-Ban smart glasses into a real-time surveillance tool by streaming video to Instagram, applying AI facial recognition against public databases, and using large language models to instantly retrieve strangers' names, addresses, phone numbers, relatives, and more from people-search sites like FastPeopleSearch—demonstrating the capability in public settings like subways and streets. The project exposes how Meta's LED recording indicator fails in practice (overlooked in crowds or low light), rendering "privacy protections" ineffective, while legally accessible components—glasses for video capture, public data aggregation—enable consumer-level invasive tracking once reserved for governments, bypassing regulations like U.S. state biometric laws or EU GDPR due to real-time processing without storage. Privacy advocates highlight regulatory gaps, corporate design flaws lacking "privacy by design," and the ecosystem of data brokers amplifying risks; students advise opting out of databases (tedious, ongoing process), minimizing social media footprints, and vigilance, warning of normalized public anonymity loss as AR glasses proliferate - Web Pro News

---

PREDATOR SPYWARE TURNS FAILED ATTACKS INTO INTELLIGENCE FOR FUTURE EXPLOITS

IMAGE SOURCE: SECURITY WEEK

APredator spyware, developed by Intellexa, features sophisticated granular anti-analysis capabilities exposed by Jamf Threat Labs, including a comprehensive error code taxonomy (301-311) via the CSWatcherSpawner class that diagnoses precise implant failure reasons—such as error 304 for security tools like Frida/netstat or 311 for multiple instances—alerting operators for troubleshooting while aborting deployments. It employs detailed detection of custom HTTP proxies/root CAs, process monitoring (e.g., killing mmaintenanced to suppress SystemMemory crash forensics), SpringBoard hooking to conceal recording indicators, boot-timing checks, and C2 callbacks revealing vendor control, enabling adaptation against researchers and privacy-conscious users. These mechanisms, more advanced than prior reports, underscore Predator's evasion prowess, with implications for air-gapped analysis, crash log preservation, and network monitoring awareness amid its history of targeting high-profile victims via zero-click exploits - Security Week

INTEL WATCH

Watching the watchers. Guarding the guardians.

APPLE BUYS 'SECRETIVE' ISRAELI FACIAL SURVEILLANCE STARTUP Q.AI

IMAGE SOURCE: IRISH EXAMINER

Apple has reportedly acquired secretive Israeli startup QAI, a facial surveillance technology firm, in a deal raising significant privacy and ethics concerns amid ongoing global scrutiny of such tools. QAI specializes in advanced facial recognition capabilities, potentially enhancing Apple's existing biometric systems like Face ID, building on its prior acquisition of PrimeSense (key to Face ID development) from the same founder, Aviad Maizels. The purchase—Apple's second-largest after Beats—signals deeper integration of AI-driven surveillance tech into consumer devices, despite criticisms over human rights implications and lack of transparency in secretive Israeli firms supplying authoritarian regimes - The Cradle

DIGITAL WALLET PLAN IS A DANGEROUS INFRINGEMENT ON PRIVACY

IMAGE SOURCE: IRISH EXAMINER

Ireland's proposed digital wallet plan risks severe privacy infringement by mandating identification through digital infrastructure, amplifying government power in ways that threaten rights to privacy, data protection, anonymity, access to information, freedom of expression, non-discrimination, and security. While governments may legitimately require identification, digital implementation demands extreme caution due to its potential for abuse—either accidental or deliberate—creating pervasive surveillance risks absent robust safeguards - Irish Examiner

INTEL WATCH

Watching the watchers. Guarding the guardians.

CLASS ACTION: WHATSAPP BREACHES PRIVACY, CRACKS ENCRYPTED CHATS

IMAGE SOURCE: MEDIANAMA

A class-action lawsuit filed January 23, 2026, in San Francisco federal court by plaintiffs from Australia, Brazil, India, Mexico, and South Africa accuses Meta and WhatsApp of deceiving over 2 billion users by falsely claiming unbreakable end-to-end encryption (E2EE) via the Signal protocol, alleging employees can request real-time access to message contents through internal "tasks" and widgets without extra decryption—viewing chats from account inception, including deleted ones, mixed with unencrypted data for analysis. Citing 2025 whistleblowers like ex-engineer Faisal Baig (fired amid similar claims of metadata access for 1,500 engineers), the suit invokes U.S./California privacy laws, deceptive marketing, and lack of consent, seeking damages amid Meta's $167M NSO victory; Meta dismissed allegations as "false and absurd," reaffirming device-only decryption - Medianama

