Issue #6

INTEL WATCH

October 2025

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

EXCLUSIVE INTELWATCH MANUAL & REPORTS

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

INTELWATCH

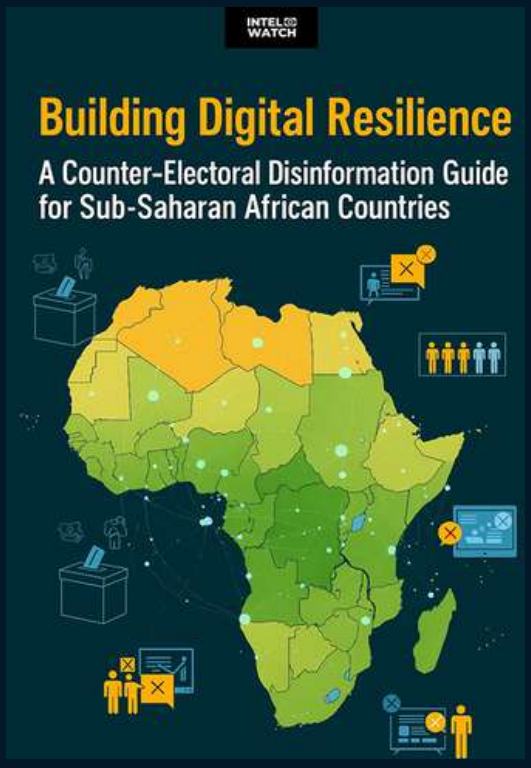
Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH MANUAL

BUILDING DIGITAL RESILIENCE: A COUNTER-ELECTORAL DISINFORMATION GUIDE FOR SUB-SAHARAN AFRICAN COUNTRIES

BY INTELWATCH

DOWNLOAD MANUAL



Executive summary

Electoral disinformation has sown disorder across Sub-Saharan Africa, damaging electoral integrity, social cohesion, and public trust in democratic norms and institutions. This guide offers a practical and context-specific roadmap to understanding and combating electoral disinformation in the region. While grounded in regional and international best practice, it dismantles the often "Global North"-lensed assumptions about information disorders. And instead, foregrounds the lived realities, vulnerabilities, and technological patterns specific to the region and its countries.

Part One of the guide unravels the WHAT, WHO, WHY, AND HOW of electoral disinformation:

• ***WHAT:*** The Conceptual Frameworks of Disinformation: What is disinformation? What are the different types of disinformation? What are its theoretical frameworks? Guidance is provided to aid in distinguishing disinformation from other information disorders, as well as from political propaganda.

• ***HOW and WHY:*** Cultural and Social Drivers: How do local contexts and specific social, political, and cultural contexts of individual countries shape susceptibility to disinformation?

• ***HOW and WHY:*** Psychological Drivers: Why does disinformation resonate so deeply and undermine trust in institutions, media, and truth?

• ***HOW and WHY:*** Technical Drivers: How are social media platforms and recommender algorithms and other design choices exploited by malign actors to amplify falsehoods at scale?

• ***WHO:*** Actors and Tactics: Who is spreading disinformation, and what strategies, both covert and overt, are they using to sway public opinion or disrupt democratic processes?

Part Two outlines the HOW TO, a practical roadmap for countering electoral disinformation. It includes:

• ***Establishing Electoral Disinformation Response Teams:*** Practical guidance on the essential roles and skills needed to monitor and combat disinformation, along with advice on building partnerships with organisations already working in the information integrity space in Sub-Saharan Africa.

• ***Digital Ecosystem Statistics:*** Guidelines for mapping national-level vulnerabilities, including gaps in digital access, weaknesses in the media landscape, and disinformation risks. Guidance is also provided on how to factor in the unique social and cultural conditions of each country as part of this process.

• ***Using Social Media Analytics (SMA) to Monitor Misinformation***: A proactive and reactive strategy that covers (1) collecting and analysing social media data, (2) a recommended SMA workplan covering the lead-up, during, and after an election is held.

A substantial annex is included to reinforce the guide's key learnings. It features:

• A comprehensive glossary of terms commonly used in the counter-disinformation field. In addition, the footnotes were specifically chosen to include text that explains the various concepts and issues extensively for those requiring deeper explanation

• Case studies of electoral disinformation monitoring projects from various African countries.

• Recommended books and articles offering deeper insights into the theoretical and technical foundations of disinformation and associated topics.

• A curated selection of similar electoral disinformation guides developed by international organisations

INTEL WATCH

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

ZIMBABWE'S SURVEILLANCE STATE: FACILITATING AN OMNIPRESENT TYRANNY

BY INTELWATCH

DOWNLOAD MANUAL

Executive summary

This report provides a comprehensive analysis of Zimbabwe's transformation into a surveillance state under successive Zimbabwe African National Union Patriotic Front (ZANU-PF) administrations, with particular emphasis on the technology-aided acceleration of these practices, under current President Emmerson Mnangagwa's regime (2017-present).

The report demonstrates how practices initially designed for counterinsurgency and political control by the-then white minority governments in Southern Rhodesia have been continually repurposed and expanded, yielding a sophisticated system of authoritarian governance that fundamentally undermines democratic institutions and human rights well into the 21st century. Zimbabwe's democratic space has contracted significantly since independence from Britain and white minority rule in 1980. This contraction continues and has accelerated through the expansion of the state's surveillance architecture targeting politicians from both the ruling party and the opposition, civil society actors, journalists and ordinary citizens. Surveillance has evolved from being a reactive, adhoc tool of crisis management to a pre-emptive and central pillar of state governance. The state employs a multi-faceted and multipronged surveillance strategy encompassing physical monitoring, digital surveillance, intelligence infiltration of political parties and civic organisations and systematic data collection through telecommunications infrastructure. The surveillance apparatus operates through three primary institutions: the Central Intelligence Organisation (CIO),1 the military intelligence (MI) arm of the Zimbabwe Defence Forces (ZDF),2 and the Zimbabwe Republic Police (ZRP).3 These security agencies function with minimal, if any, oversight and broad legal authority granted through legislation such as the Interception of Communications Act (2007) and the Cyber and Data Protection Act (2021).

Founding independence leader Robert Mugabe's regime relied on a mix of colonialera secrecy laws (e.g. the Official Secrets Act) and institutions such as the CIO and laid the foundations for digital surveillance. While current President Mnangagwa has retained many of the colonial and Mugabe-era repressive laws and institutions, his administration is distinguished by a qualitative escalation, that is, the incorporation of digital surveillance technologies, mass data interception, and biometric electoral monitoring. Where Mugabe built the scaffolding of authoritarian control, Mnangagwa engineered a technologically enhanced surveillance apparatus that monitors, anticipates, and neutralises threats in real-time.

