Issue #5

INTEL WATCH

September 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

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

SURVEILLANCE UPDATES

KASPERSKY URGES LAYERED DEFENCE AS CYBERATTACKS GROW MORE SOPHISTICATED IN SOUTH AFRICA

IMAGE SOURCE: TECH AFRICA NEWS

Kaspersky's analysis reveals a sharp increase in sophisticated cyberattacks in South Africa during the first half of 2025, with a 123% rise in backdoor attacks compared to the previous year. The cyber threat landscape includes rapid growth in banking trojans, password stealers, spyware, and malware incidents, targeting both individuals and enterprises. These attacks exploit vulnerabilities like weak perimeter defenses, unpatched systems, and unsecured IoT devices, while attackers increasingly use AI-driven malware and automated phishing campaigns. Kaspersky urges South African organizations to adopt a layered defense strategy with intelligence-led protection measures, including stronger authentication, endpoint detection tools, employee training, and improved patch management. The rising threat underscores the need for enhanced cyber resilience through technological upgrades, human capital development, and stronger law enforcement cooperation to effectively counter evolving cybercrime challenges in the region. The article emphasizes the urgency of systemic changes to safeguard the country’s digital infrastructure and economy amid escalating cyber threats - Tech Africa news

KASPERSKY: AFRICA HIT BY 138 MILLION CYBERATTACKS IN JUST 6 MONTHS

IMAGE SOURCE: TECH WEEZ

In the first half of 2025, Africa experienced a staggering 138 million cyberattacks, as reported by Kaspersky. The attacks included 42.4 million web attacks and 95.6 million on-device incidents, with significant increases in spyware, password stealers, and backdoor infections compared to the previous year. Nigeria faced over 1.46 million online attack attempts, with nearly 20% of its population targeted by various scams like phishing and fake Wi-Fi networks. Industrial sectors, especially in Nigeria, saw high malware targeting, affecting critical infrastructure such as power and construction. Despite a drop in overall phishing attempts, financial phishing surged by 46%. These trends highlight the growing sophistication and volume of cybersecurity threats across the continent, underscoring the urgent need for improved cybersecurity measures and awareness among businesses and individuals - Tech Weez

KENYA'S CYBER THREATS UP 80.8PC TO 4.6BN ON HEIGHTENED SURVEILLANCE

IMAGE SOURCE: BUSINESS CAPITAL

Kenya experienced a dramatic 80.8% increase in detected cyber threats, totaling 4.6 billion incidents between April and June 2025, up from 2.5 billion in the previous quarter, driven largely by enhanced surveillance capabilities of the upgraded KE-CIRT tools. The most significant rise was in Distributed Denial-of-Service (DDoS) attacks, which surged by 255.6%, alongside substantial increases in mobile application attacks (177.7%), web application attacks (150.8%), malware (93.1%), and system vulnerabilities (81.9%). The growth in cyber threats is attributed to heightened internet adoption, weak cybersecurity defenses, and the increasing use of artificial intelligence by cybercriminals to facilitate sophisticated social engineering, especially phishing. Kenyan firms face challenges in combating these threats due to a shortage of cybersecurity experts, emphasizing the need for improved defensive capabilities and skilled personnel in the sector - Business Capital

