Issue #11

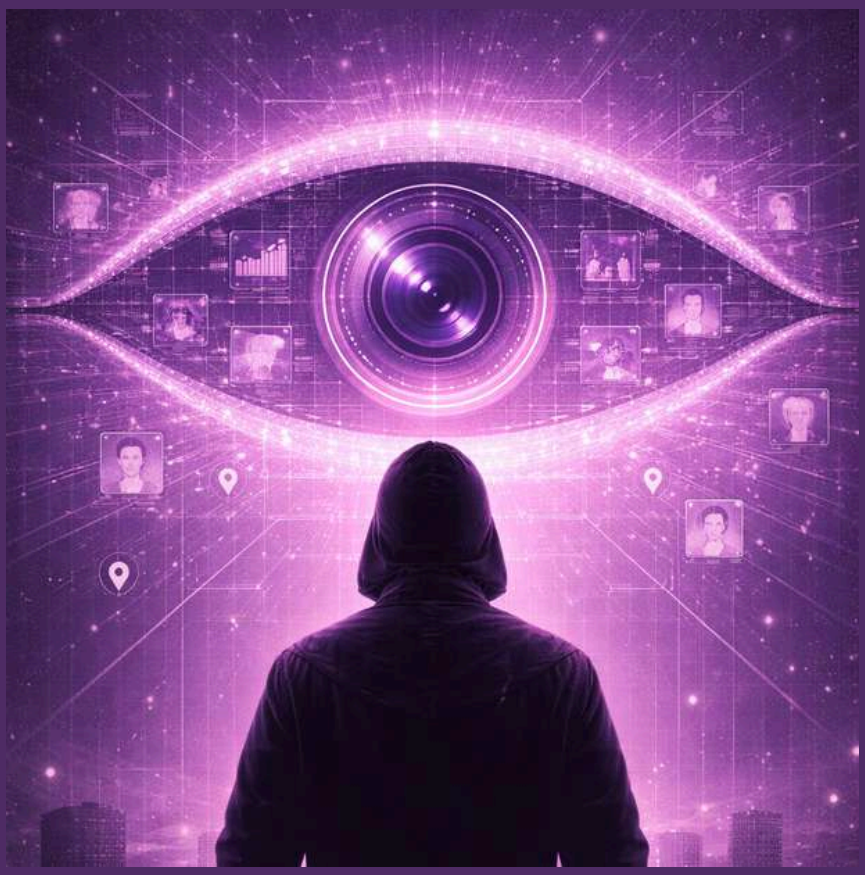
INTEL WATCH

April 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

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE UPDATES

AI DEEPFAKES AND FAKE NEWS: SOUTH AFRICA'S ELECTIONS FACE A NEW HYPER-LOCAL THREAT

IMAGE SOURCE: SA NEWS

The Electoral Commission of South Africa (IEC) is warning that generative AI is likely to reshape election disinformation in the upcoming local government elections by enabling highly targeted, "hyper-local" campaigns that focus on specific wards or communities rather than broad national narratives. Officials say AI tools make it easier to produce convincing deepfakes, fake news posts, and misleading content that can rapidly spread through social media, potentially confusing voters about voter registration, polling processes, and candidate information. The IEC highlights concerns that these tactics could be used to undermine trust in the electoral system by targeting vulnerable points such as the voters' roll, ballot handling, and vote counting. In response, the commission is developing verification tools, rapid-response fact-checking systems, and partnerships with media and civic groups to counter false information in real time and protect electoral integrity. SA News

SOUTH AFRICA WITHDRAWS AI POLICY DUE TO FAKE AI-GENERATED SOURCES

IMAGE SOURCE: ENGINEERING NEWS

South Africa withdrew its draft national artificial intelligence policy shortly after its release for public comment when it was discovered that the document contained fictitious, likely AI-generated academic references, undermining its credibility and integrity. Communications Minister Solly Malatsi acknowledged that the inclusion of unverified citations reflected a serious failure in quality control and oversight, prompting the immediate withdrawal of the policy and an internal investigation, with possible consequences for those responsible. The draft had aimed to position the country as a leader in AI by proposing new governance structures and incentives, but the incident highlighted the risks of relying on AI-generated content without proper human verification and raised broader concerns about how governments use AI in policymaking. Engineering News

LARGE TECHNOLOGY WHOLESALER IN SOUTH AFRICA HIT BY DATA BREACH

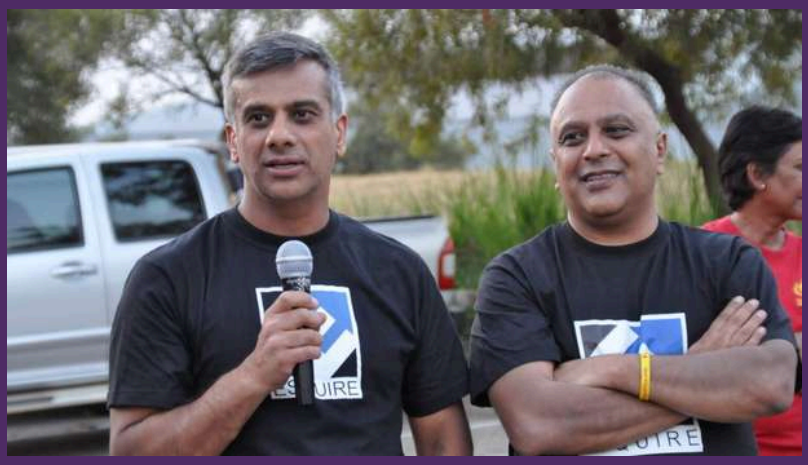


IMAGE SOURCE: MY BROADBAND

The article reports that Esquire - a large South African technology wholesaler - has suffered a data breach affecting part of its online systems, specifically an API-linked database used for order processing. While the company confirmed that its main financial and core systems were not compromised, attackers were able to access limited customer-related information such as company names, email addresses, and order history. The wholesaler says it quickly secured the affected systems, reported the incident to regulators under POPIA requirements, and is working with cybersecurity experts to strengthen its defences. No banking details or highly sensitive personal data were exposed, but customers have been advised to remain cautious due to possible follow-up phishing attempts. My Broadband

---

NEW BANK TAKES SWIFT ACTION AFTER GROUNDUP ALERTS IT TO DATA BREACH

IMAGE SOURCE: GROUNDUP

The article reports that eNL Mutual Bank - a new South African bank - quickly responded to a data breach after being alerted by the investigative journalism organisation GroundUp. The breach involved a misconfigured system that left sensitive customer data publicly accessible online, including personal and financial information. Once notified, the bank took the exposed system offline, confirmed that the issue stemmed from a technical configuration error rather than hacking, and began notifying affected customers while strengthening its security controls. The report also highlights criticism that the Information Regulator South Africa has been slow to respond or take visible action, raising concerns about gaps in enforcement of data protection laws like POPIA. GroundUp

INTEL WATCH

Watching the watchers. Guarding the guardians.

BOOKING.COM DATA BREACH AFFECTS SOUTH AFRICAN USERS

IMAGE SOURCE: MY BROADBAND

The article reports that Booking.com has suffered a data breach affecting some users globally, including South African customers, after attackers gained unauthorised access to reservation-related information. Exposed data may include names, email addresses, phone numbers, and booking details, although the company says payment information was not compromised. Booking.com has begun notifying affected users, resetting reservation PINs, and advising customers to be alert for phishing attempts that could use the leaked details to impersonate hotels or the platform. The incident highlights ongoing cybersecurity risks in online travel services and the growing use of stolen booking data for targeted scams. My Broadband

SAPS MEDICAL AID SCHEME PROBES POTENTIAL DATA BREACH

IMAGE SOURCE: IT WEB

The article reports that the Polmed (the medical scheme serving South African Police Service employees) is investigating a suspected data breach after a threat actor claimed to have accessed its systems and issued an extortion or ransom demand. The scheme confirmed it received a direct claim of compromise on 25 March and is treating the incident as a potential cyberattack while conducting forensic investigations to determine whether any member data was actually accessed or stolen. At this stage, details remain limited, and no confirmed exposure of personal information has been publicly verified, but the incident adds to growing concerns about ransomware-style attacks targeting South African public-sector and healthcare-related organisations. IT Web

SOUTH AFRICAN DATA BREACH HIGHLIGHTS NEED FOR EFFECTIVE INCIDENT RESPONSE

IMAGE SOURCE: PINSET MASONS

The article highlights how the recent Statistics South Africa data breach has reinforced the urgent need for strong and well-prepared incident response strategies within organisations. It explains that cyberattacks are becoming increasingly frequent and sophisticated, often exposing weaknesses not only in technical systems but also in how quickly companies detect, contain, and report breaches. Legal and cybersecurity experts stress that effective incident response is no longer optional but a core requirement under data protection laws such as South Africa's POPIA, which obliges organisations to notify authorities and affected individuals promptly after a breach is discovered. The report also notes that regulators are paying closer attention not just to whether breaches occur, but to how effectively organisations manage them in real time—emphasising preparation, coordination, and transparency as key factors in reducing harm and regulatory consequences. Pinset Masons