Surveillance often precedes and enables repression: it has facilitated arbitrary arrests, abductions, torture, enforced disappearances, and extrajudicial killings, illustrating the systemic entanglement of intelligence gathering with coercive state violence.4 Consequently, pervasive surveillance has cultivated and engendered widespread fear among citizens and produced chilling effects across civic life including reduced participation in democratic and civic spaces, self-censorship by journalists and a decrease in investigative journalism. Several survivors of state sponsored surveillance and the resultant brutality report enduring trauma, paranoia, and mistrust, underscoring the longterm psychosocial effects of authoritarian surveillance. 6 Many others are either fearful or too traumatized to share their experiences at the hands of Zimbabwe's security agents.

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

MOZAMBIQUE'S FIGHT AGAINST TERRORISM, FREEDOM AND SOCIO-ECONOMIC JUSTICE

BY INTELWATCH

DOWNLOAD MANUAL

Executive summary

The conflict in Mozambique's northern province of Cabo Delgado, which has raged since 2017, is conventionally understood as a jihadist insurgency. This report argues that such a narrow framing is dangerously insufficient.

The crisis is more accurately diagnosed as a profound "decivilisation process", that is, a process of social breakdown,1 and violent regression of the state driven by a toxic confluence of three systemic failures. The conflict is the product of a fractured state that has failed to secure a legitimate monopoly on violence; a neocolonial extractive economy that deepens historical marginalisation; and a development model that manufactures catastrophic risks with organised irresponsibility.2 The primary failure is that of state formation. The Mozambican state never completed the state formation process of establishing a legitimate monopoly over the means of violence and taxation.3 The national army, the Forças Armadas de Defesa de Moçambique (FADM), is a hollow institution, crippled by decades of political neglect, endemic corruption, and logistical collapse. Its operational incapacity and frequent human rights abuses against the very population it should protect have stripped it of legitimacy, transforming it into just one more predatory actor in a crowded field. A chaotic array of coercive forces has filled this vacuum.

Secondly, this crisis of the state is built upon a foundation of profound socio-economic injustice, a dynamic best understood as a modern iteration of the "global colour line."4 1 The multi-billion-dollar Liquefied Natural Gas (LNG) projects, led by multinationals such as TotalEnergies, have not alleviated the region's historical marginalisation but have instead carved a new, more brutal dividing line between a protected, globalised extractive enclave and an impoverished local periphery. This has manifested as a classic "resource curse," where the promise of immense wealth has only exacerbated inequality and conflict. This has created a fertile ground for radical ideologies that promise an alternative identity and a path to dignity through resistance.

Thirdly, the entire catastrophe has been accelerated by the logic of a "risk society."5 The decision to pursue mega-projects in a volatile and neglected region unleashed a series of "manufactured risks"—social displacement, environmental degradation, and intensified conflict—that were systematically downplayed. The subsequent security collapse is a manifestation of "organised irresponsibility," a system in which both corporate and state actors are structured to evade accountability for the devastating consequences of their decisions. As findings have demonstrated, the potential negative impacts were known beforehand, as per the analyses and assessments presented – namely in the reports of Total Energies itself and of independent entities – but these were incomplete, failing to conform with Total Energies' obligations regarding due diligence, transparency, environmental and social impacts and human rights.6 This is the first part of a two-part series reporting on the counter-terrorism laws and operations' impact on human rights and democratization in Mozambique. Part I will provide a general analysis of the underlying causes of the conflict with a focus on the socio-economic costs of the war while Part II will provide a deeper analysis on the armed groups and the impact of the laws on key civil and political liberties.

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

MOÇAMBIQUE A LUTA CONTRA O TERRORISMO, A LIBERDADE E A JUSTIÇA SOCIOECONÓMICA

BY INTELWATCH

DOWNLOAD MANUAL

Executive summary

A guerra contra o terrorismo em Moçambique tem sido travada em simultâneo com a guerra contra a liberdade e a democracia. A situação em Cabo Delgado tem servido como uma plataforma para securitizar a administração e a forma de governar o país.

Serviu durante o mandato do Presidente Filipe Nyusi (2015-2024) como uma plataforma de expansão dos variados interesses económicos que se solidificaram à volta da elite étnica Makonde no poder e de terceiros, em particular a França e o Ruanda. Essa mesma elite usou a guerra como um escudo contra a liberdade de informação e de imprensa. Por outro lado, expandiu as fragilidades políticas, fraturas sociais e o défice democrático do país. Internamente, dentro do partido no poder a FRELIMO, serviu para pressionar e silenciar vozes contestatárias ao desgoverno do país. Matou o debate interno e afirmou a autocracia tribal com o controlo total das Forças de Defesa e Segurança(FDS) pela tribo do presidente Filipe Jacinto Nyusi, os Makonde. Apesar da cosmética composição dos pelouros da defesa, inteligência e interior, na era Nyusi quem controlava os dossiers e quase sempre à revelia dos seus incumbentes e com os seus companheiros no que passou a ser chamado de Conclave Makonde. Esta repressão e a desgovernação podem piorar durante a presidência de Daniel Chapo.

Desde as eleições de 9 de outubro de 2024 que Moçambique vive numa situação de crise política no país que já resultou em cerca de 350 mortos (algumas estatísticas 1 indicam mais de 400).1 As manifestações com índices e inusitadas formas de violência (violência urbana, policial, desobediência civil, desordem pública, saques e ação localizada de grupos paramilitares) deixaram, além do rasto de mortes e milhares de feridos, várias infraestruturas destruídas e um pesado impacto nas economias vizinhas.2 Neste conflito latente e de baixa intensidade que persiste no país as forças de segurança têm sido usadas para reprimir manifestações, criando um contexto securitário em que a oposição também foi equacionada com terroristas urbanos.

A célebre expressão de Ésquilo (525 - 456 a.C.) “Na guerra a primeira vítima é a verdade” assenta perfeitamente no conflito que desde outubro de 2017 grassa a província de Cabo Delgado. Nota-se do lado estatal um enorme esforço de omitir factos que despontam das dimensões desta guerra, como por exemplo a continuidade do tráfico de minerais, da droga e de espécies proibidas. Este relatório explica e analisa os contextos da violência extremista em Cabo Delgado e da reação do Estado pelas suas instituições de defesa e segurança. Analisa brevemente as ondas concêntricas desta violência conjugada sobre as liberdades constitucionalmente consagradas e sobre a atividade jornalística em específico.