ETHIOPIA EMERGES AS TOP TARGET OF CYBERATTACKS AMID RAPID DIGITAL GROWTH

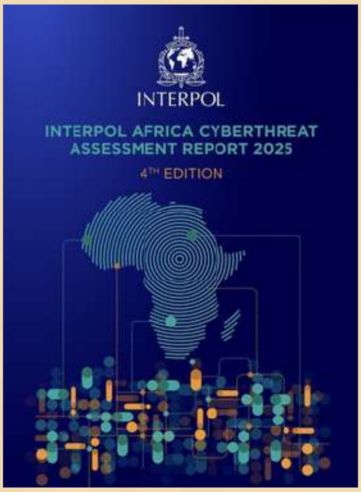

IMAGE SOURCE: CAPITAL NEWS

Ethiopia has emerged as the top target of cyberattacks globally in 2024 and early 2025, driven by rapid digital growth and increasing internet adoption. According to the INTERPOL Africa Cyberthreat Assessment Report 2025, Ethiopia leads in malware detections, with critical infrastructure such as government institutions, financial services, and major development projects frequently targeted by sophisticated cyber threats including phishing scams, AI-driven social engineering, and digital sextortion. The country has seen persistent Distributed Denial-of-Service (DDoS) attacks, especially on telecommunications, with techniques like DNS Amplification and UDP floods. In response, Ethiopia has intensified cybersecurity measures, including thwarting thousands of attacks, enhancing legal frameworks, and raising public awareness. Experts warn that as Ethiopia's digital economy expands, cyber threats will grow in complexity and volume, making proactive defense strategies and improved cyber resilience crucial for protecting national sovereignty and digital infrastructure - Capital News

AFRICAN NATIONS WARNED OF RISING AI-POWERED CYBERATTACKS ON HOTELS

IMAGE SOURCE: CHINA DAILY

The article warns African nations, particularly major tourist destinations like South Africa and Kenya and business hubs like Nigeria, about a surge in AI-powered cyberattacks targeting hotels. Cybercriminals are increasingly using sophisticated AI tools to launch phishing emails disguised as legitimate reservation or job application requests, which install malware like VenomRAT on hotel systems to access sensitive guest data, including payment information. These attacks are becoming harder to detect due to AI-generated convincing schemes. Interpol reports that cybercrime accounts for over 30% of crime in parts of Africa, with phishing being the most common threat alongside ransomware, business email compromise, and digital sextortion. The article stresses that cybersecurity is crucial for Africa's digital sovereignty, institutional resilience, and economic stability, urging hotels to enhance email security, anti-spam measures, and cautious handling of unknown files to mitigate risks. This rise in AI-driven attacks reflects a broader trend of increasing cyber threats across the continent - China Daily

KASPERSKY: SMBS IN EUROPE AND AFRICA HIT BY MALWARE DISGUISED AS LEGITIMATE TOOLS

IMAGE SOURCE: INTELLIGENT CIO

Small and medium-sized businesses (SMBs) in Europe and Africa are increasingly targeted by cybercriminals who disguise malware and potentially unwanted applications (PUAs) as legitimate and trusted productivity tools such as ChatGPT, Microsoft Office apps, and Google Workspace. According to Kaspersky, nearly 8,500 SMB users faced such cyberattacks between January and April 2025, with malware disguised most frequently as Zoom (41% of detections), followed by Microsoft Outlook, PowerPoint, Excel, Word, and Teams. In Africa, backdoors constitute over half of all malware incidents, while in Europe, Austria, Italy, and Germany are the most affected. Attackers use backdoors, trojans, and downloaders to infiltrate systems, exploiting SMBs' limited cybersecurity budgets and resources. Kaspersky emphasizes that effective defense for SMBs lies not only in expensive tools but in understanding attacker methods and reinforcing system defenses strategically. Additionally, phishing and spam campaigns targeting SMBs continue to rise, tricking businesses into credential theft and financial fraud by mimicking business needs and services - Intelligent CIO

HACKERS ARE DISGUISING MALWARE AS CHATGPT, MICROSOFT OFFICE, AND GOOGLE DRIVE TO DUPE WORKERS

IMAGE SOURCE: IT PRO

Hackers are increasingly disguising malware and potentially unwanted applications as popular productivity tools like ChatGPT, Microsoft Office apps, and Google Drive to target small and medium-sized businesses (SMBs) across Europe and Africa. Between January and April 2025, Kaspersky reported nearly 8,500 SMB users faced such cyberattacks, with attackers mimicking platforms like Zoom (41% of threats), Microsoft Outlook, PowerPoint, Excel, Word, and Teams. In Europe, Austria, Italy, and Germany saw the highest incidents, while in Africa, Morocco was most affected. The main types of threats include backdoors, trojans, and downloaders that infiltrate systems stealthily. Experts warn that SMBs, often operating with limited cybersecurity budgets, need to focus on employee awareness, strong authentication practices including multi-factor authentication, regular software updates, and controlled software installation to defend effectively against these deceptive attacks. Understanding attacker methods is emphasized as the best defense rather than relying solely on costly tools - IT Pro