GOOGLE TO PAY $68M TO SETTLE LAWSUIT CLAIMING IT RECORDED PRIVATE CONVERSATIONS

IMAGE SOURCE: BBC

WhatsApp has sided with Apple in a high-profile UK legal battle against the Home Office over a secret Technical Capability Notice (TCN) demanding backdoor access to encrypted iCloud data for national security, warning it sets a "dangerous precedent" that could spur global governments to undermine end-to-end encryption protecting billions of users. CEO Will Cathcart affirmed WhatsApp would challenge any such weakening of its services, emphasizing privacy rights, after a judge rejected full secrecy for hearings—despite government arguments for confidentiality amid crimes like terrorism and child abuse—while Apple disabled its Advanced Data Protection feature in the UK rather than comply - BBC

INTEL WATCH

Watching the watchers. Guarding the guardians.

PAYING ATTACKERS MAKES FIRMS GROW MORE VULNERABLE TO RANSOMWARE

IMAGE SOURCE: TECH CENTRAL

Rubrik warns that paying ransomware attackers heightens vulnerability, with 60% of victims facing repeat strikes within six months—often by the same groups—despite 180% global cybersecurity spending growth over a decade versus 120% rise in attacks; identity systems like Active Directory (90% incident rate, 50% targeted) now enable full business shutdowns beyond file encryption, impacting retailers/manufacturers (e.g., M&S halting orders/payments) with massive revenue/reputational damage. Cybersecurity evolves from IT silos to board-level "assume breach" governance prioritizing quick recovery over prevention, rejecting payouts that invite litigation/data corruption (e.g., Colonial Pipeline), and addressing converged cloud/app/identity risks - Tech Central

---

EXPERTS UNMASK SINISTER PAK-LINKED CYBER CAMPAIGNS AGAINST INDIA

IMAGE SOURCE: SENTINEL

IZscaler ThreatLabz uncovered two Pakistan-linked cyber-espionage campaigns—Gopher Strike (phishing PDFs with geo-targeted ISO malware downloads mimicking Adobe updates) and Sheet Attack (abusing Google Sheets/Firebase/email for C2)—targeting Indian government entities since September 2025, using novel tradecraft possibly from a new APT36 subgroup or parallel actor. Separately, Cyfirma reported APT36/Transparent Tribe's spear-phishing ZIPs deploying adaptive ReadOnly/WriteOnly malware for remote control, screenshots, clipboard monitoring, RDP, and crypto theft against Indian government/universities/strategic sites, evading AV via dynamic behavior. Active since 2013 across 30 countries, these persistent operations highlight escalating hybrid threats despite limited success rates - Sentinel

INTEL WATCH

Watching the watchers. Guarding the guardians.

WHATSAPP'S STRICT SETTINGS COULD SHIELD JOURNALISTS FROM SPYWARE

IMAGE SOURCE: HOW TO SHOUT MEDIA

Signal has urged Germany to vote against the EU's "Chat Control" proposal, warning that it would effectively end privacy rights in Europe by mandating mass scanning of all private messages, photos, and videos shared on messaging platforms. The regulation, aimed at combating child sexual abuse material (CSAM), would require messaging apps to break or weaken end-to-end encryption to scan all communications, a move Signal argues undermines security for all users, not just criminals. Signal has threatened to leave the EU market if the law passes, stressing that Germany's opposition is crucial to defending digital privacy and preventing mass state surveillance. The German government officially announced its intention to vote against the proposal, emphasizing that random chat monitoring contravenes fundamental civil rights despite the need to fight child abuse at the EU level. The controversy highlights a significant clash between privacy advocates and policymakers over security and surveillance in digital communications - How to Shout Media

