Issue #1

INTEL WATCH

May 2025

Watching the watchers. Guarding the guardians.

THE WATCHER

Monthly

DEFENDING HUMAN RIGHTS, PROTECTING CIVIC SPACE

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

EXCLUSIVE INTELWATCH REPORTS & RESEARCH

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

INTEL WATCH

Watching the watchers. Guarding the guardians.

WELCOME TO ISSUE #1 OF THE WATCHER

IN THIS ISSUE:

INTEL WATCH

Watching the watchers. Guarding the guardians.

WELCOME TO ISSUE #1 OF THE WATCHER

- Fears explode over new TSA face scan tech as privacy watchdogs sound alarm over 'surveillance'
- New Orleans Police Secretly Used Prohibited Facial Recognition Surveillance for Years
- Project NOLA's facial recognition push raises legal and civil rights questions
- TSA says new controversial technology is 'key' for airport security. Can you opt out?
- Burma Junta Adopts China's Digital Blueprint for Repression

Intelligence Agencies

- Google Expands Advanced Protection in Android 16 to Tackle Spyware Threats
- UK Fraud Bill targets benefit claimants for mass surveillance
- Open Government: Emancipation for Some, Exclusion for Others

In an era where technology is increasingly weaponized against individuals, Intelwatch exists to ask the critical question: ***Do you know who's watching you?***

EDITORIAL TEAM

EXECUTIVE DIRECTOR — PAULA CRISTINA ROQUE
EDITOR & HEAD OF ADVOCACY AND CAPACITY BUILDING — HERBERT MOYO
CONTENT, DESIGN AND LAYOUT — SISIPHO MBALO

This newsletter is more than just a publication–it's a call to action. Together, we can challenge systems of unchecked power and build a future where privacy is not a privilege but a right.

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS & RESEARCH

UGANDA'S COUNTER-TERRORISM LAWS: SUPPRESSION OF DEMOCRATIC DISSENT

BY INTELWATCH

DOWNLOAD REPORT

Key findings:

Uganda is governed by one of Africa's most effective authoritarians, President Yoweri Museveni. During his tenure he has personalized power and centralized it in the Presidency.

Ahead of the 2026 elections, Uganda's intelligence services have been intensifying authoritarian control and systematically shrinking the political and civic space by increasing repressive clampdowns thereby continuing with a pattern that began with the enactment of the anti-terrorism law. Uganda's implementation of the Anti Terrorism Act of 2002 has revealed a pattern where the law has been weaponised against individuals and groups critical of the government, straying significantly from its original aim of countering terrorism. This legislation has been leveraged to suppress political opposition, media freedom, and civil society activities, creating an environment where activism and dissent are met with legal repercussions under the guise of counter-terrorism. Politicians, journalists and civil society organisations, particularly those involved in human rights advocacy, have all been targeted. As a result, it significantly impacts the democratic space in Uganda, eroding public trust in the legal system and weakening the capacity of human rights defenders to operate freely.

The suppression of public protests further reveals how the Act has been employed to curtail democratic expressions of dissent. Key external actors, including the United States, various European countries, and international bodies like the United Nations, have played roles in operationalising these laws through training, intelligence sharing, and legislative influence, often pushing for alignment with global counter-terrorism standards. This has empowered President Yoweri Museveni and the ruling National Resistance Movement (NRM), which has maintained a firm grip on power.

This report highlights major cases that underscore the misuse of these laws and security units. It explores cases involving journalists, politicians and activists, examining the language used in these contexts, the victims targeted, and the actions taken, such as renditions, arrests, and charges related to treason or threats to national security. It will briefly describe the security units involved in such operations. Additionally, the study investigates the role of external actors in providing training, weapons, intelligence, and surveillance software, shedding light on their influence on these laws' implementation

INTEL WATCH

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS & RESEARCH

UNRAVELLING THE IBERIAN POWER CRISIS: WAS THE BLACKOUT A TEST OF CYBERWARFARE?