EXPOSED: SAMSUNG PHONES EMBEDDED WITH ‘UNREMOVABLE’ ISRAELI SPYWARE

IMAGE SOURCE: CANARY

Samsung has secretly installed spyware developed by the Israeli company IronSource on its A and M series smartphones sold across the Middle East and North Africa (MENA), raising serious concerns about digital surveillance and privacy. This pre-installed app, called AppCloud, automatically downloads additional software including one named Aura, which collects extensive personal data such as IP addresses, device fingerprints, biometrics, and location information without user consent. The spyware is especially difficult to remove as it reinstalls itself automatically, effectively making privacy protection nearly impossible for users. The collected data reportedly aids Israeli intelligence in monitoring and potentially targeting individuals, especially in politically tense regions like Lebanon, where it complements known surveillance tools used against groups like Hezbollah. This partnership between Samsung and the Israeli firm has sparked fears of cyber espionage and supply chain attacks, underlining the urgent need for independent communication infrastructures in the region to protect citizens from invasive digital monitoring - Canary

NEW REPORT ON COMMERCIAL SPYWARE VENDORS DETAILING THEIR TARGETS AND INFECTION CHAINS

IMAGE SOURCE: CYBER SECURITY NEWS

A new report by Sekoia.io’s Threat Detection & Research team reveals that commercial spyware vendors have evolved from niche technology suppliers into a sophisticated, multi-billion-dollar global ecosystem posing unprecedented threats to journalists, activists, and civil society worldwide. These private firms have industrialized spyware deployment, offering fully integrated surveillance solutions that rival state-sponsored cyber capabilities. Emerging prominently during the Arab Spring protests, companies like Gamma Group and later Israeli firms NSO Group, Candiru, and Intellexa advanced spyware technology, including zero-click exploits that allow remote compromise without user interaction. Infection chains often involve sophisticated attack vectors like malicious PDFs exploiting messaging apps’ vulnerabilities. The report highlights how these vendors continuously adapt to evade detection, utilizing complex command-and-control infrastructures and even leveraging physical device access at borders. This evolution democratizes advanced cyber surveillance, enabling widespread abuse that threatens human rights, digital privacy, and freedom globally. The findings urge urgent policy attention to regulate this growing market and protect vulnerable groups from invasive, state-backed or private hacking tools - Cyber Security News

UNSECURED SERVERS EXPOSE OVER 250M GLOBAL IDENTITY RECORDSRACT WITH PARAGON SPYWARE REVIVED

IMAGE SOURCE: SC MEDIA

A recent security incident revealed that unsecured servers exposed over 250 million global identity records, intensifying concerns about data privacy amid the revival of Paragon spyware operations. Paragon, an Israeli spyware company, is known for its stealthy Graphite spyware that can infect devices without user interaction via zero-click exploits, giving attackers full access to private communications across encrypted messaging apps like WhatsApp and Signal. The spyware was reportedly used to target journalists, activists, and civil society members, raising alarm over violations of fundamental rights and democratic principles. Paragon's advanced infection methods involve exploiting vulnerabilities through features like WhatsApp's automatic content preview, allowing infection via malicious PDFs sent after silently adding targets to attacker-controlled groups. Following public outcry and investigations, Paragon ended a controversial contract with Italy after alleged misuse against journalists and activists was exposed, highlighting ongoing challenges in regulating commercial spyware and preventing abuse by state clients - SC Media