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE UPDATES

THREATS TO PEOPLE WHO USE WHATSAPP IN SOUTH AFRICA

IMAGE SOURCE: MY BROADBAND

In South Africa, WhatsApp users face growing security threats as cybercriminals increasingly exploit the app's voice features, such as voice notes and calls, to harvest voice biometrics. These stolen voices can be used to create deepfake audio for scams like extortion and fake distress calls. Silent calls are a method criminals use to confirm active phone numbers, enhancing the value of stolen personal data for fraudulent purposes. Despite WhatsApp's end-to-end encryption, users remain vulnerable because recorded voice notes can be misused once shared. Experts advise users to adopt strict verification practices, such as using safe words and verifying callers' identities, to guard against sophisticated scams. Digital literacy and vigilance are crucial defenses against these evolving threats. The risks highlight the increasing sophistication of cybercriminal tactics targeting personal data and voice biometric information on WhatsApp in South Africa - My Broadband

WITS UNIVERSITY'S IT SYSTEM HIT BY CYBERATTACK

IMAGE SOURCE: ENCA

Wits University in Johannesburg experienced a cyberattack that compromised some of its IT systems, part of a larger, multi-country zero-day attack exploiting previously unknown software vulnerabilities without available patches. Despite the breach, university operations remain unaffected and ongoing. Wits is collaborating with Oracle and cybersecurity experts to assess the scope of data potentially compromised, and the incident has been reported to the Information Regulator as part of compliance requirements - eNCA

INTEL WATCH

Watching the watchers. Guarding the guardians.

SOUTH AFRICA IS UNDER CYBER ATTACK

IMAGE SOURCE: MY BROADBAND

ISouth Africa is experiencing a significant rise in cyber attacks, with a 14% increase in cybercriminal activities between July 2024 and July 2025, resulting in over 2,100 attacks per week targeting businesses and government departments. The attacks include various forms of cybercrime such as extortion, ransomware, and state-sponsored hacking, posing substantial risks to the country's digital infrastructure and security. Government sectors are notably affected, facing thousands of cyberattacks weekly, highlighting the urgent need for enhanced cybersecurity measures and awareness to protect critical assets and data from persistent cyber threats. - My Broadband

INFRASTRUCTURE GAPS EXPOSE SA FIRMS TO CYBER ATTACKS

IMAGE SOURCE: IT WEB

South African businesses face heightened cyber attack risks due to critical infrastructure vulnerabilities such as load-shedding and reliance on unstable backup systems, which are often targeted by ransomware attackers. The growing prevalence of remote work exposes companies to additional threats from unsecured home networks and devices. The country also suffers from a severe shortage of cybersecurity skills, as talented professionals frequently leave for international markets, limiting local defensive capabilities. Economic pressures force businesses to make challenging trade-offs between immediate operational demands and long-term security investments. Despite increasing awareness that no organization is immune to cyber threats, regulatory complexities like the Protection of Personal Information Act add to operational burdens. Overall, these factors create a complex threat landscape for South African firms, undermining service delivery and economic stability. - IT Web

INTEL WATCH

Watching the watchers. Guarding the guardians.

SIGNAL CALLS ON GERMANY TO VOTE AGAINST 'CHAT CONTROL,' SAYING IT WOULD LEAVE EU MARKET

IMAGE SOURCE: THE RECORD

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 - The Record

FACIAL RECOGNITION TURNS DATING APPS INTO A NEW SURVEILLANCE FRONT

IMAGE SOURCE: BIOMETRIC UPDATE

Facial recognition technology is increasingly transforming dating apps into tools of mass surveillance, raising significant privacy and safety concerns. Platforms like Cheaterbuster and CheatEye allow users to upload a single photo to uncover a person's dating profile and approximate location by leveraging vast biometric databases built from billions of scraped images online. These services, popularized by viral influencer campaigns, exploit exposed user data and subtle in-app location indicators to map users' neighborhoods, potentially enabling stalking, harassment, blackmail, or violence, especially for vulnerable groups like LGBTQ individuals. Dating apps such as Tinder and Bumble have introduced facial verification systems aimed at preventing bots and fakes, but these also generate large biometric data repositories that risk misuse or breaches. Legal frameworks lag behind these developments, with limited enforcement primarily in Illinois and Europe, while the industry ecosystem creates a persistent, searchable archive of intimate data. Experts warn this surveillance ecosystem erodes privacy, turning intimate relationships into constant monitoring and surveillance under the guise of safety and accountability - Biometric Update

INTEL WATCH

Watching the watchers. Guarding the guardians.

ANDROID SPYWARE IN THE UAE MASQUERADES AS ... SPYWARE

IMAGE SOURCE: DARK READING

Android spyware campaigns in the UAE, identified as ProSpy and ToSpy, masquerade as legitimate versions or add-ons of secure messaging apps Signal and ToTok. These spyware families are manually installed from deceptive third-party websites mimicking official app stores like Samsung Galaxy Store, bypassing official app stores entirely. Once installed, they maintain persistence on devices and exfiltrate a wide range of sensitive data, including contacts, SMS, photos, chat backups, and device information, with ToSpy particularly targeting ToTok backup files for conversation history extraction. These spyware operations have been ongoing since around mid-2022, with active command-and-control servers noted in 2025. Users are advised to only install apps from official sources, disable unknown source installations, and keep Google Play Protect enabled, which now automatically blocks these spyware variants. The campaigns highlight a growing digital privacy threat targeting privacy-conscious users in the UAE through sophisticated impersonation and social engineering techniques - Dark Reading

NEW CLAYRAT SPYWARE TARGETS ANDROID USERS VIA FAKE WHATSAPP AND TIKTOK APPS

IMAGE SOURCE: THE HACKER NEWS

The ClayRat Android spyware campaign, primarily targeting users in Russia, spreads through fake Telegram channels and phishing websites that impersonate popular apps like WhatsApp, TikTok, Google Photos, and YouTube. It tricks victims into downloading malicious APKs by inflating download counts and using fake reviews, often hiding its true payload behind fake update screens. Once installed, ClayRat can steal SMS messages, call logs, notifications, device information, and even take photos with the front camera. It aggressively propagates by sending malicious SMS messages to all contacts in the infected device, turning each device into a distribution node. The spyware exploits Android's default SMS handler role to bypass permission prompts and access sensitive data stealthily. Over 600 samples and 50 droppers have been detected in the past three months, each iteration increasing its evasiveness against security tools. Protection relies on user vigilance to avoid sideloading apps outside official stores and on security solutions like Google Play Protect that can detect known variants - The Hacker News

INTEL WATCH

Watching the watchers. Guarding the guardians.