MASSIVE POLICE DATA BREACH RAISES NATIONAL SECURITY ALARM IN SOUTH AFRICA

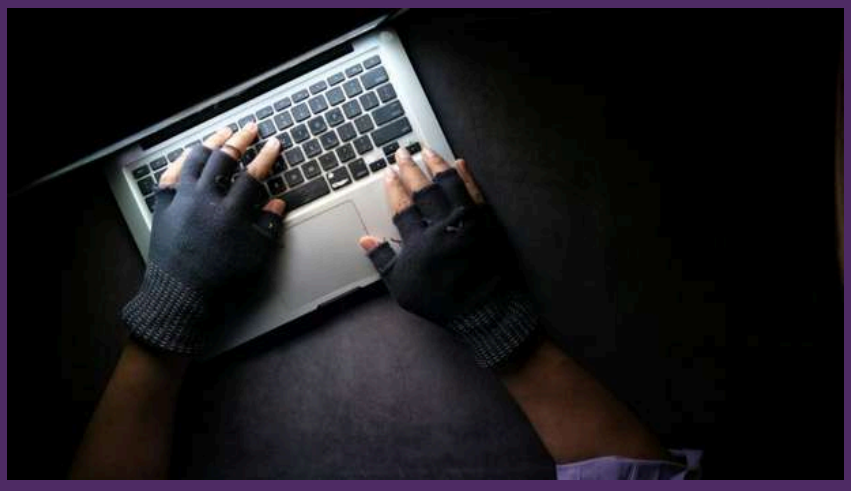


IMAGE SOURCE: CAPE TOWN ETC

A major cyberattack targeting South Africa's Police Medical Aid Scheme (Polmed) has exposed highly sensitive personal and professional information belonging to police officers, triggering serious national security concerns. The breach reportedly involved the theft of identity numbers, home addresses, medical records, financial details, and job-related information, which experts warn could be exploited for identity theft, blackmail, or even targeted attacks against law enforcement personnel. The incident is believed to have been carried out by an international hacking group and highlights vulnerabilities in the systems used to store critical government-linked data. Authorities have launched investigations and notified relevant oversight bodies, while cybersecurity experts caution that the scale of the leak poses risks not only to individual officers but also to the broader integrity and operational security of the police service. Cape Town etc

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI JUST EXPOSED THOUSANDS OF SECURITY FLAWS—NOW SOUTH AFRICA'S BIGGEST BANKS ARE BRACING FOR IMPACT

IMAGE SOURCE:OCEAN VIBE

The article reports that a powerful experimental AI model developed by Anthropic has uncovered thousands of previously hidden software vulnerabilities across major systems, triggering concern among South Africa's leading banks as they rush to strengthen cybersecurity defenses. The tool, capable of detecting flaws far faster than humans, revealed critical long-standing bugs—even in highly secure platforms—highlighting how AI is rapidly transforming the cyber threat landscape. Experts warn this shift toward "machine-scale" vulnerability discovery could overwhelm traditional security systems, especially in environments like South Africa with high fraud levels and reliance on legacy infrastructure. While banks such as Standard Bank and FNB say they are adapting by boosting monitoring, patching, and defensive strategies, the broader concern is that the same AI capabilities could soon be used by attackers, accelerating the global cybersecurity arms race and increasing the risk of large-scale breaches. 2 Oceans Vibe

HACKED EVERY 3 HOURS: WHY SOUTH AFRICA'S CYBER CRISIS IS MOSTLY SELF-INFLICTED

IMAGE SOURCE: SUNDAY INDEPENDENT

The article highlights a growing cybersecurity emergency in South Africa, where organisations are experiencing a data breach roughly every three hours—yet an estimated 90% of these incidents could have been prevented. Experts say the main issue isn't highly sophisticated hackers but internal weaknesses such as overly complex security systems, poor access controls, and fragmented tools that make threats harder to detect and respond to. With breaches rising sharply—up about 60% in early 2025—and organisations juggling dozens of security platforms while lacking skilled personnel, the country's expanding digital infrastructure is becoming increasingly vulnerable. The article argues that simplifying systems, improving coordination, and addressing basic security gaps could significantly reduce risks, emphasizing that the crisis is less about external threats and more about fixable internal failures. Sunday Independent

INTEL WATCH

Watching the watchers. Guarding the guardians.

RUSSIAN AI IN A SOUTH AFRICAN MALL: THE QUIET EXPANSION OF SMART SURVEILLANCE TECH

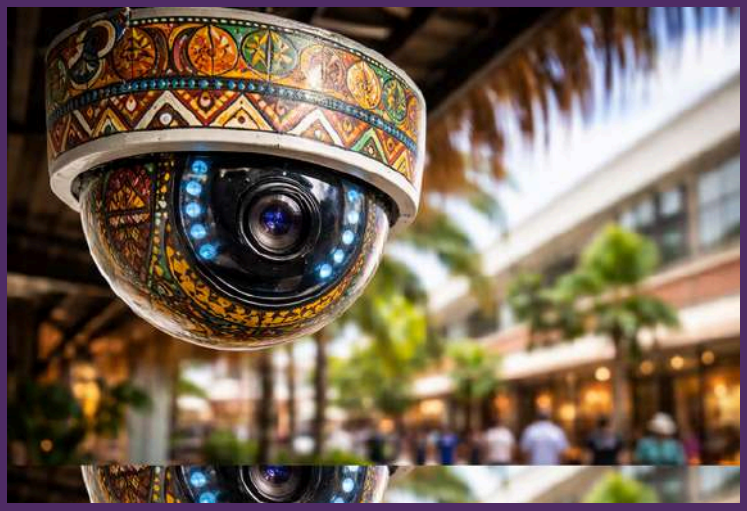


IMAGE SOURCE: RU NEWS

The article reports that a Russian-developed artificial intelligence video analytics system by NtechLab has been deployed in a major shopping centre in South Africa, where it monitors live camera feeds to track visitor numbers, manage crowd flow, and improve staffing efficiency in real time. Beyond operational uses like reducing queues and optimizing service, the system also enforces compliance rules by detecting restricted-area access attempts and checking whether staff are following safety protocols such as wearing protective equipment. Marketed as a pilot project, this deployment is part of NtechLab's broader global expansion of AI surveillance tools used in dozens of countries, raising broader implications about the growing role of foreign AI systems in everyday public spaces and the normalization of automated monitoring in commercial environments. RU News

ALEXFORBES CEO'S EMAIL HACKED IN LATEST FINANCIAL CYBERATTACK

IMAGE SOURCE: NEWS 24

The article reports that the email account of Alexforbes CEO Dawie de Villiers was compromised in a cyberattack discovered on 28 April 2026, marking another incident in a growing wave of financial-sector cybercrime in South Africa. According to the company, the breach involved unauthorised access to the CEO's work email, but there is currently no evidence that client data or internal systems were directly affected. Investigations are underway to determine how the intrusion occurred and whether any sensitive information was exposed, while cybersecurity experts warn that such targeted attacks on executives are increasingly used for phishing, fraud, and further network infiltration. News 24

INTEL WATCH

Watching the watchers. Guarding the guardians.

PSA DEMANDS PUBLIC SECTOR CYBERSECURITY OVERHAUL AFTER STATS SA BREACH

IMAGE SOURCE: IOL NEWS

The article reports that the Public Servants Association (PSA) has called for an urgent overhaul of cybersecurity across South Africa's public sector following a data breach at Statistics South Africa (Stats SA). The union warned that weak digital security systems are putting sensitive citizen and employee information at risk, highlighting broader vulnerabilities in government infrastructure. It urged authorities to strengthen data protection measures, improve cybersecurity policies, and invest in better systems and skills to prevent future breaches, stressing that failure to act could lead to more frequent and damaging cyber incidents. IOL News

SANDTON SCAM KINGPIN CAUGHT: INSIDE THE R69 MILLION CYBERCRIME NETWORK THAT SPANNED CONTINENTS

IMAGE SOURCE: MY BROADBAND

A Nigerian national has been sentenced after being arrested in Sandton, Johannesburg, for running a sophisticated cybercrime operation that defrauded victims of about R69 million through business email compromise and money laundering schemes. According to the report, the syndicate used tactics like email spoofing and unauthorized access to corporate communication systems to trick businesses into transferring funds into accounts controlled by the criminals, who then laundered the money through layered transactions and withdrawals. The case, which involved cooperation between South African authorities, Interpol, and U.S. law enforcement, led to the suspect's extradition to the United States where he received a 90-month prison sentence and was ordered to pay restitution. Officials say the investigation highlights both the global reach of cybercrime networks and the importance of international cooperation in dismantling them, as well as the growing financial and reputational harm caused to victims worldwide. My Broadband

1.2TB OF BANK DATA LEAKED: STANDARD BANK HACK SPARKS NATIONWIDE CYBERSECURITY ALARM

IMAGE SOURCE: IT WEB

Standard Bank is facing a major cybersecurity crisis after hackers known as Rootboy allegedly leaked around 1.2TB of stolen customer data, including account numbers, identity details, contact information, and limited credit card information. The breach, which reportedly began in February 2026, has escalated concerns about the security of South Africa's financial sector as the exposed data circulates publicly, raising risks of fraud, identity theft, and further exploitation. The incident has intensified scrutiny of banking cybersecurity practices at a time when financial institutions are rapidly adopting cloud systems, AI tools, and digital platforms. Experts warn that the breach highlights both the sophistication of modern cybercriminal groups and the ongoing vulnerabilities in large-scale data protection systems, prompting calls for stronger safeguards and faster incident response mechanisms across the industry. IT Web

GLOBAL CYBERCRIME: NIGERIA AND SOUTH AFRICA AMONG AFFECTED NATIONS

IMAGE SOURCE: MORDEN GHANA

The article reports that cybercrime has become a major global issue, with losses reaching over $20 billion in 2025 and more than one million complaints filed worldwide, according to FBI Internet Crime Complaint Center data. Nigeria and South Africa are listed among the top 20 countries with the highest number of cybercrime complaints, reflecting their growing exposure as their digital economies expand, especially in fintech, mobile banking, and cryptocurrency. Common threats include phishing, identity theft, business email compromise, and investment scams, which exploit weak cybersecurity systems and limited public awareness. While their rankings are lower than countries like the United States and Canada, their inclusion highlights how rapidly African economies are becoming part of the global cyber threat landscape, prompting calls for stronger cybersecurity infrastructure, education, and international cooperation. Modern Ghana