REPRESSION MONITOR

KENYAN FILMMAKERS INSTALLED WITH FLEXISPY SPYWARE THAT MONITORS MESSAGES AND SOCIAL MEDIA

IMAGE SOURCE: CYBER SECURITY NEWS

Four Kenyan filmmakers-MarkDenver Karubiu, Bryan Adagala, Nicholas Wambugu, and Christopher Wamae—had FlexiSPY spyware covertly installed on their devices while in police custody in mid-2025, according to forensic analysis by the University of Toronto’s Citizen Lab. The spyware, capable of comprehensive monitoring including real-time access to messages, emails, social media, calls, location, passwords, photos, videos, and microphone activation, represents a severe breach of journalistic privacy and security. The filmmakers were initially arrested on charges related to a BBC documentary implicating Kenyan security forces in killings but were released without charges, though their devices remained in custody for over two months, allowing installation of the spyware. FlexiSPY’s advanced persistence allows it to evade detection and removal, posing serious risks to the confidential communications of journalists, raising broader concerns over state surveillance abuses against media professionals and press freedom advocates in Kenya and globally.Four Kenyan filmmakers had FlexiSPY spyware secretly installed on their devices while in police custody in 2025, according to forensic analysis from the University of Toronto’s Citizen Lab. The filmmakers were arrested in connection to a BBC documentary implicating Kenyan security forces in protester killings but released without charges, although their devices stayed with authorities for months, allowing spyware installation. FlexiSPY grants comprehensive access to private communications, including messages, emails, social media, calls, location, passwords, and can activate microphones, posing a severe breach of journalistic privacy. Its advanced stealth and persistence enable long-term monitoring and data collection, highlighting growing concerns about state surveillance targeting journalists and media professionals, threatening press freedom and source confidentiality globally - Cyber Security News

INTERNET SHUTDOWNS IN AFRICA ON UPWARD TRAJECTORY

IMAGE SOURCE: TECH TARGET

Internet shutdowns in Africa have increased significantly, with more than 190 incidents recorded across 41 countries since 2016, according to the African Digital Rights Network (ADRN). Governments frequently use these blackouts to suppress dissent, disrupt protests, and influence elections, effectively reinforcing authoritarian control. Countries like Ethiopia, Sudan, and Algeria have experienced the highest number of shutdowns, with Ethiopia using internet blackouts notably during armed conflicts to limit political discourse and conceal human rights abuses. Shutdown tactics include power cuts to communication infrastructure, traffic manipulation, deep packet inspection, and data throttling, often implemented with the cooperation of telecom companies under government pressure. These shutdowns severely impact citizens' access to information, communication, and economic activities while violating fundamental rights such as freedom of expression and association. Despite these challenges, African civil society has shown resilience by employing technologies like VPNs and satellite internet to bypass shutdowns and advocating through litigation and public campaigns. The trend reflects a troubling normalization of digital authoritarianism that threatens democratic participation and human rights on the continent - Tech Target

GOV'T DISPLAYS DISREGARD FOR PRIVACY LAWS AS DIGITAL SURVEILLANCE USED TO TAME CRITICS

IMAGE SOURCE: CITIZEN DIGITAL

The article highlights the Kenyan government's growing disregard for privacy laws as it increasingly uses digital surveillance to monitor, intimidate, and suppress critics and dissenting voices. Recent legislative efforts, such as the Kenya Information and Communications (Amendment) Bill 2025, propose sweeping surveillance powers without adequate safeguards, enabling real-time tracking of internet usage and social media activity. These moves coincide with crackdowns on activists, journalists, and opposition figures through tactics including enforced disappearances, abductions, and prosecutions under cybercrime laws. Civil society groups warn that the expanding surveillance infrastructure threatens freedom of expression, privacy, and democratic participation, creating a chilling effect on political dissent. Despite constitutional protections, Kenya risks becoming a state where mass digital monitoring is normalized and used to silence opposition under the guise of national security and public order.The Kenyan government has increasingly disregarded privacy laws by employing extensive digital surveillance to monitor and suppress critics. Legislative proposals like the 2025 Kenya Information and Communications (Amendment) Bill threaten to expand government surveillance powers, enabling real-time monitoring of online activity without adequate safeguards. This digital crackdown coincides with protests, enforced disappearances, and criminalization of dissent, particularly targeting activists, journalists, and political opponents. Civil society warns that these measures undermine free expression, privacy, and democracy, creating a chilling effect on political dissent despite constitutional protections. The government's moves align with a broader global trend of using digital tools to stifle opposition under the pretense of national security - Citizen Digital