ALTAMIDES – THE NEW SPYWARE THAT CAN INFILTRATE YOUR PHONE WITHOUT A TRACE

IMAGE SOURCE: PPSA

Altamides, developed by Jakarta-based First Wap, is an advanced spyware system that infiltrates smartphones without installing malware or leaving digital traces, unlike Pegasus. It exploits vulnerabilities in the outdated telecom network protocol SS7 to covertly track real-time locations, intercept calls and text messages, extract data from encrypted messaging apps, and monitor user movements. This technology, marketed to government entities for fighting organized crime and terrorism, has been used globally, with leaked data revealing extensive surveillance of targets in over 100 countries. Recent investigative journalism exposed how Altamides is sold through intricate channels, including evasion of international sanctions, and how it can deploy pervasive spying capabilities without tipping off victims through typical spyware symptoms like device slowdown or battery drain. The spyware's stealth and breadth pose serious privacy and human rights concerns, exacerbated by weak telecom security and inadequate regulatory oversight worldwide - PPSA

SALT TYPHOON HIT GOVERNMENTS ON THREE CONTINENTS WITH SHAREPOINT ATTACKS

IMAGE SOURCE: THE REGISTER

China-based threat actor groups, including Salt Typhoon, exploited a critical zero-day vulnerability in Microsoft SharePoint servers called ToolShell (CVE-2025-53770), before a patch was released in July 2025. These attackers targeted over 400 organizations globally, comprising government agencies, telecommunications companies, universities, finance firms, and critical infrastructure, across multiple continents including the Middle East, Africa, South America, Europe, and the US. Salt Typhoon notably used malware like Zingdoor, an HTTP backdoor, ShadowPad Trojan, and KrustyLoader to steal credentials and maintain sustained, stealthy access for espionage. Other Chinese groups such as Linen Typhoon and Violet Typhoon also exploited this flaw. The attacks involved techniques like DLL sideloading and exploitation of SQL and Apache ColdFusion server vulnerabilities for initial access. The widespread attacks indicate mass scanning to identify vulnerable networks before executing targeted intrusions, highlighting severe risks to critical government and private sector systems worldwide - The Register

INTEL WATCH

Watching the watchers. Guarding the guardians.

APPLE'S IOS 26 UPDATE BREAKS ABILITY TO DETECT SPYWARE INFECTIONS

IMAGE SOURCE: CYBER INSIDER

The iOS 26 update has introduced a significant change that hinders the detection of spyware infections such as Pegasus and Predator by altering the behavior of the shutdown.log file, a critical forensic artifact stored within Apple's Sysdiagnose tool. Previously, this log preserved entries across device shutdowns and reboots, enabling researchers to identify subtle indicators of advanced spyware activity. However, with iOS 26, the shutdown.log is now overwritten every time the device restarts, erasing historical data and removing a key source of forensic evidence. This change appears systemic, likely aimed at improving performance or system hygiene, rather than a deliberate move to aid spyware developers. Nevertheless, it undermines a vital layer of spyware detection, raising concerns amidst ongoing high-profile spyware campaigns targeting journalists, government critics, and other high-risk users. Apple has yet to clarify whether this change is intentional or a regression. Meanwhile, experts advise high-risk users to generate and securely store a sysdiagnose file before updating, to preserve forensic data potentially crucial for detecting infections - Cyber Insider

NY SCHOOL DISTRICT'S AI-POWERED CLASSROOM SURVEILLANCE WORRIES CIVIL LIBERTIES ADVOCATES

IMAGE SOURCE: STATE SCOOP

The Plainedge Union Free School District in Long Island, New York, has installed an AI-powered emergency response and threat detection system from XSponse, becoming the first US district to do so. The $250,000 system includes auto-locking doors, constant audio monitoring with AI voice activation for keywords, and situational video monitoring with two cameras per classroom that activate only during lockdowns. Cameras have physical shutters for privacy, but if a lockdown is triggered, law enforcement and administrators can remotely control them. Staff carry smart badges with panic buttons linked to a mass-notification system. The New York Civil Liberties Union criticized the installation for lack of public disclosure and privacy risks to students, noting broader concerns about AI surveillance in schools. Critics worry about excessive monitoring, data privacy, and the effectiveness of such systems, emphasizing the need for transparency and cautious spending of public funds on surveillance technologies in education - State Scoop

INTEL WATCH

Watching the watchers. Guarding the guardians.

REPRESSION MONITOR

AI PROMISES IN ETHIOPIA SHADOWED BY DEEPFAKES AND RESTRICTED INTERNET FREEDOMS, SAYS NEW REPORT

IMAGE SOURCE: SHEGA

A new report by CIPESA highlights Ethiopia's early AI adoption amid substantial challenges. While AI shows promise for governance and service delivery, Ethiopia faces low internet penetration (21%) and restricted digital freedoms, scoring 27/100 on Freedom House's Internet Freedom Index. The country is battling a surge in AI-driven misinformation, deepfakes, and state surveillance, which exacerbate ethnic tensions, intimidate journalists and activists, and deepen social exclusion, especially for women, rural populations, and minorities. The government's national AI policy and strategies aim for responsible AI use aligned with African Union digital transformation goals, with increased investment exemplified by a 42% budget rise for the Ethiopian Artificial Intelligence Institute. However, realizing Ethiopia's "digital future" requires stronger regulations, transparency, local data sets to reduce bias, and education campaigns to prepare citizens for the AI era- Shega

LICENSE TO WATCH: HOW UGANDA'S DIGITAL NUMBER PLATES BECAME SPY TOOLS

IMAGE SOURCE: THE INDEPENDENT

Uganda's digital number plates, part of the broader Intelligent Transport Monitoring System (ITMS), have transformed traditional vehicle identification into a sophisticated surveillance tool. Developed through a partnership with Russian firm Joint Stock Company Global Security, these plates embed RFID chips and QR codes to enable real-time vehicle tracking, monitoring movement, and locating vehicles across the country. The system is integrated with Uganda's CCTV networks, police databases, and taxi authority records, effectively creating a pervasive surveillance grid. While officially aimed at enhancing traffic management and curbing vehicle theft, critics warn that the system is increasingly being used for political surveillance, targeting opposition figures, activists, and critics, raising severe concerns over privacy, data security, and potential misuse. The secrecy surrounding key operational facilities and the system's integration with other surveillance infrastructure underscore fears of an expanded, invasive state surveillance apparatus lacking robust legal safeguards. - The Independent

INTEL WATCH

Watching the watchers. Guarding the guardians.