HACKERS TARGET STUDENTS AND JOBSEEKERS IN SOUTH AFRICA

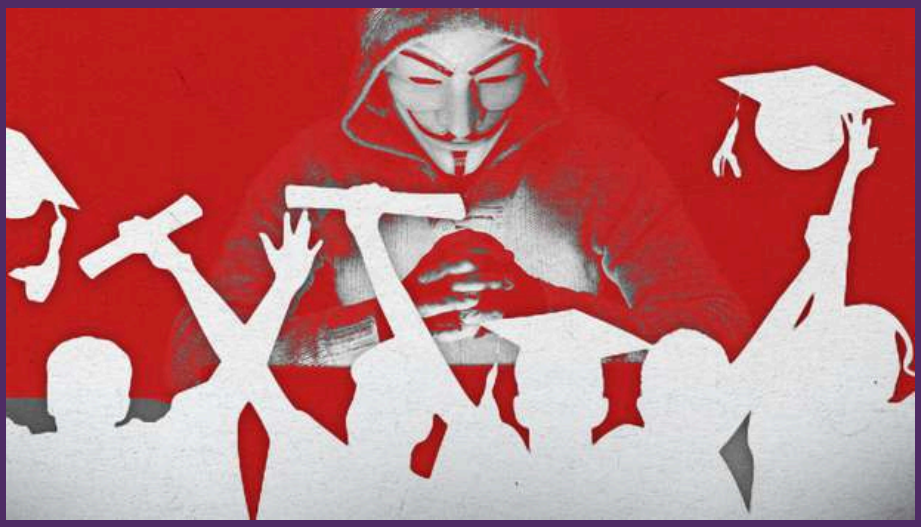


IMAGE SOURCE: MY BROADBAND

A recent MyBroadband report explains that a newly emerged cybercrime group called XP95 has been targeting South African organisations to steal sensitive data belonging to students and jobseekers, with breaches affecting entities like Statistics South Africa, the Gauteng Provincial Government, and a student bursary provider. The attacks focused on databases containing personal information submitted through job application and education systems, highlighting how vulnerable these platforms are to cyberattacks. The incidents form part of a broader rise in ransomware and data-theft operations in the country, with experts warning that government and public-sector systems remain prime targets due to valuable personal data and often inadequate cybersecurity measures. My Broadband

NIGERIA RAISES ALARM OVER RISING CYBERATTACKS ON CRITICAL INFRASTRUCTURE

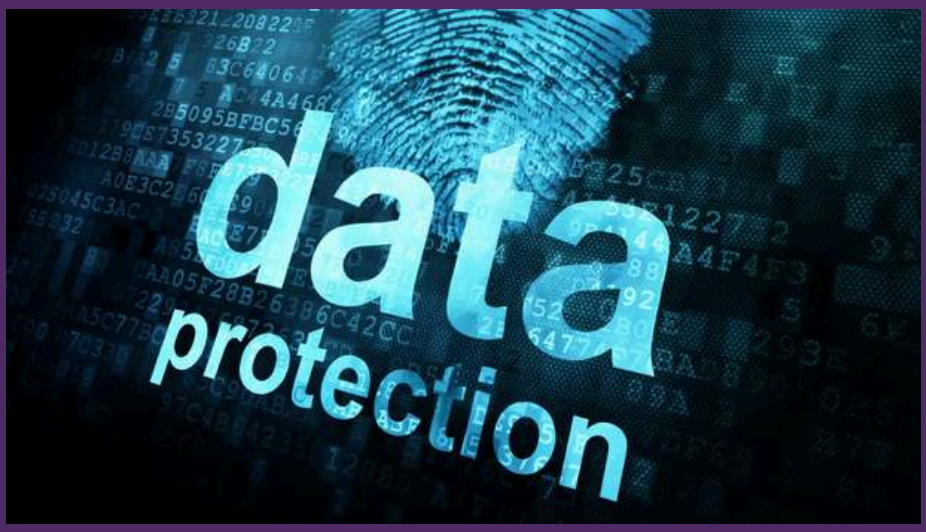


IMAGE SOURCE: THE GUARDIAN

The article reports that Nigeria's Federal Government, through the Nigeria Data Protection Commission (NDPC), has warned citizens and organisations about a surge in Distributed Denial-of-Service (DDoS) attacks targeting critical national infrastructure, with thousands of cyberattacks occurring weekly and disrupting digital services. Authorities say these attacks are becoming more sophisticated and persistent, posing risks to government systems, businesses, and essential services, and are urging stronger cybersecurity awareness, stricter compliance with data protection regulations, and improved defensive measures. The warning highlights broader concerns about national security and economic stability, as successful attacks could cause service outages, financial losses, and weakened resilience of key infrastructure. The Guardian

DIGITAL MERCENARIES: HACK-FOR-HIRE CAMPAIGNS TARGET JOURNALISTS ACROSS MENA

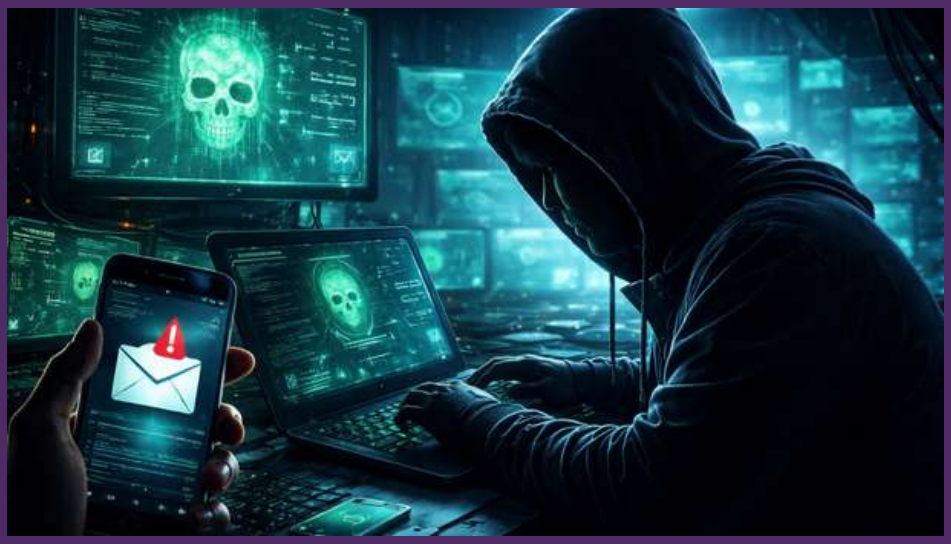


IMAGE SOURCE: STORYBOARD 18

The article reports that a sophisticated "hack-for-hire" cyber-espionage campaign has been targeting journalists and human rights defenders across the Middle East and North Africa (MENA), using highly personalised phishing tactics to gain access to sensitive data. According to findings from digital rights groups, attackers impersonate trusted contacts or organisations through messaging platforms, tricking victims into revealing login credentials or installing malicious software that allows access to emails, messages, and cloud backups. The campaign highlights how commercialised hacking services are increasingly being used to monitor, intimidate, or silence critical reporting, raising serious concerns about press freedom, source protection, and the growing accessibility of advanced surveillance tools to both state and non-state actors. Storyboard 18

SOUTH AFRICAN PAYMENT PROCESSOR BREACHED, SOURCE CODE ALLEGEDLY STOLEN

IMAGE SOURCE: MY BROADBAND

The article reports that a South African payment processing company has allegedly suffered a major cyber breach in which attackers stole its proprietary source code, raising concerns about the security of financial infrastructure and potential risks to its systems and clients. While no customer data has been confirmed as leaked, cybersecurity experts warn that access to source code could allow attackers to study system vulnerabilities, potentially enabling future fraud or disruption of payment services. The incident highlights growing threats facing fintech companies in South Africa and the increasing value cybercriminals place on intellectual property rather than just personal data. My Broadband

THE AI MODEL THAT'S EXPOSING WEAK SPOTS IN EVERY MAJOR SYSTEM

IMAGE SOURCE: BBC

TThe episode of The Global Story explores Anthropic's development of a highly advanced AI model that the company has deliberately withheld from public release due to concerns that it may be too capable at identifying and exploiting cybersecurity vulnerabilities. Instead of launching it widely, Anthropic has restricted access to a small group of major technology companies, including cloud and cybersecurity firms, to test and strengthen their systems against potential weaknesses in operating systems, browsers, and critical infrastructure. The discussion raises a central debate: whether this cautious approach reflects responsible AI governance or is partly a strategic move to generate attention and competitive advantage. Experts featured in the episode highlight the dual-use nature of such AI—capable of significantly improving cybersecurity defenses while also potentially lowering the barrier for malicious actors if misused—underscoring growing global anxiety about how to safely manage increasingly powerful AI systems.. BBC

IT'S NOT THE HACKERS: THE REAL REASON AFRICA KEEPS GETTING BREACHED

IMAGE SOURCE: CIRCLE ID

The article argues that Africa's cybersecurity challenges are not primarily caused by hackers but by deep internal weaknesses in systems, governance, and human capacity, which create easy opportunities for attacks in the first place. It explains that many organizations across the continent prioritize functionality over security, resulting in poorly designed systems, weak access controls, and minimal monitoring, while laws and regulations often exist but are weakly enforced. Combined with a shortage of skilled cybersecurity professionals, low user awareness, and fragmented coordination between institutions, these structural gaps make breaches almost inevitable. The author stresses that blaming hackers distracts from accountability, urging a shift toward building secure-by-design systems, strengthening governance, investing in skills, and improving collaboration to create long-term digital resilience. Circle ID

INTEL WATCH

Watching the watchers. Guarding the guardians.