FAKE ROMANCE TRAP: ANDROID SPYWARE UNLEASHED

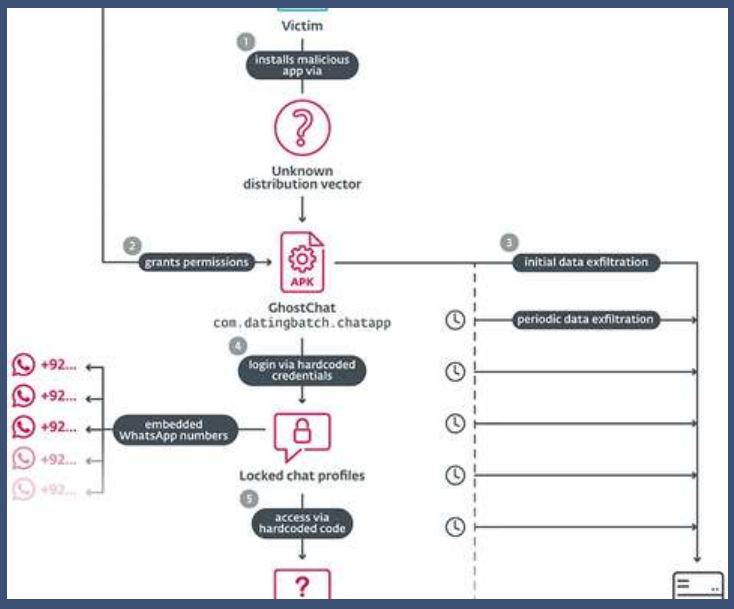


IMAGE SOURCE: HELP NET SECURITY

ESET researchers uncovered GhostChat, an Android spyware campaign targeting Pakistanis via romance scams, where victims sideload a fake dating app (mimicking legitimate icons, never on Google Play) showing 14 "locked" female profiles with hardcoded passcodes that redirect to threat actor-controlled Pakistani WhatsApp numbers for credibility. While users engage, the app silently exfiltrates device IDs, contacts, files (images/PDFs/Docs), monitors new images via content observers, and scans documents every 5 minutes to C2 servers, persisting post-boot; part of broader operations using fake gov sites for ClickFix PC compromises and GhostPairing QR scams hijacking WhatsApp accounts - Help Net Security

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE FIRMS TRACK PHONES VIA AD DATA

IMAGE SOURCE: LE MONDE

Surveillance firms, primarily Israeli ex-intelligence startups (e.g., Rayzone, Wave Guard, RCS's Ubiqo, Penlink) with ~15 players worldwide, harvest geolocation data from ad marketplaces—gathered by everyday apps like games/weather—for "Adint" tools promising law enforcement near-real-time (2min-24hr updates), 10-year historical tracking of phones globally to meter accuracy without telco cooperation, as demoed at Milipol and bought by U.S. ICE ($5M). These "black box" systems de-anonymize ad IDs (95% claimed in Italy) via cross-referencing leaked/hacked databases, enabling smuggler profiling or embassy visitor lists, yet suffer 80-85% unusable data and skirt regs by claiming commercial consent despite EU bans on repurposing ad data. Lax oversight—versus spyware—fuels demand amid rising secrecy, though some firms now push malicious ads for spyware installs, raising mass privacy alarms - Le Monde

HACKERS FOOL FACIAL RECOGNITION WITH SIMPLE PHOTOS

IMAGE SOURCE: THE EASTLEIGH VOICE

Cybersecurity experts warn that hackers are bypassing facial recognition systems using simple high-resolution photos printed or displayed on devices, exploiting vulnerabilities in liveness detection and image processing that fail to distinguish 2D spoofs from real faces, as demonstrated in low-tech attacks on ATMs, banking apps, and access controls. Advanced methods include video playback, deepfakes, kernel-level face swaps, app memory hooks, traffic interception, and business logic exploits, enabling identity theft, account takeovers, and unauthorized access despite biometric hype. Mitigation demands robust liveness checks (e.g., 3D depth, gestures), multi-factor biometrics, server-side validation, and AI anti-spoofing, as social media photos fuel these persistent threats - The Eastleigh Voice

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE FIRMS TRACK PHONES VIA AD DATA

IMAGE SOURCE: WEBPRONEWS

Amnesty International's Surveillance Watch platform maps a sprawling global AI-driven surveillance ecosystem in 2026, spotlighting firms like Palantir, Clearview AI, NSO Group (Pegasus), and Hikvision supplying facial recognition, biometrics, and analytics to 100+ countries, enabling governments/corporations to profile citizens via urban cameras, border scans, and predictive policing—often without consent, oversight, or rights safeguards. U.S. ICE/DHS aggressively deploys real-time tracking tools amid lax rules, while UK/EU push encryption backdoors and India mandates device location/logs/apps, fueling mass data hoarding that chills speech, enables discrimination, and targets migrants/protesters via biased AI from IBM/AWS. Pushback grows via U.S. city contract cancellations (e.g., Flock Safety), EU AI Act debates, state privacy laws, and grassroots advocacy demanding data minimization, bans on abusive tech, and ethical design, as wearables/grocery biometrics normalize constant monitoring with profound human costs - WebProNews