PAKISTAN SPYING ON ITS OWN CITIZENS USING CHINESE TECHNOLOGY, CLAIMS AMNESTY INTERNATIONAL INVESTIGATION REPORT

IMAGE SOURCE: WION NEWS

Amnesty International's 2025 investigation reveals that Pakistan employs extensive and unlawful mass surveillance and censorship systems built with technology from Chinese, European, Emirati, North American, and Canadian companies. Key components include a Chinese-supplied internet firewall known as the Web Monitoring System (WMS 2.0), which censors social media and filters online content, and the Lawful Intercept Management System (LIMS) from Germany via an Emirati company, which enables phone tapping and real-time interception of calls and messages from over 4 million citizens simultaneously. These technologies facilitate pervasive monitoring and censorship designed to suppress political opposition, restrict freedom of expression, and control internet access, particularly intensifying after political upheavals in 2022. The report highlights regulatory failures allowing global corporations to fuel human rights abuses through surveillance exports, as well as the harmful impact on democratic freedoms and public trust in Pakistan - Wion News

STUDENTS UNDER SURVEILLANCE

IMAGE SOURCE: TD ORIGINAL

The article "Students Under Surveillance" from Truthdig highlights the accelerating use of advanced digital surveillance technologies on university campuses, especially targeting student activism around Palestine. Unlike traditional CCTV systems, modern surveillance employs interconnected AI-powered video management systems that can track individuals across multiple locations using facial recognition and behavioral analytics. This is combined with social media monitoring and big data analysis to profile and repress protesters. Since protests began in late 2023, universities have increased police involvement, arrests, and surveillance infrastructure, leading to the chilling of student activism and academic freedom. Foreign students are particularly vulnerable, facing deportation risks linked to protest participation. Surveillance extends beyond cameras to include online surveillance, doxxing by organizations like Canary Mission, and partnerships between universities and law enforcement using sophisticated software. Despite these challenges, some universities have rolled back surveillance after negative public exposure, and advocates call for legal challenges and greater transparency to protect students' constitutional rights to protest and free speech in the face of widespread digital repression.The article "Students Under Surveillance" from Truthdig details the increasing use of advanced digital technologies for repressing student activism, particularly related to Palestine solidarity protests on U.S. campuses since late 2023. Unlike older analog surveillance, new AI-powered video management systems connect numerous cameras across campus to track individuals' movements and behavior using facial recognition and pattern analysis. Social media monitoring and big data analytics are also employed to identify, profile, and target protesters, with heightened police involvement resulting in arrests and deportations, especially targeting foreign students. This surveillance extends to doxxing campaigns by organizations like Canary Mission, which shares information with government authorities, amplifying repression. Despite some universities reducing surveillance after public backlash, the expansion of these digital tools poses significant threats to freedom of expression, academic freedom, and civil rights, calling for legal challenges and increased transparency to counter this growing digital repression - TD original

GREECE USED PREDATOR SPYWARE ON MINISTERS AND MILITARY

IMAGE SOURCE: DATA ECONOMY

The 2022 Greek surveillance scandal, known as "Predatorgate," revealed that the Greek National Intelligence Service (EYP) used Predator spyware, marketed by the Israeli company Intellexa, to target at least 87 individuals including government ministers, senior military officials, journalists, and opposition figures. The spyware allowed deep device compromise, granting access to calls, messages, cameras, and microphones. The scandal began when Nikos Androulakis, a Member of the European Parliament, was targeted by a malicious message designed to install the spyware. The crisis led to the resignation of the EYP head Panagiotis Kontoleon and Prime Minister Mitsotakis's aide and nephew Grigoris Dimitriadis, who oversaw the intelligence agency. Though the government denied official use of Predator, investigations showed an overlap between targets surveilled by EYP and those targeted by the spyware, raising suspicions of coordination. Greece subsequently legalized spyware use under strict conditions, but critics argue the law reduces transparency and accountability. The scandal has sparked significant political fallout and international scrutiny over Greece's democratic practices - Data Economy