NIGERIA'S GOVERNMENT IS USING DIGITAL TECHNOLOGY TO REPRESS CITIZENS

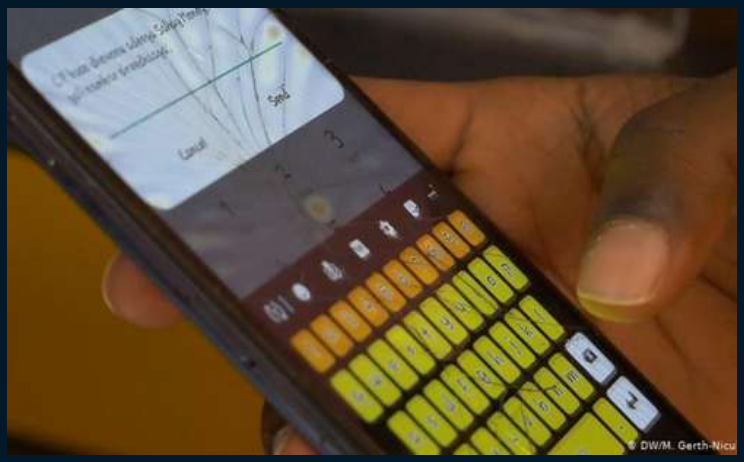


IMAGE SOURCE: ALL AFRICA

Digital authoritarianism is rising in Africa, with governments using digital tools for control under the guise of national security, regime survival, counterterrorism, electoral competition, and modernization. The Nigerian case illustrates this trend, where government repression has extended into digital spaces, including social media shutdowns and efforts to build internet firewalls modeled on China's Great Firewall to censor and monitor online content. Foreign suppliers from countries like China, Russia, Israel, France, and the US provide these technologies and expertise, often motivated by economic and geopolitical interests. Although some technologies serve development needs, they have dual use potential for repression. Addressing digital authoritarianism requires global efforts to restrict the sale of repressive technologies, addressing broader political repression, and establishing legal and institutional oversight with human rights safeguards to protect digital freedoms and privacy- All Africa

ISRAEL'S USE OF AI-DSS AND FACIAL RECOGNITION TECHNOLOGY: THE EROSION OF CIVILIAN PROTECTION IN GAZA

IMAGE SOURCE: LIEBER INSTITUTE

Israel's use of artificial intelligence decision-support systems (AI-DSS) like Lavender and facial recognition technology in Gaza has drastically eroded civilian protections under international humanitarian law. These systems generate "kill lists" by scoring Palestinians for suspected militant affiliations with a high reported error rate, leading to widespread misidentifications and civilian casualties. Facial recognition checkpoints forcibly collect biometric data, often without consent, raising serious legal and ethical concerns, including potential violations of protection against coercion and privacy under international law. The lowered threshold for classifying individuals as militants and minimal review of AI-generated targets prioritize quantity and speed over accuracy and human judgment, undermining principles of distinction and proportionality. This reliance on flawed AI-driven targeting risks cognitive biases and reduces critical human decision-making in military operations, exacerbating civilian harm and threatening fundamental protections during armed conflict - Lieber Institute

HOW TECHNOLOGY COMPANIES SHIP SURVEILLANCE AI TO FRAGILE STATES

IMAGE SOURCE: VERDICT

Technology companies are increasingly supplying AI-powered facial recognition and surveillance tools to fragile and authoritarian states under the guise of public safety and smart city development. These systems, marketed as ways to improve security, emergency response, and crime prevention, often facilitate mass surveillance and data harvesting that disproportionately target marginalized populations and suppress dissent. Such deployments frequently occur without robust regulatory oversight or transparency, leading to abuses including privacy violations and political repression. Regulations lag behind the rapid export and use of these intrusive technologies, which can entrench authoritarian control and erode human rights, particularly in countries with weak legal protections and governance. This practice raises significant ethical questions about the responsibility of tech firms in enabling oppressive surveillance regimes under commercial pretenses - Verdict

[OPINION] TURKEY'S DIGITAL AUTHORITARIANISM: HOW ERDOĞAN PERFECTED THE ART OF INVISIBLE REPRESSION

IMAGE SOURCE: TURKISH MINUTE

Turkey under President Recep Tayyip Erdoğan exemplifies a modern digital authoritarian regime that suppresses dissent through "invisible repression," using technology as a tool for control rather than liberation. This system employs extensive digital surveillance, censorship, manipulation, and legal intimidation to monitor citizens via facial recognition, metadata analysis, and internet throttling. The government criminalizes online expression and floods social media with propaganda and disinformation to shape public opinion. Since the 2016 coup attempt, Erdoğan's regime has institutionalized digital repression through laws granting broad censorship powers and surveillance capabilities integrated with Chinese technologies. The state uses these tools not only to silence opposition and journalists but also to induce self-censorship among citizens, creating an atmosphere of fear without overt legal bans on speech. This model of digital authoritarianism blends advanced surveillance with a legal façade, maintaining control by embedding repression within national security and anti-disinformation rhetoric - Turkish Minute

INTEL WATCH

Watching the watchers. Guarding the guardians.