WEGMANS DEBATE: SURVEILLANCE INVADES WORKPLACES

IMAGE SOURCE: FORBES

Wegmans grocery chain sparked backlash after revealing facial recognition use in high-risk NYC stores (Manhattan/Brooklyn) to identify prior bad actors via cameras—signage-compliant but limited to security, discarding data post-need—amid broader U.S. surveillance trends like ICE/police facial tech (biased against darker skin), pandemic-era employee monitoring, gig worker tracking, and loyalty programs exposing health/pregnancy data. Critics highlight privacy erosion, morale drops, turnover (per 2025 Zety report), and disproportionate harm to Black/marginalized groups via flawed AI, urging consent, transparency, data protection laws, and balanced safety vs. overreach as workplaces/customers face "Orwellian" tools - Forbes

GROCERY SCANS: BIOMETRIC SURVEILLANCE ON YOUR SHOPPING LIST

IMAGE SOURCE: MARKETPLACE

Grocery stores like Wegmans are deploying biometric surveillance—facial recognition, eye-tracking, gait analysis, and voice patterns—to monitor shoppers for theft prevention and personalized pricing, evolving from manual "naughty lists" to AI-driven insights on dwell time (e.g., cookie aisle hesitation) that maximize profits by charging what users tolerate. Amazon's palm-to-pay at Go/Whole Foods exemplifies convenience trade-offs, but flawed tech (e.g., Rite Aid's biased false positives against women/POC) erodes privacy amid no federal disclosure mandates, patchwork local laws, and limited opt-outs—shop or surrender data. Experts warn of vulnerability exposure without meaningful consent, urging stronger regs as surveillance normalizes dynamic pricing and profiling - MarketPlace

INTEL WATCH

Watching the watchers. Guarding the guardians.

REPRESSION MONITOR

‘HANG UP NOW’: IRAN SPIES ON AUSTRALIAN-IRANIAN CALLS AMID UPRISING

IMAGE SOURCE: THE GUARDIAN

Australians with relatives in Iran report intercepted phone calls amid the 2026 uprising and regime crackdown, where callers are abruptly warned "you need to hang up now" mid-conversation—likely by Iranian authorities monitoring brief, one-minute outgoing international calls permitted after a communications blackout, as families relay arrests, violence, and heavy security presence while fearing reprisals. These high-cost, surveilled lines fund the regime, exacerbate diaspora anxiety, and obscure protest death tolls (600+ estimated), with limited inbound access and satellite flickers providing scant relief amid global Iranian protests in Australia and beyond - The Guardian

FROM PROTEST TO PERIL: CELLEBRITE USED AGAINST JORDANIAN CIVIL SOCIETY

IMAGE SOURCE: CITIZEN LAB

Citizen Lab's investigation reveals Jordanian authorities abusing Cellebrite's forensic tools (UFED/Physical Analyzer) since at least 2020 to non-consensually extract data—chats, photos, locations, deleted files—from seized phones of activists, journalists, and human rights defenders during 2023-2025 Gaza solidarity protests, violating ICCPR rights via repressive 2023 Cybercrime Law prosecutions for "fake news," "sedition," or "hate speech" (2,928 Article 15 cases by 2024). Forensic IoCs on four analyzed devices (three iOS, one Android)—including HostID 90169269806589377613722O7, mnm processes with "com.cellebrite.bruteforce" queues, checkm8 exploits, and com.client.appA packages—plus three court records confirm extractions often exceeding case scope (e.g., password tabs viewed unnecessarily), enabled by coerced Face ID, passcode notes, or BFU/AFU bypasses amid GID/Cybercrime Unit detentions. Cellebrite's vague responses dodge specifics despite ethics committee claims, as tools persist in repressive contexts (Russia/Belarus post-sales halt); recommendations urge watermarking, investigations, strong passcodes, Lockdown Mode, and app features like remote account locks - Citizen Lab

INTEL WATCH

Watching the watchers. Guarding the guardians.