FAKE WHATSAPP APP USED AS SPYWARE TRAP: HOW A SURVEILLANCE FIRM INFILTRATED PHONES IN ITALY

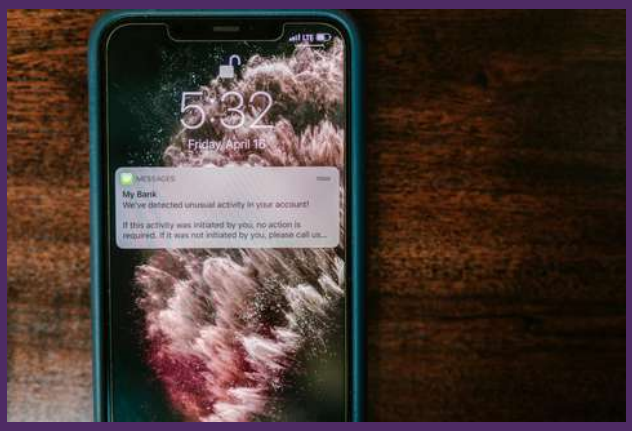


IMAGE SOURCE: AFRICA SILICON CANALS

The article reports that Meta's WhatsApp has uncovered a targeted spyware campaign in which around 200 users—mostly in Italy—were tricked into installing a fake version of WhatsApp containing government-grade surveillance malware. The operation is attributed to Italian surveillance firm SIO and its subsidiary ASIGINT, which allegedly used social engineering tactics and unofficial app distribution channels to deceive victims into downloading the malicious software. Once installed, the fake app functioned like WhatsApp but secretly enabled extensive device access, allowing operators to monitor communications and potentially extract sensitive data. WhatsApp responded by logging affected users out, warning them about the risks, and urging them to reinstall the official app, while also pursuing legal action. The incident highlights the growing role of commercial spyware firms working with or alongside government entities, and how easily widely trusted apps can be cloned to enable covert surveillance. Silicon Canals

FAKE APPLE PAGES, REAL VICTIMS: HOW HACKERS ARE STEALING ICLOUD BACKUPS IN A SILENT GLOBAL SCAM

IMAGE SOURCE: 9 TO 5 MAC

The article reports on a hack-for-hire operation that uses highly convincing fake Apple login pages to trick users into handing over their Apple ID credentials, allowing attackers to access and download full iCloud backups containing messages, photos, contacts, and other sensitive data. According to cybersecurity researchers from multiple organizations, the campaign has been active for years and has targeted journalists, activists, government officials, and other high-value individuals across the Middle East, North Africa, and beyond. The operation relies on large-scale phishing infrastructure with nearly 1,500 spoofed domains mimicking Apple and other major platforms, rather than advanced technical exploits, highlighting how effective social engineering remains. Investigators also link the activity to a hack-for-hire group connected to a private surveillance industry trend where governments or clients outsource digital spying for plausible deniability and lower costs than commercial spyware. 9 to 5 Mac

INTEL WATCH

Watching the watchers. Guarding the guardians.

CLICK, TRAP, HACK: NEW PHISHING CAMPAIGN STILL BREAKING INTO IPHONE AND ANDROID DEVICES

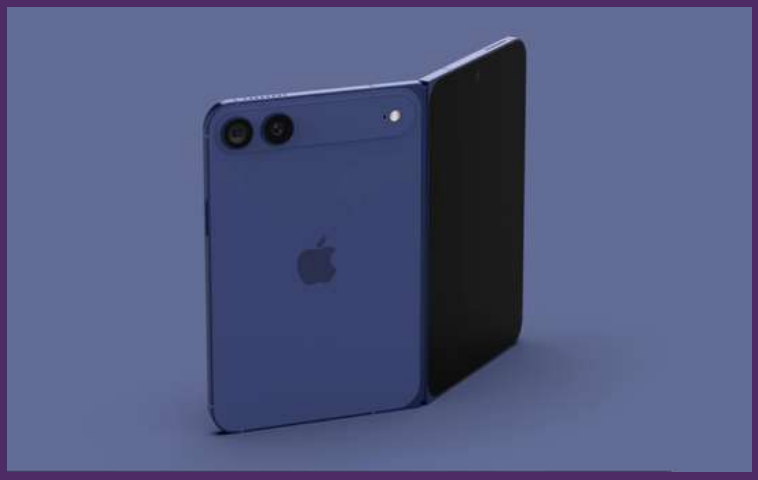


IMAGE SOURCE: TECH TIMES

The article reports on a hack-for-hire cyber espionage campaign that continues to successfully target both iPhone and Android users using relatively simple but highly effective phishing tactics. According to cybersecurity researchers, attackers linked to a group known as BITTER APT lure victims—often journalists, activists, and government officials—into fake login pages that mimic trusted services like Apple and Google, tricking them into handing over credentials. Once obtained, these logins allow attackers to access sensitive data, including iCloud backups, messages, and account information, sometimes without needing to install advanced spyware. Investigators note that the operation spans multiple countries and reflects a broader trend of "cybercrime as a service," where hacking is outsourced to private groups for surveillance purposes, showing that even basic social engineering remains one of the most dangerous tools in modern cyberattacks. Tech Times

SMART GLASSES, BIG SECRETS: META PRESSURED TO REVEAL FACIAL RECOGNITION PLANS AND POLICE TIES

IMAGE SOURCE: BIOMETRIC UPDATE

More than 70 civil society and digital rights organizations are urging Meta to stop its planned rollout of facial recognition features in its Ray-Ban and Oakley smart glasses, warning that the technology could enable real-time identification of people in public without consent and deepen mass surveillance. The coalition—backed by groups like the ACLU and EFF—also demands that Meta disclose any partnerships or discussions with law enforcement agencies such as ICE or CBP, arguing that the company has not been transparent about how biometric data from wearables could be used or shared. Critics say the proposed "Name Tag" feature, which would identify people through the glasses' AI system, poses serious risks of stalking, harassment, and abuse, especially for vulnerable groups, and cannot be safely mitigated through opt-outs or minor design changes. They are also calling for stronger privacy protections and an end to biometric data collection without explicit user consent, citing Meta's history of privacy controversies and regulatory fines as reasons for distrust. Biometric Update

AI THAT CAN CRACK BANKS? MYTHOS MODEL SPARKS GLOBAL PANIC OVER FINANCIAL CYBERSECURITY RISKS

IMAGE SOURCE: BBC

Finance ministers, central bankers, and major financial institutions are raising alarm over a new AI system called "Mythos," developed by Anthropic, after early tests suggested it may be exceptionally capable at identifying vulnerabilities in complex software systems used by banks and critical infrastructure. The model has reportedly exposed weaknesses in operating systems and web browsers, prompting urgent discussions at IMF meetings and internal crisis briefings about potential risks to global financial stability. While Anthropic has restricted public release and instead shared the system with select tech companies and security partners for testing, experts warn that such AI could be used both to strengthen cybersecurity and to exploit it if misused by malicious actors. Officials from institutions like the Bank of England and Barclays stress the need for urgent safeguards, improved resilience, and deeper understanding of how such "dual-use" AI systems could reshape cyber threats in the financial sector. BBC

NO MORE PRIVATE CHATS: INSTAGRAM'S ENCRYPTION ROLLBACK SPARKS MAJOR PRIVACY ALARM

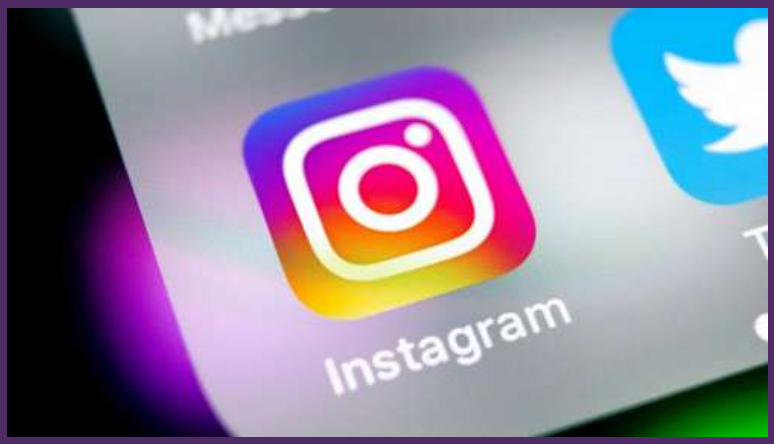


IMAGE SOURCE: TECH RADAR

The article explains that Meta is removing end-to-end encryption (E2EE) from Instagram direct messages, a move that means private conversations on the platform will no longer be protected so that only the sender and recipient can read them. The company says the feature was not widely used and is being discontinued as part of a broader shift in its messaging approach, with encrypted communication still available on WhatsApp and Messenger. Privacy experts, however, warn that the rollback weakens user security and increases exposure to surveillance, data breaches, and potential misuse of personal messages, especially for journalists, activists, and vulnerable users. Critics argue that removing encryption from a major platform like Instagram signals a broader industry trend away from strong default privacy protections, raising concerns about how social media companies balance user safety, regulatory pressure, and business interests. Tech Radar

INTEL WATCH

Watching the watchers. Guarding the guardians.

REPRESSION MONITOR

SMART CITIES, SILENT CONTROL: HOW AI SURVEILLANCE IS BEING USED TO MONITOR DISSENT ACROSS AFRICA

IMAGE SOURCE: DW

The article explains how at least 11 African governments have invested over $2 billion in Chinese-built "smart city" surveillance systems that combine AI-powered CCTV, facial recognition, biometric databases, and automatic number-plate recognition to monitor public spaces under the justification of improving security and urban management. However, research shows there is no clear evidence that these systems reduce crime or terrorism; instead, they are frequently used to track activists, monitor protests, and suppress political opposition, creating a chilling effect on freedom of expression and assembly. Countries such as Uganda and Zimbabwe have reportedly used these tools directly against dissenters, while others have deployed them in politically sensitive areas despite low security threats. The systems are often financed through opaque deals and foreign loans, limiting transparency and oversight, while reliance on external vendors—mainly Chinese firms—creates long-term dependency. Human rights experts warn that without strong legal frameworks, independent oversight, and transparency, these technologies risk normalizing population-wide surveillance and shrinking civic space across the continent. All Africa

DIGITAL BORDERS RISING: HOW AI SURVEILLANCE COULD UNDERMINE MIGRANTS' FREEDOM ACROSS WEST AFRICA

IMAGE SOURCE: ELECTRIFYING

The article explains how governments across West Africa are rapidly adopting AI-powered border technologies—such as biometric ID systems, facial recognition, and data-driven monitoring—transforming traditionally open regional borders into "digital borders" that track and control movement through databases and algorithms. While these systems are promoted as tools to combat terrorism, trafficking, and irregular migration, critics warn they pose serious risks to migrants' rights, including privacy violations, indefinite storage and sharing of sensitive biometric data, and algorithmic discrimination that may unfairly target certain groups. The expansion is also heavily influenced by European migration policies, which fund surveillance systems in Africa to curb migration before it reaches Europe. Ultimately, the article argues that without stronger legal safeguards and regional oversight, these technologies could weaken long-standing free movement agreements and normalize intrusive surveillance across the region. The Conversation