BY PAULA CRISTINA ROQUE

Key findings:

On April 28, 2025, a massive blackout struck Portugal, Spain, and parts of southern France, leaving nearly 60 million people without power for approximately 11 hours. The outage caused widespread disruption, shutting down airports, public transport, and communication networks, which led to panic buying and significant challenges for emergency services and the public alike. The blackout was triggered by a sudden "electrical shock" at a critical grid connection between Aragón and Catalonia, which caused erratic power flows and the disconnection from the French grid. This led to a rapid drop in grid frequency and the automatic shutdown of a large portion of solar and wind farms, resulting in the collapse of the entire Iberian power grid within seconds.

At the time, renewables, particularly solar power, supplied around 70% of electricity, but while some officials initially suggested renewables contributed to the instability, experts and government ministers emphasized that the root causes were more complex, involving grid vulnerabilities and underinvestment in storage capacity. The blackout coincided with NATO's largest cyber defense exercise, raising suspicions of a cyberattack, especially after Lisbon airport's radar systems failed an hour prior. Shortly after the blackout, coordinated disinformation campaigns spread false claims of Russian cyberattacks, intensifying public fear. Intelligence agencies had warned of increased Russian cyber activity targeting European infrastructure, and cybersecurity experts highlighted the growing vulnerability of digitally controlled grids. While investigations continue, the event exposed the fragility of interconnected energy systems and underscored the urgent need for enhanced grid resilience and cybersecurity. Overall, the blackout is viewed not only as a technical failure but potentially as a complex hybrid incident involving cyber and disinformation elements, serving as a test of Europe's preparedness against cyberwarfare targeting critical infrastructure - Daily Maverick

EXCLUSIVE INTELWATCH REPORTS & RESEARCH

WHEN BAIL BECOMES A 'VICTORY' – ZIMBABWE'S DANGEROUS WAR ON JOURNALISM CONTINUES

BY HERBERT MOYO

Key findings:

Blessed Mhlanga, a senior journalist with independent Heart and Soul TV in Zimbabwe, was arrested on 24 February 2025 and charged under the Cyber and Data Protection Act with "transmitting data messages that incite violence or damage to property." His arrest followed the airing of interviews with Blessed Geza, a war veteran and former senior member of the ruling ZANU-PF party, who publicly criticized President Emmerson Mnangagwa's government, calling for his resignation over corruption and economic mismanagement.

Mhlanga was detained for 72 days without trial, during which he was denied bail multiple times despite legal appeals. His prolonged pre-trial detention sparked widespread condemnation from international human rights organizations including Amnesty International, Human Rights Watch, the Committee to Protect Journalists, and the International Press Institute (IPI). These groups highlighted the charges as baseless attempts to silence critical journalism and a clear violation of press freedom guaranteed under Zimbabwe's constitution.

On 6 May 2025, Mhlanga was finally granted bail after persistent legal efforts and international pressure, though he still faces serious charges that could lead to imprisonment of up to five or ten years and significant fines. His trial has been postponed to June 17, 2025. The case exemplifies the Zimbabwean government's broader pattern of using cybercrime and other laws to harass, intimidate, and criminalize independent journalists and dissenting voices.

Mhlanga's arrest is not an isolated incident; he had previously faced harassment and arrest in 2022 while reporting on political opposition activities. The article underscores how the government weaponizes the judiciary and legal system to suppress media freedom, with bail itself becoming a hard-won and precarious victory rather than a guarantee of justice or freedom.

In this hostile environment, journalists face threats, intimidation, and censorship, fostering fear and self-censorship within the media. The article calls for the Zimbabwean authorities to drop all charges against Mhlanga and other journalists, uphold constitutional protections for free expression, and create an enabling environment for independent journalism essential to democratic debate and accountability - Daily Maverick

SURVEILLANCE UPDATES

BINANCE ROLLS OUT A AI-DRIVEN THREAT DETECTION SUITE

IMAGE SOURCE: IT NEWS AFRICA

Binance has launched an AI-driven threat detection suite in response to a surge in AI-powered crypto fraud across Africa, particularly in South Africa, where 60% of organizations have reported increases in AI-facilitated financial crimes. These crimes include deepfake-based "face attacks," where scammers use harvested photos and voice clips to create lifelike video and audio clones that can bypass facial recognition and trick victims into surrendering sensitive information. To combat these threats, Binance's new safeguards feature real-time liveness detection, behavioral biometrics, and transaction anomaly algorithms to distinguish genuine users from AI-generated imposters and detect suspicious activity. Binance's global compliance team, which has handled nearly 60,000 law enforcement requests and trained South African officers, collaborates with local regulators while emphasizing ethical AI development and privacy protection to help secure Africa's growing crypto community against evolving cyber risks - IT News Africa

NDPC URGES AFRICA-WIDE DATA PROTECTION, SIGNS MOU WITH SOMALIA AND LAUNCHES PRIVACY ACADEMY.