HUNGARY'S DIGITAL CITIZENSHIP TRAPS CITIZENS IN FIDESZ SURVEILLANCE WEB

IMAGE SOURCE: IMPACT INTERNATIONAL

Hungary's Digital Citizenship Programme (2022–2026), via the Digital Citizenship Application (DÁP), promises efficient services like birth registration and identity verification amid high digital adoption (82% online public admin use), but critics warn it traps citizens in a Fidesz surveillance web ahead of April 2026 elections, integrating facial recognition linked to FaceKom—a firm tied to PM Orbán's son-in-law István Tiborcz—deployed against LGBTQ+ Pride protests in violation of the EU AI Act, alongside rushed 2023 data laws, Digital Civic Circles for propaganda, citizenship suspensions for "sovereignty threats," and probes by the Sovereignty Protection Office, eroding privacy and enabling opposition monitoring in a Chinese-style model contrasting Estonia's openness - Impact International

SURVEILLANCE, HARASSMENT, BRIBES: MIGRANTS' DAILY HELL IN RUSSIA

IMAGE SOURCE: RFI

Russia's 6.5 million migrants, mainly Central Asian laborers in low-skilled jobs, endure intensifying digital surveillance via the mandatory Amina app—requiring daily location check-ins to avoid blacklisting, frozen bank accounts, job loss, or deportation—coupled with stricter 2025 Putin policies limiting family stays, imposing ultra-tough language tests (blocking 87% of migrant kids from schools), routine bribes to police, street harassment, humiliation, and surging xenophobia fueled by inflation, war taxes, the 2024 Moscow concert hall attack blamed on Tajiks, and ultranationalist rhetoric portraying migrants as threats to jobs, traditions, and society - Rfi

INTEL WATCH

Watching the watchers. Guarding the guardians.

THE DEATH OF DIGITAL FREEDOM IN SO CALLED 'SHINING INDIA'

IMAGE SOURCE: DAILY PAKISTAN

India's Modi government is imposing draconian digital controls, mandating from December 2025 that all smartphones sold come pre-loaded with the undeletable, non-disableable Sanchar Saathi app—requiring permissions for calls, messages, photos, and camera access under the pretext of anti-fraud and lost phone recovery (700,000 reclaimed), effectively turning 1.2 billion devices into state surveillance tools akin to those in Russia and China, while a January 2026 proposal demands manufacturers like Apple and Samsung hand over proprietary source codes and notify Delhi of updates, eroding privacy, consent, and democratic norms amid India's world-leading 600+ internet shutdowns since 2012 - Daily Pakistan

ICE UNLEASHES ADVANCED SURVEILLANCE TECH ARSENAL IN IMMIGRATION CRACKDOWN

IMAGE SOURCE: MEZHA

ICE is deploying advanced surveillance tools like Mobile Fortify (NEC-powered facial recognition and fingerprint matching against CBP databases, storing images 15 years), iris scanners, geolocation software for extensive tracking, reinstated spyware contracts for phone infiltration, AI-driven social media profiling (Facebook/TikTok), SmartLINK app with facial/GPS check-ins for Alternatives to Detention, and Palantir integrations—aiming for 1M annual deportations under Trump amid privacy fears of mission creep to citizens/protesters, lacking oversight despite DHS's 100+ AI systems and $2.7B border tech funding - Mezha

INTEL WATCH

Watching the watchers. Guarding the guardians.

THE FBI IS USING FACIAL RECOGNITION TO IDENTIFY ICE PROTESTORS IN SOCIAL MEDIA VIDEOS

IMAGE SOURCE: FORBES

IThe FBI deployed facial recognition technology on YouTube videos and city surveillance footage to identify and charge anti-ICE protesters in Minneapolis following the January 7, 2026, shooting death of Renee Nicole Good by an ICE agent, targeting suspects for vandalism, theft from government vehicles, and property damage without warrants. In three documented cases, the FBI matched images to social media profiles via its Facial Recognition Services division and Clearview AI—drawing from a vast scraped database—leading to arrests like that of Thomas James-Jones for courthouse window damage, amid citizen footage from Mercado Media sparking outrage over unaware use. ACLU's Nathan Freed Wessler warns of biased, error-prone tech (wrongfully detaining Black individuals and citizens) enabling warrantless mass surveillance of protesters, while ICE/CBP expand tools like Mobile Fortify app for on-street biometric scans against 200M+ images, fueling civil liberties fears over First/Fourth Amendment violations - Forbes