DIGITAL SURVEILLANCE: HOW STATES ARE SPYING ON THE RESISTANCE

IMAGE SOURCE: BERLIN

The article "Digital Surveillance: How States Are Spying on the Resistance" from Berlin.de examines the growing sophistication and scale of state surveillance used to monitor, suppress, and criminalize resistance movements worldwide. Governments increasingly deploy AI-driven technologies such as facial recognition, biometric tracking, and big data analytics, often in partnership with private companies like Palantir, to convert public spaces into zones of constant observation. These tools enable authorities to preemptively identify and target activists, disrupt protests, and stifle free expression. The article highlights how digital repression reshapes dissent by forcing movements underground or making traditional forms of protest untenable due to pervasive surveillance and repression. Historical parallels to Jeremy Bentham's panopticon are drawn, illustrating how modern tech instills a sense of constant watchfulness that influences behavior and reduces resistance. The challenges faced by contemporary movements include overcoming integrated state-private surveillance networks, transnational policing, and highly lethal military technologies, all of which exacerbate power asymmetries and reduce space for effective opposition - Berlin

SURVEILLANCE BY AL GOVT: SPENDING SPIKED BEFORE LAST THREE ELECTIONS

IMAGE SOURCE: BIOMETRIC UPDATE

UK police facial recognition technology has reached a new scale, with live facial recognition (LFR) systems scanning over 50,000 faces in a single day around London Underground stations in August 2025. The Metropolitan Police have expanded the use of LFR as part of efforts to reduce crime, deploying more cameras and specialized police vans equipped with real-time facial recognition software from NEC. The number of individuals on police watchlists has increased to over 16,000 in 2025 from under 7,000 in 2022, driving a rise in daily scans from under 12,000 to over 50,000. While police credit the technology with over 1,000 arrests to date, including serious crimes like domestic abuse and rape, privacy advocates criticize the rapid expansion, urging the UK government to introduce stricter regulations and safeguards. A judicial review is underway to assess the system's alignment with human rights law amid ongoing debates about the technology's impact on privacy and civil liberties - Biometric Update

CHINESE SPIES IMPERSONATED KEY HOUSE REPUBLICAN TO INFECT US GOVERNMENT WITH MALWARE

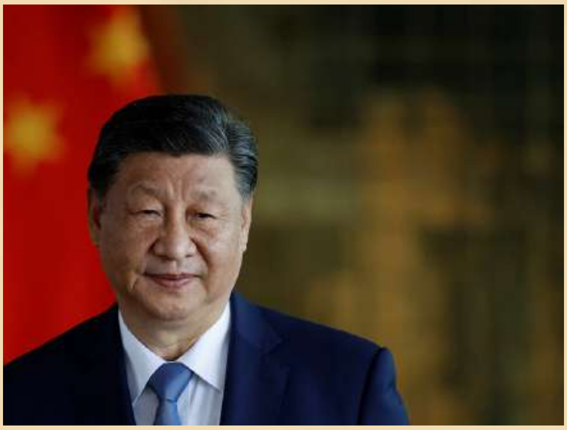

IMAGE SOURCE: RAW STORY

Chinese state-backed hackers impersonated Representative John Moolenaar, the chair of the U.S. House Select Committee on China, in a sophisticated phishing campaign targeting U.S. government agencies, trade organizations, law firms, think tanks, and foreign governments amid sensitive trade negotiations. The hackers sent emails under Moolenaar's name containing attachments that deployed malware to compromise recipients' systems, aiming to steal sensitive data related to U.S.-China trade policies. The campaign, linked to the notorious APT41 hacking group associated with Beijing’s Ministry of State Security, sought to exploit trust by posing as a known critic of China to elicit quick responses. This cyber espionage reflects an advanced threat targeting congressional processes and broader U.S. policy deliberations, highlighting vulnerabilities in the U.S. legislative system and the strategic importance of securing communications around high-level negotiations - Raw Story

POLICE FACIAL RECOGNITION VANS 'FEEL TOTALITARIAN'