INVASIVE' SURVEILLANCE TECH VIOLATES AFRICANS' FREEDOMS

IMAGE SOURCE: EURASIA REVIEW

The article warns that the rapid spread of AI-powered surveillance technologies across Africa - often supplied by Chinese companies - is enabling governments to monitor citizens on an unprecedented scale, threatening fundamental rights like privacy, free expression, and freedom of movement. Framed as "smart city" solutions to fight crime and modernize infrastructure, these systems include facial recognition cameras, biometric tracking, and mass data collection, yet experts say there is little evidence they actually reduce crime. Instead, they are increasingly used to track journalists, activists, and political opponents, especially in countries with weak legal safeguards and oversight. With billions spent and limited accountability, critics argue this growing surveillance infrastructure risks entrenching authoritarian practices and creating a chilling effect where citizens self-censor out of fear of constant monitoring. Eurasia Review

HOW YOUR EVERYDAY APPS ARE FEEDING A MASSIVE GLOBAL SURVEILLANCE MACHINE

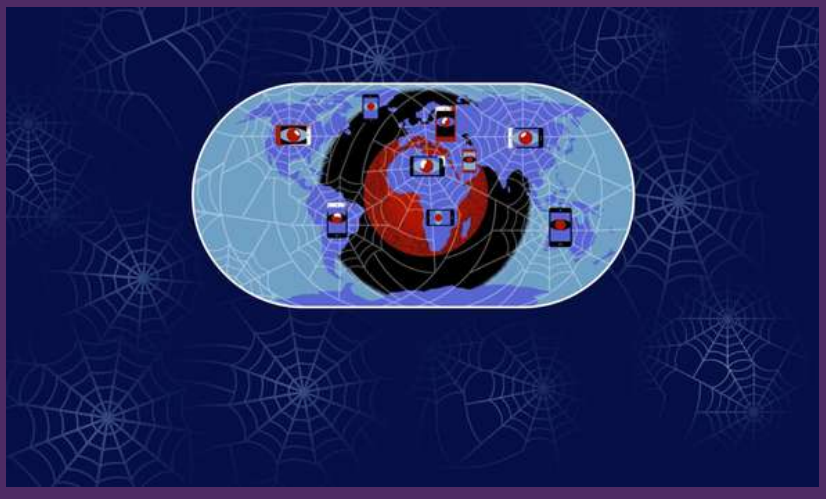


IMAGE SOURCE: CITIZEN LAB

The Citizen Lab investigation reveals that a surveillance system called Webloc, developed by Cobwebs and now sold by Penlink, uses data harvested from mobile apps and digital advertising to track the movements of hundreds of millions of people worldwide—often without their knowledge or a warrant. By exploiting advertising data streams and device identifiers, the system allows governments and law enforcement agencies to monitor individuals' locations in real time and even ย้อนหลัง for years, exposing highly sensitive details about their lives, including habits, relationships, and beliefs. Used by agencies in countries like the U.S., Hungary, and El Salvador, the technology highlights how commercial data ecosystems are being repurposed for mass surveillance with minimal oversight, raising serious concerns about privacy, legality, and the growing normalization of tracking entire populations through seemingly harmless everyday apps. Citizen Lab

INTEL WATCH

Watching the watchers. Guarding the guardians.

ICE JUST SIGNED A $12 MILLION DEAL TO TRACK MIGRANTS WITH AI

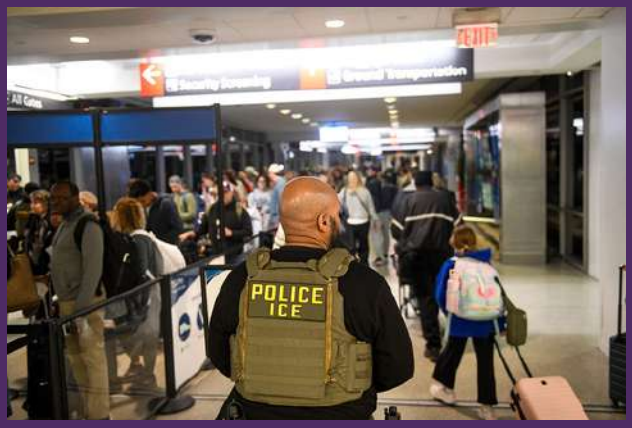


IMAGE SOURCE: JACOBIN

The article reports that U.S. Immigration and Customs Enforcement (ICE) has signed a $12.2 million contract for an AI surveillance system designed to map and predict immigrants' movements, routines, and behaviours by compiling large datasets into detailed "patterns of life" profiles. The tool, described in procurement records as Project SAFE HAVEN, uses multiple data sources—including location tracking and personal identifiers—to flag individuals as potential security risks and support enforcement operations. Critics argue this represents a major escalation in immigration surveillance, shifting from targeted investigations to continuous, automated monitoring of entire populations. Civil liberties groups condemn the move and warn that the system raises serious concerns about privacy, due process, and the potential for error or bias, especially if individuals are incorrectly profiled or tracked based on incomplete data. The contract is part of a broader trend of ICE expanding its use of AI and private contractors to build a large-scale digital surveillance infrastructure for immigration enforcement. Jacobin

ICE ADMITS TO PHONE HACKING: ZERO-CLICK SPYWARE MARKS A NEW ERA OF GOVERNMENT SURVEILLANCE

IMAGE SOURCE: CAPTAIN COMPLIANCE

The article reports that U.S. Immigration and Customs Enforcement (ICE) has confirmed it is using advanced commercial spyware known as "Graphite," which can remotely hack into smartphones without any user interaction through so-called zero-click exploits. Once installed, the tool can bypass encrypted messaging apps, access private communications, photos, location data, and other sensitive information, effectively turning a phone into a surveillance device. ICE says it is using the technology to target serious criminal activity such as drug trafficking and transnational crime, but civil liberties groups warn it represents a major expansion of domestic surveillance power with little transparency or oversight. Critics also argue that such tools—previously linked to spying campaigns against journalists and activists abroad—raise serious risks of misuse, mission creep, and violations of constitutional rights, especially if deployed against immigrants, protesters, or other vulnerable groups in the U.S. Captain Compliance

IRAN'S AUTHORITIES USING NTECHLAB'S LIVE FACIAL RECOGNITION TO CRUSH DISSENT

IMAGE SOURCE: BIOMETRIC UPDATE

The investigation reports that Iranian authorities are using a powerful Russian-developed facial recognition system from NtechLab (FindFace) as part of a wider surveillance network to identify, track, and suppress political dissent. The technology, acquired through intermediary companies linked to state security structures, allows officials to match faces captured by CCTV cameras in public spaces—such as streets, universities, and metro stations—against large databases of personal images. According to researchers and leaked documents cited in the report, this system has been deployed in the context of protests and unrest, enabling authorities to retrospectively identify demonstrators and monitor their social networks. While marketed as a security and identification tool, critics warn it significantly strengthens the state's ability to conduct mass surveillance with minimal visibility or accountability, increasing risks for activists, journalists, and ordinary citizens caught in its reach. Biometric Update

ANTI-DRUG CRACKDOWNS OR MASS SURVEILLANCE? KASHMIR REPORT WARNS OF EXPANDING STATE CONTROL

IMAGE SOURCE: KASMIR MEDIA SERVICE

The article claims that in Indian-administered Jammu and Kashmir, authorities are intensifying surveillance and repression under the pretext of anti-drug campaigns, with critics arguing these measures are being used to suppress political dissent and control the population. It describes how new laws and enforcement strategies are allegedly targeting young people, linking dissent to criminal activity and enabling arrests, monitoring, and expanded tracking systems. Observers cited in the report say surveillance now extends into everyday life, including schools and rural sectors, contributing to an atmosphere of fear and insecurity. The report further argues that these policies reflect a broader shift toward continuous population monitoring, with anti-drug operations serving as justification for expanding state control rather than purely addressing narcotics issues. Kasmir Media Service

MEXICO'S SURVEILLANCE SURGE: HOW SMART TECH IS BLURRING THE LINE BETWEEN SAFETY AND CONTROL

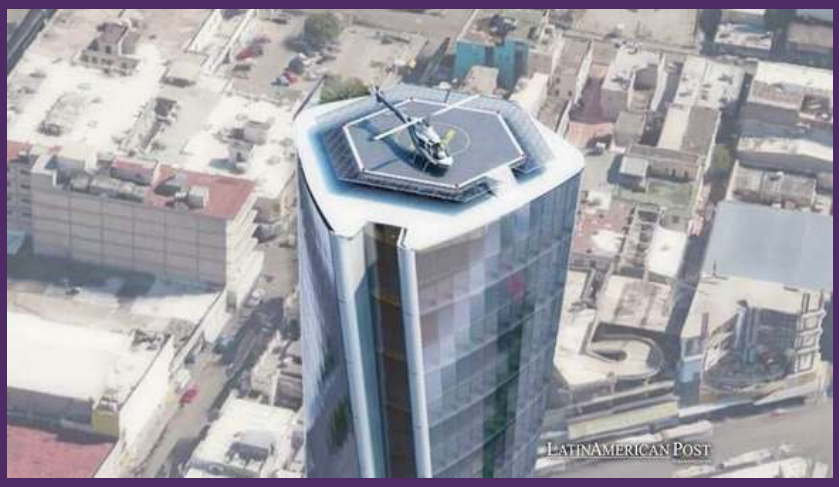


IMAGE SOURCE: LATIN AMERICAN POST

The article describes the rapid expansion of surveillance technologies across Mexico, particularly along the U.S. border, where governments are increasingly deploying AI-powered cameras, drones, biometric systems, and integrated command centers to monitor public spaces and migration routes. These systems are framed as tools for improving public safety, combating crime, and managing border security, but critics argue they also enable widespread monitoring of civilians with limited transparency or oversight. The growth of this infrastructure is closely tied to partnerships with private security firms and international tech providers, contributing to a broader "smart security" ecosystem that collects and analyzes large volumes of personal and location data. While authorities claim these tools enhance efficiency and protection, human rights advocates warn that the lack of clear regulation and accountability risks normalizing mass surveillance and blurring the boundary between legitimate security operations and intrusive population tracking. Latin American Post