HOW ICE SPIES ON WHATSAPP

IMAGE SOURCE: FORBES

ICE uses WhatsApp surveillance to assist in immigration enforcement by monitoring metadata from suspects' WhatsApp accounts rather than accessing encrypted message content. A 2024 warrant revealed that ICE's Homeland Security Investigations unit obtained a pen register order to collect data such as contacts and timing of communications from a woman suspected of distributing fake IDs. Using this metadata, ICE agents cross-referenced multiple databases to identify individuals interacting with the suspect, highlighting how metadata alone can reveal extensive personal networks. This method is part of ICE's broader expansion of digital surveillance tools, including facial recognition, phone-hacking spyware, and social media monitoring to track and target undocumented immigrants and alleged domestic threats. Civil rights advocates express concern that these powerful tools may dangerously infringe on privacy and freedom of expression - Forbes

GREEK WATCHDOG REPORTS SHARP INCREASE IN SECRET WIRETAPS

IMAGE SOURCE:BUSINESS AND HUMAN RIGHTS RESOURCE CENTER

The Italian government admitted to using Israeli spyware from Paragon Solutions to target pro-immigration activists and members of migrant rescue groups, notably Mediterranean NGOs, between 2023 and 2024 as part of investigations related to combating illegal immigration. The Parliamentary Committee for the Security of the Republic (COPASIR) confirmed that this surveillance was legally authorized and overseen by prosecutors, though civil rights groups criticized the government for framing human rights advocates as national security threats. While the government denied spying on journalists, at least one investigative journalist claimed to have been targeted. Political fallout led Italy to terminate its contracts with Paragon following a media scandal and public outcry regarding the misuse of spyware for political surveillance. The episode highlights ongoing concerns about state surveillance overreach, lack of transparency, and the criminalization of migration assistance under the guise of national security - Business and Human Rights Resource Center

INTEL WATCH

Watching the watchers. Guarding the guardians.

ICE JUST BOUGHT NEW TOOL TO MONITOR HUNDREDS OF MILLIONS OF SMARTPHONES. EXPERTS SAY IT'S DANGEROUS

IMAGE SOURCE: INDEPENDENT

U.S. Immigration and Customs Enforcement (ICE) has acquired a powerful surveillance tool from PenLink that enables tracking of hundreds of millions of mobile phones daily by compiling billions of location data points. This tool, which also includes face detection, advanced facial search, and dark web data monitoring, allows ICE agents to monitor people's locations without needing a warrant, exploiting legal loopholes around purchasing sensitive data from commercial brokers. The acquisition reverses privacy reforms under the Biden administration that previously restricted such mass surveillance practices. Privacy advocates warn this technology could lead to unconstitutional warrantless surveillance and enable ICE to target not only immigration suspects but also lawful citizens and protesters. The surveillance capability is part of a broader expansion of ICE's high-tech monitoring arsenal, including facial recognition linked to government databases, mobile phone hacking tools, and AI analytics on social media and dark web data, raising concerns about civil liberties, privacy, and overreach under the current Trump administration - Independent

GREEK WATCHDOG REPORTS SHARP INCREASE IN SECRET WIRETAPS

IMAGE SOURCE: GREEK CITY TIMES

A report by the Hellenic Authority for Communication Security and Privacy (ADAE) reveals a 23% surge in state-sanctioned wiretaps in Greece during 2024 and early 2025, largely justified by vague "national security" reasons without detailed judicial oversight. This rise follows a temporary dip in 2023 linked to backlash against illegal surveillance involving Predator spyware and parallel networks operated by the National Intelligence Service (EYP). Most wiretaps are now initiated by the Counter-Terrorism Service and EYP through prosecutorial orders, bypassing rigorous court scrutiny. Meanwhile, court-approved wiretaps for organized crime have declined by 8%. ADAE calls for legislative reforms to grant it broader powers to inspect surveillance agencies, seize evidence of violations, and destroy illegally obtained data. Despite security officials citing the need to monitor extremist groups and prison communication, experts say the rationale does not fully explain the spike in wiretaps. The report warns that unchecked state surveillance is increasing again, undermining citizens' privacy rights under the pretext of national security - Greek City Times

INTEL WATCH

Watching the watchers. Guarding the guardians.

AN INVISIBLE WEB: THE SHADOW OF DIGITAL SURVEILLANCE LAWS

IMAGE SOURCE: THE PRINT

India's digital surveillance laws create a broadly enabling environment for government agencies to conduct extensive electronic monitoring and data interception with limited oversight. Central pieces of legislation include Section 69 of the IT Act, 2000, allowing the interception and decryption of information under vague terms such as “public safety” and “sovereignty,” and the pre-Independence Indian Telegraph Act authorizing communication interception with minimal transparency. The recently enacted Digital Personal Data Protection (DPDP) Act, 2023, while framed as a privacy safeguard, contains broad exemptions that allow government processing of personal data without consent for legal obligations, further expanding state access. Surveillance procurements and deployments often lack public accountability, aided by secretive budgets and unclear forensic protocols when confiscating devices from journalists and activists. Pressure on platforms to facilitate traceability and gateway access into encrypted communications intensifies state control over digital footprints. Real-world impacts include targeting of journalists, activists, and political opponents through device seizures and data extraction often linked to financial or anti-terror investigations. These legal and technical frameworks collectively suppress civil discourse, induce self-censorship, and undermine digital privacy rights essential to democratic functioning - The Print

AMAZON'S RING CAMERAS PUSH DEEPER INTO POLICE AND GOVERNMENT SURVEILLANCE

IMAGE SOURCE: AOL

Amazon's Ring security cameras have deepened their integration with law enforcement through new partnerships, notably with Flock Safety, a company providing AI-powered license-plate readers and surveillance cameras to thousands of police agencies across the U.S. This collaboration enables law enforcement to send "Community Requests" via the Ring Neighbors app, inviting Ring camera owners to voluntarily share video footage relevant to criminal investigations in their area. The requests specify case details and timeframes, and while participation remains voluntary, the system streamlines police access to vast troves of private video surveillance. The Ring footage shared with police is securely stored on Flock’s platform, addressing previous concerns about chain-of-custody issues. Privacy advocates raise alarms about the blurred lines between voluntary cooperation and amplified government surveillance, especially given reports that ICE and other federal agencies access Flock's extensive surveillance networks. The partnerships mark an expansion of Ring's role in mass surveillance, raising critical debates about privacy, consent, racial profiling, and the potential misuse of video data by authorities - AOL

INTEL WATCH

Watching the watchers. Guarding the guardians.