UK POLICE TO USE AI FACIAL RECOGNITION TECH LINKED TO ISRAEL'S WAR ON GAZA

IMAGE SOURCE: ALJAZEERA

IUK police are set to expand live facial recognition (LFR) deployment from 10 to over 50 vans nationwide under Home Secretary Shabana Mahmood's sweeping reforms, partnering with Digital Barriers which subcontracts controversial Israeli firm Corsight AI—whose tech was used by Israel during its Gaza war, drawing accuracy concerns from intelligence officials. The £115M Police.AI national center will accelerate AI tools across 43 forces to combat digital-age crime (90% with digital elements), including fraud and organized networks, while creating a "British FBI" via the National Police Service merging key agencies. Civil liberties groups like Liberty warn of mass surveillance tracking daily lives without limits, amid High Court challenges and calls for regulation, as the Home Office touts it as policing's biggest modernization in 200 years.- Aljazeera

INTEL WATCH

Watching the watchers. Guarding the guardians.

INTELLIGENCE AGENCIES

IRELAND PLANS LAW ALLOWING LAW ENFORCEMENT TO USE SPYWARE

IMAGE SOURCE: THE RECORD

TIreland's government is advancing the Communications (Interception and Lawful Access) Bill to replace its outdated 1993 surveillance law, granting police powers to deploy spyware (e.g., from NSO Group or Intellexa), intercept encrypted communications across apps/IoT/email, use IMSI catchers for location tracking, and conduct covert recordings—strictly for "serious crime/security threats" with judicial warrants, proportionality tests, and provider cooperation, amid civil liberties concerns over privacy erosion in the smartphone era - The Record

CHINA'S SOCIAL CREDIT & INFO CONTROL SURVEILLANCE TRAP

IMAGE SOURCE: ORF

China's Social Credit System (SCS), formalized in 2014 and evolving through pilots, integrates financial credit scoring with behavioral monitoring via blacklists/redlists, data aggregation from 47+ government bodies/private firms, and real-time big data algorithms to assess "trustworthiness" of individuals, businesses, and officials—rewarding compliance (e.g., easier loans, priority services) while punishing violations like court debts, tax evasion, or uncivil acts (e.g., travel bans, job restrictions)—aiming to reduce corruption, boost transparency, and enforce norms under Xi Jinping, though raising privacy/data security fears amid decentralized, non-unified implementation - ORF

INTEL WATCH

Watching the watchers. Guarding the guardians.

UNITED STATES, THE EUROPEAN UNION, BRITAIN AND AUSTRALIAN GOVERNMENTS PUSH DIGITAL IDS, SURVEILLANCE, CENSORSHIP

IMAGE SOURCE: WSWS

US, EU, UK, and Australian governments are coordinating to eliminate online anonymity through universal digital ID systems under the guise of child protection, advancing bills like KOSA/COPPA 2.0 (US age verification for social media/AI), Australia's under-16 social media ban (effective Dec 2025, fines up to $49.5M), EU's Chat Control (scanning encrypted messages), and UK on-device surveillance mandates—requiring biometric/ID proofs that tie real-world identities to all online activity, enabling mass surveillance/censorship to suppress dissent from Arab Spring to Gaza protests, amid broader assaults on strikes, asylum, and press freedoms - WSWS

AMAZON SELLS FACE RECOGNITION TECHNOLOGY TO US LAW ENFORCEMENT AGENCIES

IMAGE SOURCE: BETA NEWS

Amazon Rekognition is AWS's cloud-based AI service for image/video analysis, enabling face detection/analysis (attributes like age, emotions, glasses), facial recognition/matching against collections, object/scene/text detection, unsafe content moderation, celebrity ID, and custom labels via AutoML—widely marketed for user verification, content search, people pathing, and security, with configurable confidence thresholds but criticized for biases and privacy risks in law enforcement uses- Beta News

INTEL WATCH

Watching the watchers. Guarding the guardians.

WASHINGTON COUNTY EYES AI SPY GUARDRAILS

IMAGE SOURCE: GOVERNMENT TECHNOLOGY

Thurston County, Washington commissioners unanimously advanced Commissioner Carolina Mejia's draft ordinance to regulate AI-enabled surveillance technologies like biometrics, predictive policing, and behavioral analysis, establishing board approval requirements via detailed "surveillance impact reports" assessing privacy, equity, and vendor practices, plus annual reports on usage, audits, costs, and incidents—banning real-time facial recognition, discriminatory profiling, unauthorized data sharing, and covert ops without sheriff sign-off, while mandating minimal data collection/retention, robust IT security (e.g., encryption), and vendor audits to prevent unchecked normalization amid community fears post-Olympia's Flock camera decommissioning- Government Technology.