BRITISH UNIVERSITIES PAID SECURITY FIRM TO 'SPY' ON PRO-PALESTINE STUDENTS

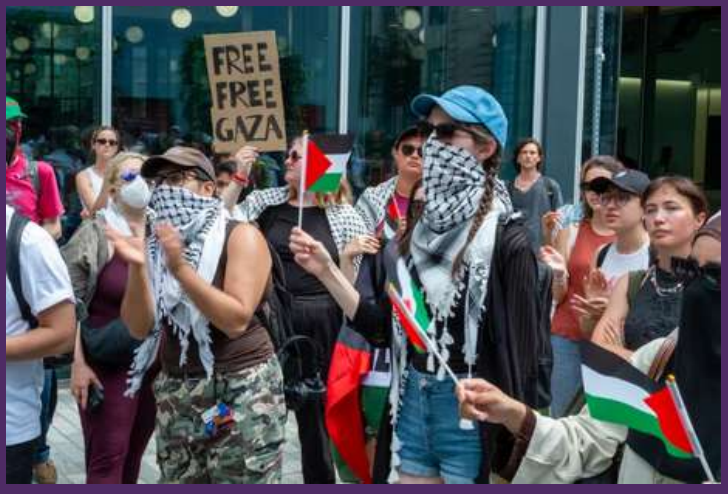


IMAGE SOURCE: ALJAZEERA

An investigation reveals that multiple UK universities, such as Bristol University, have paid a private intelligence-linked security firm to monitor students' social media activity and conduct background surveillance on protesters and academics, particularly those involved in pro-Palestinian activism. The firm reportedly used open-source intelligence tools and AI systems to scan posts, flag individuals, and produce risk assessments that were shared with university administrators. Critics argue this amounts to covert surveillance of lawful student expression and protest, raising serious concerns about privacy, academic freedom, and the outsourcing of security functions to private contractors with limited oversight. Universities involved defend the practice as necessary for campus safety and risk management, but rights groups and union representatives warn it reflects a broader trend of increasing surveillance and repression of student activism under the guise of security. Aljazeera

INTEL WATCH

Watching the watchers. Guarding the guardians.

WATCHED AT THE GAME: INSIDE THE SECRET SURVEILLANCE SYSTEM TRACKING FANS AND CRITICS

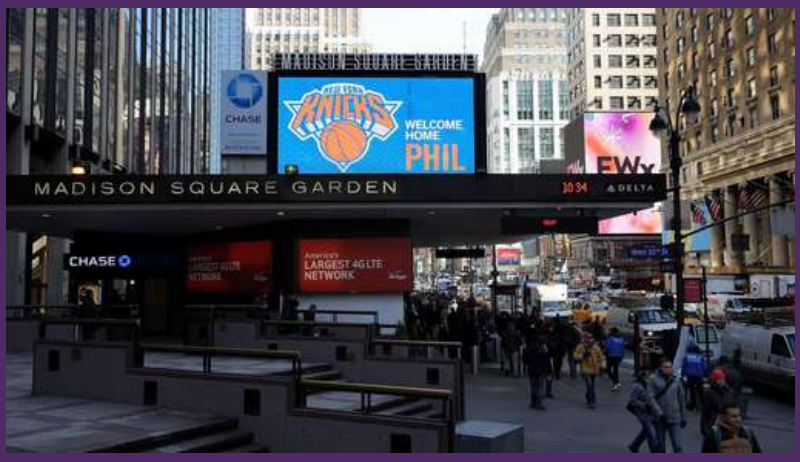


IMAGE SOURCE: YNET NEWS

The article reveals that Madison Square Garden operates an extensive and controversial surveillance network under owner James Dolan, using tools like facial recognition, behavioural tracking, and watchlists to monitor not just attendees but also employees and critics. According to an investigation cited in the piece, individuals who have publicly criticized Dolan or been involved in disputes with the company have faced targeted scrutiny, including being denied entry to events. The system reportedly extends beyond the venue itself, raising serious concerns about corporate overreach, privacy violations, and the growing power of private entities to track and control individuals in public and semi-public spaces. Ynet News

YOUR PHONE ISN'T PRIVATE: THE SECRET GLOBAL SYSTEM TRACKING PEOPLE WITHOUT THEM KNOWING

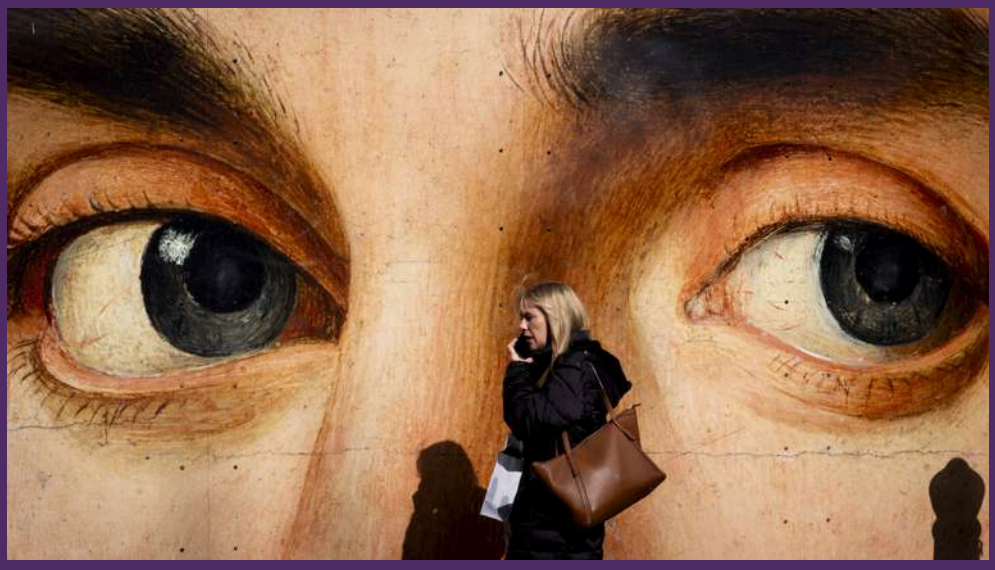


IMAGE SOURCE: REVEAL NEWS

The podcast investigation by Reveal and Lighthouse Reports uncovers how a little-known company called First Wap has built a vast global phone-tracking operation capable of locating people anywhere in the world without accessing their devices. Using its software Altamides, the company exploits weaknesses in telecom networks to track locations, intercept communications, and monitor targets across more than 160 countries, often without legal oversight or user awareness. The investigation—based on a massive leaked dataset—shows that not only governments but also private actors have used the technology to monitor journalists, activists, business figures, and even ordinary individuals, challenging claims that such tools are only used for fighting crime and exposing a largely unregulated surveillance industry operating on a global scale. Reveal News

OMINOUS SURVEILLANCE "SCARECROWS" APPEARING ACROSS AMERICA

IMAGE SOURCE: FUTURISM

The article describes the rapid spread of mobile surveillance towers—nicknamed "scarecrows" or "COWs" (cameras on wheels)—across the United States, where police and private security firms deploy trailer-mounted systems equipped with solar power, CCTV cameras, and sometimes AI-driven facial recognition. These units can be quickly installed in public or commercial areas and connected to wider monitoring networks, allowing authorities to fill surveillance gaps with minimal effort. Marketed as crime deterrents that can "stop crimes before they start," they are part of a booming multi-billion-dollar policing technology industry, with companies operating vast networks of cameras nationwide. However, their growing use raises concerns about the normalization of constant monitoring, the expansion of for-profit surveillance, and the broader implications of turning everyday spaces into heavily watched environments. Futurism

META'S SMART GLASSES FACIAL RECOGNITION PLAN IS TRIGGERING A PRIVACY BACKLASH

IMAGE SOURCE: WIRED

The WIRED article reports on growing resistance from more than 70 civil society and digital rights organisations, including the ACLU and Electronic Privacy Information Center, against Meta's reported plans to add real-time facial recognition ("Name Tag") to its Ray-Ban and Oakley smart glasses. Critics warn that embedding biometric identification into wearable glasses would allow users—or potentially third parties like law enforcement or stalkers—to silently identify people in public without consent, effectively eliminating practical anonymity in everyday life. Advocacy groups argue the feature cannot be safely "opted out of" because bystanders have no control over whether they are scanned or identified, raising serious concerns about privacy, surveillance abuse, and discrimination against vulnerable groups such as immigrants, activists, and LGBTQ+ people. Meta has stated it currently does not offer facial recognition on its glasses and would approach any future deployment cautiously, but leaked internal discussions and prior reporting suggest the company has explored ways to roll it out despite expected backlash. Wired

INTEL WATCH

Watching the watchers. Guarding the guardians.

WHY NEW AI SURVEILLANCE TOOLS IN STORES ARE CREATING LEGAL TROUBLE FOR RETAILERS

IMAGE SOURCE: OGLETREE

The article explains that retailers are increasingly adopting advanced surveillance technologies—such as AI-powered cameras, facial recognition systems, biometric tracking, and audio/video monitoring—to combat rising theft and improve store security, but these tools are creating significant legal risks. Depending on the jurisdiction, these systems may violate privacy and biometric data laws if companies fail to properly notify customers or obtain consent, especially in states with strict regulations on facial recognition and audio recording. The piece highlights that while video surveillance in public store areas is generally allowed, more intrusive tools like biometric identification and audio capture can trigger liability under laws governing consumer privacy, data protection, and unfair business practices. It also warns that the rapid rollout of these technologies is outpacing regulation, leaving retailers exposed to lawsuits, enforcement actions, and compliance challenges if they do not implement clear policies and transparency measures. Ogletree