UNIONS SUE TRUMP ADMINISTRATION OVER ALLEGED IDEOLOGICAL SURVEILLANCE ON SOCIAL MEDIA

IMAGE SOURCE: CUBA HEADLINES

Three major U.S. labor unions—the United Auto Workers, Communications Workers of America, and American Federation of Teachers—have filed a lawsuit against the Trump administration accusing it of using artificial intelligence and social media surveillance to monitor and suppress the online expression of lawful non-citizen visa holders and permanent residents. The lawsuit alleges the government targets those who post political opinions it disfavors, including criticisms of U.S. policies, support for Palestine, or commentary on specific incidents like the killing of conservative activist Charlie Kirk, with punishments including visa revocation and deportation. The lawsuit, supported by the Electronic Frontier Foundation, frames these surveillance and punitive actions as unconstitutional violations of free speech and association rights, causing significant chilling effects and self-censorship among union members and affecting their ability to organize and communicate. It highlights the surveillance program as an interagency effort lacking sufficient judicial oversight, using large-scale data collection and AI tools to enforce ideological conformity - Cuba Headlines

---

AS 'NO KINGS' PROTESTS DENOUNCE TRUMP, SURVEILLANCE WORRIES EMERGE - RED LAKE NATION NEWS

IMAGE SOURCE: RED LAKE NATION NEWS

The "No Kings" protests on October 18, 2025, were a massive nationwide movement against President Donald Trump's policies and perceived authoritarian rule, with events held at over 2,700 locations across the U.S. and international solidarity actions. Organizers estimated attendance near 7 million, making it one of the largest single-day protests in U.S. history. The protests united diverse groups opposing Trump's immigration enforcement, federal budget cuts to education and environment, and other policy issues, emphasizing democracy and constitutional rights. These largely peaceful demonstrations were marked by warnings of authoritarianism and calls to protect democracy. Amid the protests, concerns about surveillance emerged as activists and participants feared government monitoring and repression in response to the large-scale dissent. Some states mobilized National Guard troops, and there was heightened awareness about law enforcement surveillance capabilities potentially targeting organizers - Red Lake Nation News

INTEL WATCH

Watching the watchers. Guarding the guardians.

NEW ORLEANS AI SURVEILLANCE CAMERAS: PUBLIC SAFETY OR PRIVACY VIOLATION?

IMAGE SOURCE: THE TULANE HULLABALOO

The New Orleans Police Department (NOPD) secretly installed around 200 AI-driven facial recognition cameras across the city through a partnership with Project NOLA, a nonprofit headquartered at the University of New Orleans, using a vast network of nearly 5,000 cameras owned by homes and businesses. These cameras use AI to scan faces and license plates, comparing them against databases from mugshots, driver's licenses, and social media to identify suspects in real time, notifying officers immediately. While the program contributed to crime reduction—including an 80% decrease in gun violence in a high-crime area and a 39% drop in murders citywide—there are growing privacy concerns. The surveillance program violates a 2022 city ordinance restricting facial recognition use to specific investigations, risking false arrests, especially given AI's lower accuracy for people of color, women, and older adults. Many residents remain unaware of the cameras, sparking debates about privacy, transparency, and the balance between public safety and civil liberties. The city council later moved to formalize and regulate this live surveillance program, which has broad implications for policing and surveillance nationwide - The Tulane Hullabaloo

MOSCOW USING FACIAL RECOGNITION TO DETAIN MEN CHALLENGING MILITARY CONSCRIPTION, RIGHTS GROUP SAYS

IMAGE SOURCE: THE MOSCOW TIMES

Moscow police are using facial recognition technology in the metro system to detain men who have legally challenged their military conscription orders, according to the Civil Alliance of Russia rights group. When individuals appeal their draft decisions in court, their data is flagged in government databases as draft dodgers, leading to automatic detention when flagged by surveillance cameras. A 19-year-old man contesting his call-up was detained in the metro and taken to a conscription center along with around 20 others similarly identified. Lawyers have been reportedly denied access to detainees even with notarized power of attorney. Authorities have advised men appealing drafts to avoid metro use and to contest detentions legally. This fall's conscription campaign is the largest since 2016, with plans to call up 135,000 men aged 18 to 30. Detained individuals face penalties including restrictions on travel, financial activities, driving, and possible fines, as well as potential military service. The use of facial recognition for enforcement highlights concerns about privacy and human rights amid increased conscription efforts - The Moscow Times

INTEL WATCH

Watching the watchers. Guarding the guardians.

INTELLIGENCE AGENCIES

NEWLY SIGNED CYBERCRIME LAW SPARKS LEGAL SHOWDOWN AND SOCIAL MEDIA UPROAR IN KENYA

IMAGE SOURCE: DAWAN AFRICA

Kenya's newly signed Computer Misuse and Cybercrimes (Amendment) Act, 2025, expands and updates the original 2018 law to address modern digital threats including cyber fraud, digital terrorism, identity theft, and harmful online content. It grants authorities powers to swiftly block websites and mobile apps promoting illegal activities like terrorism and child exploitation, marking a significant shift towards tighter control over online content. The law modernizes definitions to include virtual assets and cybercrimes, introduces stringent penalties, and mandates critical information infrastructure providers to report incidents within 24 hours and store sensitive data locally. However, a Kenyan High Court has recently suspended key provisions criminalizing the publication of false or misleading information due to concerns over potential abuse and threats to free expression, reflecting ongoing legal and social debates around balancing cybersecurity with civil liberties- Dawan Africa

MORE THAN 60 UN MEMBERS SIGN CYBERCRIME TREATY OPPOSED BY RIGHTS GROUPS

IMAGE SOURCE: RFI

The United Nations Convention against Cybercrime, signed by 65 member states in Hanoi in October 2025, is a landmark global treaty aimed at strengthening international cooperation to prevent and combat cybercrime, including offenses such as ransomware, financial fraud, terrorism, and online trafficking. The treaty establishes legal standards for investigation, prosecution, and sharing electronic evidence across borders, as well as a 24/7 network for rapid cooperation. While hailed by UN officials as a crucial multilateral step for global digital security, the treaty has drawn criticism from rights groups and tech firms who fear it may enable government overreach, data sharing that undermines privacy, and the criminalization of ethical hackers. Concerns focus on ambiguous definitions that could facilitate misuse to suppress dissent and curtail freedoms, making the balance between cybersecurity and human rights a central challenge for its implementation. - RFI

BELARUS BOUGHT SECRETIVE TRACE-FREE SPYWARE USED IN 100 COUNTRIES

IMAGE SOURCE: TVP WORLD

Belarus is among the buyers of Altamides, an advanced, untraceable spyware system developed by the Indonesian company First Wap. Altamides covertly tracks and locates individuals in real-time by exploiting the obsolete SS7 telephony protocol, used worldwide by phone carriers. Unlike traditional spyware like Pegasus, Altamides leaves no digital trace on targeted devices and does not require a victim to click malicious links. It can intercept calls and SMS messages and even access encrypted messaging apps such as WhatsApp. First Wap markets the tool solely to government entities stating compliance with legal mandates, but investigative journalism uncovered that sales include workaround methods to bypass sanctions, and customers include various countries with questionable human rights records. Altamides is capable of pervasive surveillance without the typical signs of malware infection and is used in law enforcement and intelligence operations globally, raising significant concerns about privacy, legality, and abuse in authoritarian contexts - TVP World