THE TRUMP ADMINISTRATION IS STRENGTHENING ITS SURVEILLANCE CAPABILITIES

IMAGE SOURCE: THE 1A

Thurston County, Washington commissioners unanimously advanced a draft ordinance proposed by Commissioner Carolina Mejia to regulate AI-enabled surveillance technologies (e.g., biometrics, predictive policing, behavioral analysis), requiring board approval via detailed "surveillance impact reports" on privacy/equity risks, vendor audits, data policies, costs, and alternatives, plus annual usage reports—banning real-time facial recognition in public, discriminatory profiling, predictive policing on individuals/communities, unauthorized data sharing/covert ops, while mandating minimal data collection/retention, encryption, and IT security to prevent unchecked expansion amid community fears, informed by state guidance and models from Seattle/Oakland, with phase two eyeing vendor data control. - The 1A

INTEL WATCH

Watching the watchers. Guarding the guardians.

A MESSAGE FROM THE TEAM: COMPLIMENTS OF THE NEW SEASON!

New Year; The Course Is The Same- Full Steam Ahead

Dear Reader,

Welcome to the first edition of The Watcher for 2026.
As we step into a new year, it is vital to look back at the journey we began together last year. When we launched this newsletter, our goal was simple yet ambitious: to cut through the noise and provide you with critical updates on the opaque worlds of state and private surveillance. Your engagement over the past twelve months has proven that there is a hunger for accountability and a need for rigorous oversight.

In 2026, Intelwatch remains committed and steadfast in its mission. The landscape of surveillance is not static; it is constantly changing at break-neck speed. From AI-driven biometric monitoring to the unchecked data brokering of private intelligence firms, the tools used to track citizens are becoming increasingly sophisticated and harder to detect. This year, The Watcher will continue to be your frontline resource, unpacking these evolving trends and ensuring that neither tech giants nor government agencies operate in the dark.

We are already hitting the ground running. Just this week, we co-hosted a critical conversation on Twitter Space under the hashtag #UGANDANOTALONE. The discussion highlighted the digital rights crisis facing citizens in Uganda and underscored a universal truth: the fight for rights is a global fight for democracy. If you missed it, a link is provided as one of the key takeaways in this edition.

Thank you for standing with us as we continue to 'watch the watchers'.

In solidarity,
Intelwatch Editorial Team

Watching the watchers. Guarding the guardians.

HAVE YOUR SAY!
LETTER TO THE EDITOR

Dear Readers:

Welcome to the "Letter to the Editor" section of our newsletter - a safe space dedicated to your voice and your views. As an organisation rooted in the Global South but whose work extends across borders, our mission is to promote democratic oversight of intelligence and surveillance activities worldwide. We monitor, report, educate, and advocate to ensure that surveillance laws and practices respect human rights and democratic principles.

We strongly believe that meaningful change begins with dialogue, and that's where you come in. We invite you to share your thoughts about the issues we cover, your concerns, and experiences related to surveillance in your community or country and suggest topics or questions you want us to explore. Your insights help shape the conversation and strengthen our shared commitment to Defending Human Rights, Protecting Civic Space in the digital age, amplifying the need for transparency and accountability and holding power accountable.

Send your letters, stories, or feedback to us at advocacy@intelwatch.org.za, and together, let's strengthen the global movement for democratic oversight.

We look forward to hearing from you and building a Intelwatch-out community where everyone's voice matters.

Warm regards
The Intelwatch Team

LETTER TO THE EDITOR:
INFO@INTELWATCH.ORG.ZA

INTEL WATCH

Watching the watchers. Guarding the guardians.

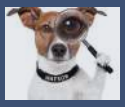
GET INVOLED!

Sign up to get occasional news and briefings on intelligence oversight and surveillance reform in Southern Africa and beyond

FIND US ON SOCIAL MEDIA

@IntewatchNews

HAVE ANY QUESTIONS?



info@intelwatch.org.za

The Reynolds Foundation Now for tomorrow

Global Dialogue

Luminate

Funded by the European Union

We are grateful for the support of our donors!