MOVING GOALPOSTS: FOOTBALL, FACIAL RECOGNITION AND THE EXPANSION OF SURVEILLANCE

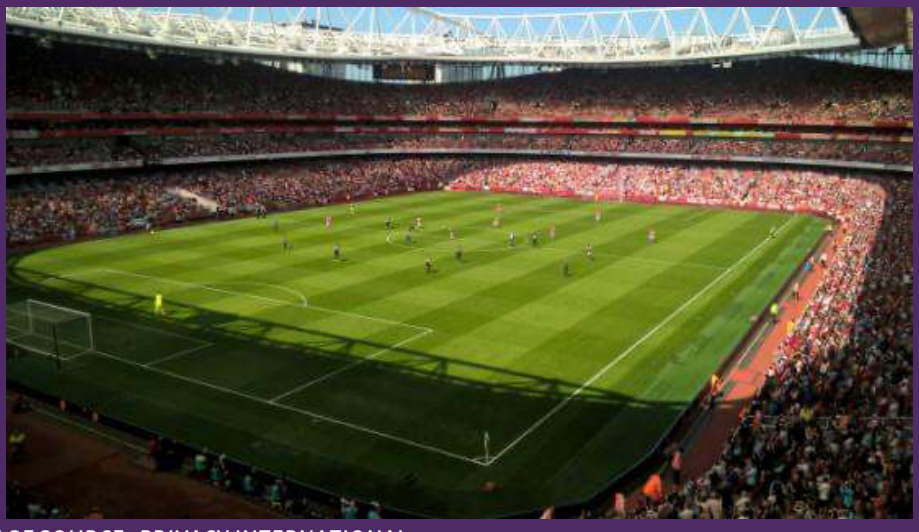


IMAGE SOURCE: PRIVACY INTERNATIONAL

The Privacy International report examines how facial recognition technology (FRT), first introduced in f under the justification of improving security and managing crowds, is increasingly being normalized and expanded into broader public spaces and policing contexts. It highlights how deployments in sports environments—often involving limited transparency, weak consent, and unclear oversight—create "testing grounds" for biometric surveillance systems that can later be reused or scaled beyond their original purpose. The report points to examples where FRT has been used to identify and exclude individuals, sometimes without clear avenues for appeal, and warns that data collection at stadium entry points can feed wider surveillance infrastructures. Overall, it argues that decisions made in sport are shaping wider societal acceptance of constant biometric monitoring, raising concerns about privacy, accountability, and the gradual expansion of surveillance into everyday life. Privacy International

INTEL WATCH

Watching the watchers. Guarding the guardians.

ICE'S USE OF PALANTIR TECH SPARKS MASS SURVEILLANCE CONCERNS

IMAGE SOURCE: GOLDMAN HOUSE

A coalition of U.S. lawmakers led by Representatives Dan Goldman, Nydia Velázquez, and Senator Ron Wyden is demanding detailed explanations from Immigration and Customs Enforcement (ICE) and the Department of Homeland Security over their use of Palantir-developed data systems and related surveillance technologies. The lawmakers express concern that these tools—combined with facial recognition, social media monitoring, cellphone tracking, and large-scale data aggregation systems—may be enabling a "mass surveillance ecosystem" that collects and analyzes personal information about individuals who are not suspected of wrongdoing, including journalists and protesters. They are requesting transparency on contracts, data sources, safeguards, and how such systems are used in immigration enforcement operations, warning that the technologies could be weaponized against constitutionally protected activities like lawful protest. The letter highlights broader fears in Congress about weak oversight and the growing role of private tech firms in government surveillance infrastructure. Goldman House

MORE THAN A DOZEN WRONGFUL ARRESTS DUE TO POLICE RELIANCE ON FACIAL RECOGNITION TECHNOLOGY

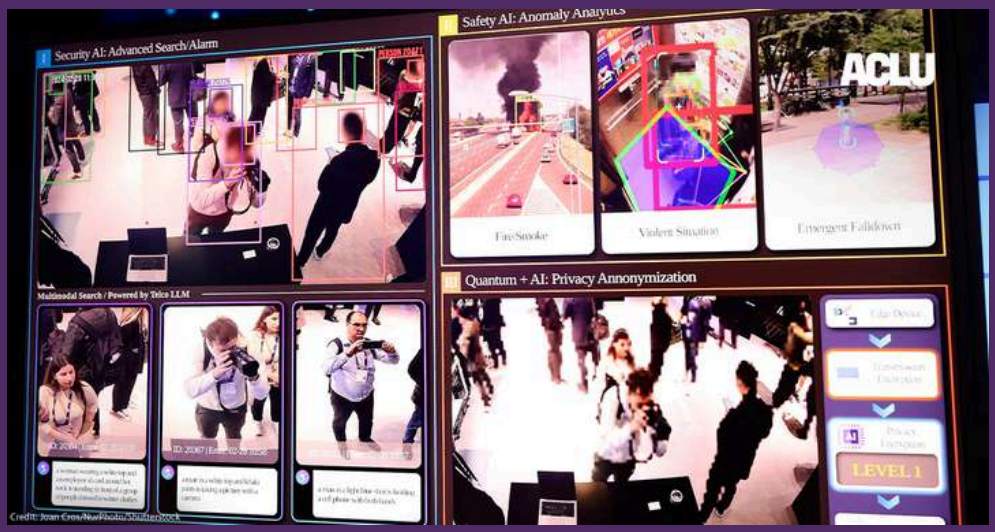


IMAGE SOURCE: ACLU

The ACLU reports that at least 14 people in the United States have been wrongfully arrested after police relied on facial recognition technology that misidentified them as suspects, often without adequate independent investigation. In multiple cases, including that of Kimberlee Williams, individuals were jailed for crimes they did not commit after flawed algorithmic matches were treated as strong evidence, sometimes leading directly to arrest warrants. The technology has been shown to produce higher error rates for people of color and can "taint" investigations by steering officers toward incorrect suspects while discouraging them from pursuing contradictory evidence. Civil liberties advocates argue that many police departments fail to disclose when facial recognition is used and sometimes treat it as more reliable than it actually is. The ACLU is calling for stricter regulations or bans, warning that without safeguards, these systems will continue to produce unjust arrests and undermine due process. ACLU

INTELLIGENCE AGENCIES

IRELAND'S NEW SPY POWERS: THE SURVEILLANCE BILL TESTING EU PRIVACY AND HUMAN RIGHTS LIMITS

IMAGE SOURCE: IMPACT POLICIES

The article explains how Ireland's proposed Communications (Interception and Lawful Access) Bill would significantly expand state surveillance powers by formally allowing police to use spyware, device-hacking tools, encrypted-message interception, and forensic extraction technologies to access digital communications. Framed by the government as an update to outdated 1993 legislation, the bill aims to give law enforcement clearer legal authority to investigate serious crime and national security threats, including access to both message content and metadata. However, digital rights advocates warn that the law could normalise intrusive surveillance practices such as remote phone hacking and mass data extraction, potentially affecting journalists, activists, and ordinary citizens. Critics argue that Ireland's weak oversight structures and broad definitions of "serious crime" risk conflict with strict EU privacy and human rights standards, especially the requirement that surveillance be necessary, proportionate, and tightly controlled. Impact Policies

CREEPING DIGITAL AUTHORITARIANISM AND (IN)SECURITY IN PAKISTAN SURVEILLANCE

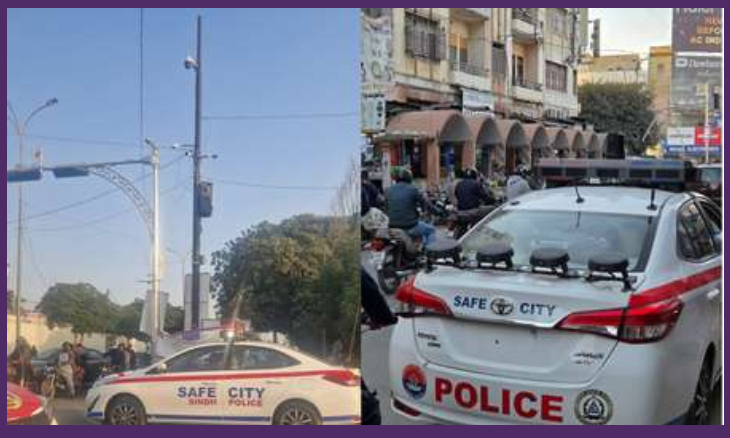


IMAGE SOURCE: ST AUGUSTINE RECORD

The article argues that Pakistan is gradually sliding into "digital authoritarianism" through a combination of advanced surveillance technologies and expansive cybercrime laws like PECA, which together allow the state to monitor, censor, and punish online and offline dissent. It explains how tools such as "Safe City" surveillance systems, facial recognition, and telecom monitoring—paired with vague legal provisions criminalizing "anti-state" or "false" content—create a chilling effect, pushing journalists, activists, and ordinary citizens toward self-censorship and fear-driven behavior. The piece highlights how narratives like the "digital terrorist" are used to justify these measures, while weak legal safeguards and lack of transparency enable abuse, ultimately undermining political freedoms, restricting protest, and reshaping everyday digital life under constant surveillance. Focaalblog

MEXICO'S SURVEILLANCE GIANT: HOW SEGURITECH BUILT A QUIET EMPIRE WATCHING ENTIRE CITIES

IMAGE SOURCE: REST OF WORLD

The investigation by Rest of World reveals how Mexican company Grupo Seguritech has quietly built a massive surveillance empire by supplying governments with integrated "smart security" systems that combine thousands of CCTV cameras, facial recognition tools, license plate readers, drones, and AI-powered command centers. Originally starting as a home alarm business, the company has grown into a major contractor managing large-scale "C5" security hubs that allow authorities to monitor entire cities in real time, including prisons, highways, and border regions. The system is marketed as a public safety and crime-fighting solution, but its scale and integration give governments continuous visibility into public spaces, raising concerns about oversight, transparency, and potential misuse. The report also highlights Seguritech's expansion beyond Mexico into other Latin American countries and even the United States, showing how privatized surveillance infrastructure is becoming increasingly transnational and deeply embedded in state security operations. Rest of World

HIDDEN SPY POWERS: HOW A LEGAL LOOPHOLE COULD PUT BLACK COMMUNITIES UNDER WATCH

IMAGE SOURCE: NEWSONE

The Foreign Intelligence Surveillance Act Section 702 is under scrutiny as critics argue it enables warrantless surveillance that disproportionately harms Black communities, continuing a long history of government monitoring of Black activists and movements. The article warns that loopholes in the law allow authorities to access Americans' private communications without sufficient oversight, raising fears of political targeting—especially under administrations accused of expanding surveillance powers. Drawing parallels to past abuses like COINTELPRO, it highlights bipartisan concern but stresses that reforms have been insufficient, urging stronger protections such as warrant requirements and greater accountability to prevent civil liberties violations and protect marginalized communities from being unfairly labelled as threats. Newsone

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI ON THE STREETS: BIHAR'S HIGH-TECH TRAFFIC SYSTEM THAT WATCHES EVERY MOVE

IMAGE SOURCE: PATNA PRESS

The article explains how Bihar is rolling out an AI-powered Intelligent Traffic Management System (ITMS) that uses advanced surveillance tools—including high-definition cameras, automatic number plate recognition, and in some cases facial recognition—to monitor roads, detect violations, and automatically issue fines without human intervention. Covering hundreds of busy intersections and expanding across major cities like Patna, the system aims to reduce congestion, improve road safety, and crack down on offenses such as speeding, helmet violations, and reckless driving. While officials present it as a modern, efficient solution that minimizes corruption and improves enforcement, the growing use of real-time monitoring and biometric technologies raises concerns about increased surveillance, data privacy, and the broader implications of constant tracking in public spaces. Patna Press

ALBANIA'S AI TURN: A SURVEILLANCE STATE WITHOUT OVERSIGHT?