FACE ID DATABASE RAISES SECURITY CONCERNS

IMAGE SOURCE: TURKISH MINUTE

The Australian government is launching a National Driver Licence Facial Recognition Solution (NDLFRS) by the end of 2025, integrating facial images from passports and driver's licenses into a centralized biometric verification system. The system aims to enhance identity verification security, reduce identity fraud, and provide government agencies, including law enforcement, with streamlined access to identity databases. It builds on prior projects dating back to 2017, consolidating facial recognition capabilities across states and territories under a federal framework managed by the Attorney-General's Department, supported by legislation introduced in 2024. While the system includes strong privacy safeguards and oversight by the Office of the Australian Information Commissioner, concerns remain around centralization risks, biometric data collection, digital divide issues, and the potential expansion of use into private and less-transparent sectors by 2026. The system's rollout has seen phased data integration, with some states temporarily withdrawing data pending agreement renewals under the new legislative requirements - Government News

INTEL WATCH

Watching the watchers. Guarding the guardians.

SPYWARE MAKER NSO GROUP CONFIRMS ACQUISITION BY US INVESTORS

IMAGE SOURCE: TECH CRUNCH

Israeli spyware maker NSO Group has confirmed that a U.S. investment group led by Hollywood producer Robert Simonds has acquired controlling ownership of the company in a deal valued at tens of millions of dollars. Despite the change in ownership, NSO's headquarters and core operations remain in Israel, continuing under Israeli regulatory oversight including the Ministry of Defense. The acquisition marks the end of involvement from NSO's co-founder and executive chairman Omri Lavie, who will step away from the company. NSO has a controversial history of selling spyware used by governments to hack journalists, activists, and dissidents globally. The deal awaits regulatory approval from both Israeli and U.S. authorities, amid scrutiny over Simonds' past business ties to China. Critics express concern about NSO's intent to enter the U.S. market and its ongoing impact on privacy and security - Tech Crunch

HONG KONG TO INSTALL SURVEILLANCE CAMERAS WITH AI FACIAL RECOGNITION

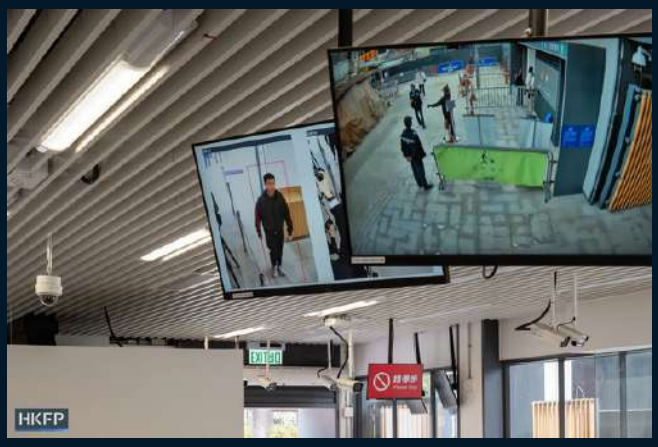


IMAGE SOURCE: HONG KONG FREE PRESS

Hong Kong plans to greatly expand its surveillance network to around 60,000 CCTV cameras equipped with AI-powered facial recognition technology by 2028, increasing from just under 4,000 cameras currently. The expansion is part of the police's SmartView program aimed at crime prevention, national security, and public safety, with AI used to monitor crowds, read license plates, and track criminal suspects in real time. The initiative reflects a closer alignment with Mainland China's extensive use of surveillance technology. While facial recognition could be rolled out as early as the end of this year, the city lacks strong independent oversight and clear regulations governing police use of AI, raising concerns about privacy, potential misuse, and wrongful arrests due to false matches. The program is set to integrate surveillance across public transport, government departments, and housing complexes, utilizing cloud analytics for real-time video analysis and threat detection. The government's privacy office mandates impact assessments and data use guidelines, but civil liberties groups warn of escalated surveillance and erosion of personal privacy - Hong Kong Free Press

INTEL WATCH

Watching the watchers. Guarding the guardians.

TRUMP GOES ON SPYWARE PURCHASING BLITZ TO HELP ICE FIND PEOPLE WHO THEY CLAIM WANT TO 'OVERTHROW OF THE UNITED STATES GOVERNMENT

IMAGE SOURCE: AOL

The Trump administration has embarked on an extensive spyware purchasing spree to equip U.S. Immigration and Customs Enforcement (ICE) with advanced surveillance tools aimed at locating undocumented migrants and individuals it alleges are planning to "overthrow the United States Government." ICE is investing tens of millions in contracts for eye-scanning and facial recognition apps, smartphone hacking software operable without a court warrant, and expanding a social media monitoring network targeting platforms such as Facebook, Instagram, and X. The spyware acquisitions include a $3.75 million contract with Clearview AI for facial recognition software and a reactivated $2 million deal with Paragon Solutions, an Israeli spyware vendor previously banned due to human rights concerns but now U.S.-owned. The expanded surveillance efforts have alarmed lawmakers and civil rights groups who fear the technology will also target political protesters and suppress free speech. ICE's social media monitoring involves analyzing data from friends and associates of individuals of interest, raising privacy and constitutional concerns - AOL

THE U.S. HAS REACTIVATED ITS PARAGON CONTRACT — AND IT SHOULD ALARM EVERYONE

IMAGE SOURCE: ACCESS NOW

The U.S. Immigration and Customs Enforcement (ICE) has reactivated a $2 million contract with Israeli spyware maker Paragon Solutions, which had previously been paused due to concerns over compliance with Executive Order 14093 that restricts federal agencies from using spyware posing significant security or human rights risks. Paragon's flagship spyware, Graphite, has been implicated in human rights abuses globally, including spying on journalists and activists. The contract reactivation follows Paragon's acquisition by U.S.-based private equity, allowing ICE to circumvent restrictions on foreign-owned spyware vendors. This move has alarmed activists and lawmakers who warn of potential misuse, lack of transparency, and violations of constitutional protections such as free speech and privacy. Critics demand immediate suspension of the contract, increased congressional oversight, transparency, and reforms to prevent domestic use of spyware linked to abuses - Access Now

INTEL WATCH

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.

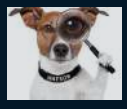
GET INVOLED!

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

Global Dialogue

Luminate

Funded by the European Union

We are grateful for the support of our donors!