IMAGE SOURCE: MSN

The article discusses serious privacy and national security concerns related to Chinese-made connected vehicles, especially electric vehicles (EVs), which collect vast amounts of data and are susceptible to hacking. These cars generate extensive user and biometric data, including geographic locations, driving behavior, voice commands, and smartphone interactions, which can be transmitted to manufacturers and potentially shared with third parties including governments. Chinese components, particularly cellular IoT modules (CIMs), dominate the global market, raising fears that the Chinese government could exploit these vehicles for intelligence gathering, surveillance, or remote sabotage during geopolitical conflicts. While no public evidence yet confirms deliberate misuse, security experts warn about the potential for catastrophic outcomes if vulnerabilities are exploited, such as disabling vehicle functions remotely. Western governments and companies have responded with restrictions and warnings to mitigate these risks amid growing geopolitical tensions with China - MSN

INTELLIGENCE AGENCIES

TRUMP’S ICE EXPANDS SURVEILLANCE TECH FOR DEPORTATION CRACKDOWN

IMAGE SOURCE: IT SECURITY NEWS

The article reports that the U.S. Immigration and Customs Enforcement (ICE) agency has significantly expanded its surveillance capabilities to support President Trump’s mass deportation campaign, which has resulted in about 350,000 deportations within the first eight months of his administration. ICE has invested millions in advanced technologies, including a $3.75 million contract with Clearview AI for facial recognition software that uses an extensive online photo database to identify individuals. Additional tools include forensic software, enterprise licenses for facial recognition, and digital surveillance technologies aimed at tracking and identifying undocumented immigrants across the U.S. These technologies aid ICE in locating and surveilling individuals, raising concerns about privacy violations and the possible chilling effects on immigrant communities. The agency’s technological arsenal reflects a broader effort to use AI and big data to enhance immigration enforcement while sparking debate over civil rights and data privacy - IT Security News

US INVESTMENT IN SPYWARE IS SKYROCKETING

IMAGE SOURCE: WIRED

U.S. investment in the commercial spyware industry surged dramatically in 2024, making the country the largest investor by deal count according to an Atlantic Council report. The number of U.S.-based investors rose from 12 to 31 within a year, outstripping other key investors such as Israel, Italy, and the U.K. This surge undermines U.S. government efforts to restrict abusive spyware through sanctions, entity listings, and executive orders, as some American firms continue to fund spyware vendors with dubious human rights records. Notably, investments in companies like Paragon Solutions and Candiru have sparked controversy due to their products being used to target activists and journalists. The report highlights a significant enforcement gap between U.S. policy and private sector investments, calling for expanded government oversight and stricter controls on outbound investments in spyware to curb its proliferation and misuse. This investment trend raises concerns about human rights abuses and challenges U.S. credibility in regulating the global spyware market - Wired

US IMMIGRATION AGENCY REACTIVATES PARAGON SPYWARE CONTRACT

IMAGE SOURCE: WEBSITE PLANET

The U.S. Immigration and Customs Enforcement (ICE) agency has reactivated a $2 million contract with Israeli spyware company Paragon Solutions, whose spyware can covertly hack smartphones, access encrypted messaging apps like WhatsApp and Signal, and turn devices into listening tools. The contract, initially signed during the Biden administration in 2024, was placed under a stop-work order amid concerns over misuse of Paragon's "Graphite" spyware against journalists and activists in countries like Italy. However, the contract was quietly reinstated in August 2025 under the Trump administration after Paragon was acquired by a U.S.-based private equity firm, effectively reclassifying it as a domestic vendor and bypassing a Biden-era executive order restricting spyware use from foreign companies. This reactivation has sparked controversy due to the spyware’s invasive capabilities and its documented history of human rights abuses, raising alarms about privacy violations and misuse within U.S. law enforcement operations - Website Planet