IMAGE SOURCE: TRANSITIONS

The article explores how Albania's rapid adoption of artificial intelligence—symbolized by the appointment of a virtual AI "minister" and the rollout of a nationwide "Smart City" surveillance system—is being promoted as a leap toward efficiency, transparency, and anti-corruption, but is unfolding with little public oversight or accountability. While officials claim these systems simply assist human decision-making, critics highlight a troubling lack of transparency about how the technology works, who controls the data, and the role of foreign companies in managing critical infrastructure. Combined with weak legal frameworks, no prior risk assessments, and limited public consultation, the expansion of AI-driven governance and surveillance raises serious concerns about privacy, data protection, and democratic control, with experts warning that Albania risks normalizing powerful monitoring systems before safeguards are in place. Transitions

INTEL WATCH

Watching the watchers. Guarding the guardians.

PAPAL VISIT OR MASS SURVEILLANCE? EQUATORIAL GUINEA ROLLS OUT CAMERAS ACROSS THE NATION

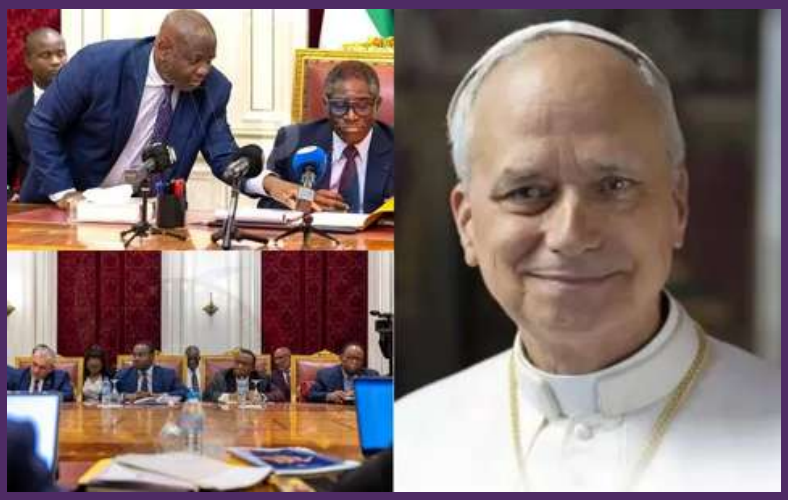


IMAGE SOURCE: ACI AFRICA

The article reports that Equatorial Guinea's government plans to install a network of surveillance cameras across key locations nationwide, with Chinese tech giant Huawei providing the system ahead of the visit of Pope Leo XIV. Officials say the move is aimed at strengthening security and coordination during the high-profile event, which is expected to attract large crowds and global attention. The deployment—offered at no cost to the government—may also include advanced traffic-monitoring features such as speed-detecting radars integrated into the broader system. While framed as a temporary safety measure for the papal visit, the initiative reflects a broader trend of expanding surveillance infrastructure in public spaces, raising questions about how such systems might be used beyond the event and what safeguards, if any, are in place. Aci Africa

FACIAL RECOGNITION PUT ON HOLD: UK POLICE BACKTRACK OVER RACIAL BIAS CONCERNS

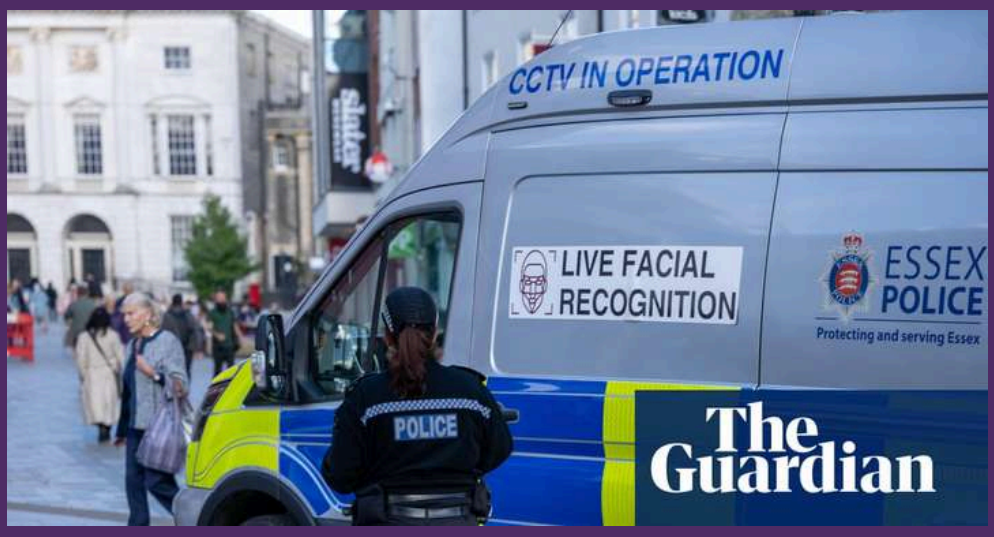


IMAGE SOURCE: TRANSITIONS

Essex Police has paused its use of live facial recognition cameras after a study raised concerns that the technology may produce biased outcomes, particularly in how accurately it identifies people from different demographic groups. The decision follows a Cambridge University-led evaluation of real deployments, which found that while false positives were rare, the system was more likely to correctly identify Black individuals compared to other ethnic groups and showed differences in accuracy based on gender. Although officials say the tool can help locate suspects on watchlists and is intended to improve public safety, regulators like the Information Commissioner's Office have urged caution and further testing to ensure fairness. The pause highlights growing scrutiny of AI-driven policing in the UK, with critics warning that without stronger safeguards, facial recognition could reinforce existing inequalities and undermine public trust. The Guardian

FISA SURVEILLANCE VOTE SPARKS FIERCE DEBATE AS CONGRESS SPLITS ON WARRANTLESS MONITORING

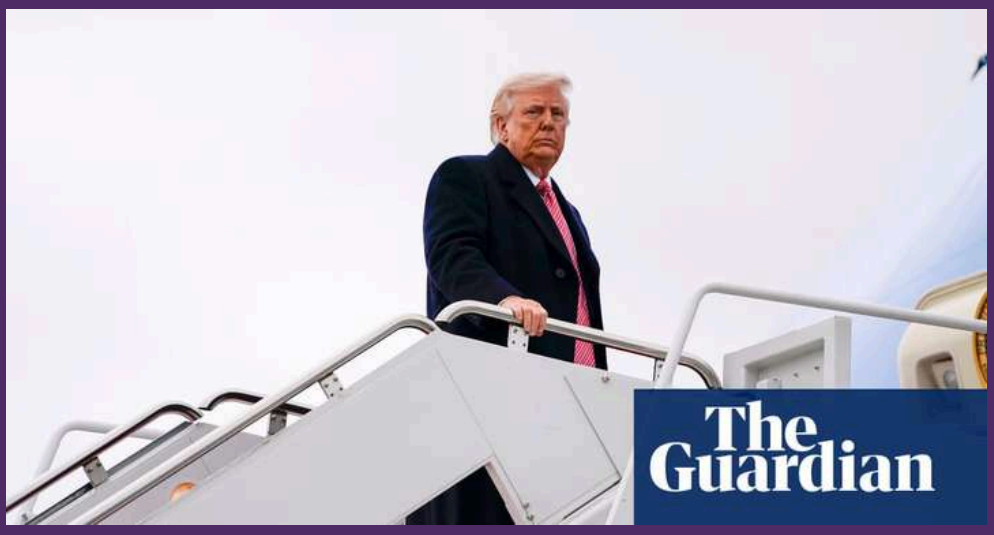


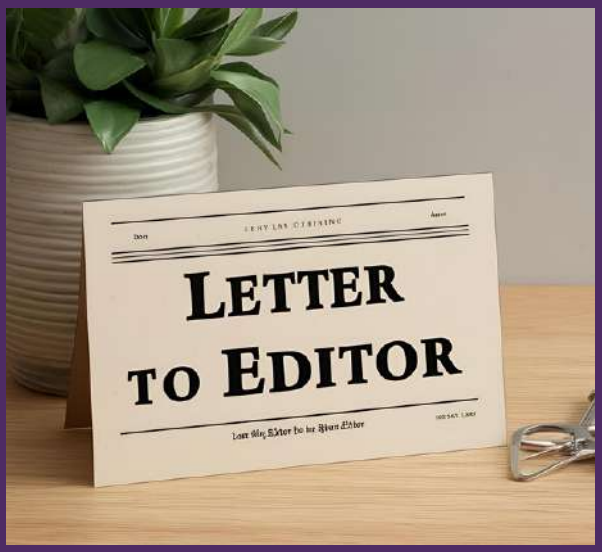
IMAGE SOURCE: THE GUARDIAN

The article covers the intense political battle in the United States over renewing Section 702 of the Foreign Intelligence Surveillance Act (FISA), a controversial law that allows intelligence agencies to conduct surveillance on foreign targets without a warrant but can also capture Americans' communications. Lawmakers are deeply divided, with national security officials and some politicians pushing for a "clean" renewal to maintain surveillance capabilities, while a bipartisan group of critics demands reforms such as requiring warrants to protect civil liberties. The disagreement led to failed votes and only a short-term extension of the law, highlighting growing unease about past abuses—including improper searches of Americans' data—and the broader tension between security and privacy in the digital age. The Guardian

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 Now for tomorrow

Global Dialogue

Luminate

Funded by the European Union

We are grateful for the support of our donors!