SURVEILLANCE SHOWDOWN: ICE UNLEASHES AI & SPYWARE FOR MASS DEPORTATIONS

IMAGE SOURCE: OPEN TOOLS

The article explains that U.S. Immigration and Customs Enforcement (ICE) has reactivated a $2 million contract with Paragon Solutions, an Israeli-founded spyware company, which had previously been put on hold due to concerns over misuse and human rights violations. Paragon's technology, known as Graphite, is highly intrusive, capable of hacking smartphones, accessing encrypted messaging apps, extracting data, and turning devices into listening tools. The contract was initially suspended during the Biden administration after investigations revealed Paragon's spyware was used against journalists and activists in Europe, potentially violating an executive order restricting U.S. government use of commercial spyware with abusive histories. However, the contract was reinstated after Paragon was acquired by a U.S.-based investment firm and merged with another American company, effectively making it a domestic vendor. This move has sparked controversy and renewed debates about privacy, civil rights, and the ethical use of spyware by law enforcement, especially in light of ICE's aggressive deportation campaigns - Open Tools

AI STARTUP SAYS IT WILL END CRIME BY BLANKETING THE ENTIRE UNITED STATES IN EVER-WATCHING SPY CAMERAS

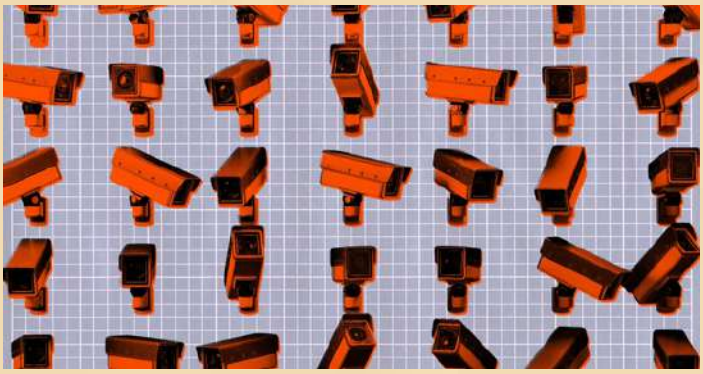

IMAGE SOURCE: FUTURISM

The article covers the AI surveillance startup Flock Safety, which aims to drastically reduce crime in the U.S. by deploying and operating a vast network of over 80,000 AI-powered cameras across highways, roads, and parking lots. Valued at $7.5 billion, the company partners with law enforcement, private businesses, and homeowners associations to create an integrated surveillance web that simplifies data access for police investigations. Flock is also introducing American-made drones equipped with cameras to expand their monitoring capabilities. While touting crime prevention and public safety benefits, critics express concern that such mass surveillance disproportionately targets minority and immigrant communities, raising privacy and civil liberty issues. Despite backlash and some jurisdictions banning license plate reader technologies, Flock continues to grow its presence with AI-enhanced tools and expansive data integration aimed at delivering real-time insights for law enforcement and city management - Futurism

UN EXPERTS DENOUNCE TRANSNATIONAL SURVEILLANCE OF NICARAGUANS IN EXILE

IMAGE SOURCE: CONFIDENCIAL

The article covers the AI surveillance startup Flock Safety, which aims to drastically reduce crime in the U.S. by deploying and operating a vast network of over 80,000 AI-powered cameras across highways, roads, and parking lots. Valued at $7.5 billion, the company partners with law enforcement, private businesses, and homeowners associations to create an integrated surveillance web that simplifies data access for police investigations. Flock is also introducing American-made drones equipped with cameras to expand their monitoring capabilities. While touting crime prevention and public safety benefits, critics express concern that such mass surveillance disproportionately targets minority and immigrant communities, raising privacy and civil liberty issues. Despite backlash and some jurisdictions banning license plate reader technologies, Flock continues to grow its presence with AI-enhanced tools and expansive data integration aimed at delivering real-time insights for law enforcement and city management - Confidencial

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

CONFIDENTIAL
Operational and Performance Review
The following table depicts
CDSO

FIND US ON SOCIAL MEDIA

@IntewatchNews

HAVE ANY QUESTIONS?

info@intelwatch.org.za

Global Dialogue

Funded by the European Union

We are grateful for the support of our donors!