IMAGE SOURCE: BIOMETRIC UPDATE

At a major data protection conference in Abuja, Nigeria's government called for Africa-wide collaboration on secure data protection, emphasizing that economic growth and trust in institutions depend on it, especially as the African Continental Free Trade Area expands1. The event saw the launch of the Nigeria Virtual Privacy Academy, Africa's first platform for virtual data protection training, and the announcement of a digital trade desk to support Nigeria's digital exports. Nigeria's Data Protection Commission (NDPC) also signed a memorandum of understanding with Somalia's Data Protection Authority to enhance cross-border cooperation, legal assistance, and enforcement of privacy laws. The NDPC is further partnering with the International Organisation for Migration to strengthen identity management and with Microsoft to provide advanced data protection training, highlighting a continent-wide push for improved data governance, privacy, and digital innovation - Biometric update

ANDROID 16'S NEW 'ADVANCED PROTECTION' MODE IS A LIFELINE FOR AT-RISK JOURNALISTS, POLITICIANS, AND ACTIVISTS

IMAGE SOURCE: TECH-ISH

Android 16 introduces a new "Advanced Protection" mode specifically designed for high-risk users like journalists, activists, and politicians who face targeted digital threats, especially in surveillance-heavy environments such as Kenya. This mode enforces persistent, hardware-backed security measures including mandatory strong authentication (disabling weaker options like basic face unlock), blocking USB data transfers unless explicitly approved, and restricting side-loading of apps to prevent spyware infections. It also features AI-powered theft detection that can instantly lock the device if suspicious behavior is detected, and logs all intrusion attempts in a secure, exportable format. Unlike Apple's Lockdown Mode, Google's approach aims to balance robust protection with everyday usability. Advanced Protection will debut on Pixel devices with Android 16 and expand to other brands, offering a much-needed, system-level defense for those most at risk of digital and physical attacks - Tech-ish

TELEMESSAGE SECURITY SNAFU WORSENS AS 60 GOVERNMENT STAFFERS EXPOSED

IMAGE SOURCE: THE REGISTER

The article highlights several major cybersecurity developments: Secrets from the Trump administration may have been exposed after hackers breached the TeleMessage service used by US officials, with leaked messages appearing online and prompting a White House investigation. Europol and international law enforcement announced the takedown of five major malware groups, resulting in 20 arrests, €21.2 million seized, and 18 suspects added to the EU's most wanted list, demonstrating ongoing efforts to disrupt cybercriminal infrastructure. Security experts proposed a new predictive system to help prioritize patching of vulnerabilities most likely to be exploited, combining existing databases and machine learning. The article also reports on critical vulnerabilities under active attack, including a severe flaw in Samsung MagicINFO 9 Server and another in Ivanti Endpoint Manager Mobile. GoDaddy settled with the US FTC over poor security practices that led to years-long breaches, agreeing to improve security and undergo independent audits. Finally, a researcher discovered an unsecured database containing 184 million unique login credentials from major platforms, likely harvested by infostealer malware, underscoring the persistent risks of data breaches and the need for robust cybersecurity vigilance. - Daily Mail

184M LOGINS LEAKED OF SOCIAL MEDIA, FINANCIAL, GOV ACCOUNTS: INFOSTEALER BREACH HITS GLOBAL USERS

IMAGE SOURCE: WINBUZZER

A massive data breach exposed 184 million unique login credentials–including usernames and passwords for social media, financial, healthcare, and government accounts–after cybersecurity researcher Jeremiah Fowler discovered an unprotected 47GB database likely compiled by infostealer malware. The leaked data, which included plaintext passwords and login URLs for services like Facebook, Instagram, banking portals, and government sites, poses a severe risk of identity theft, account takeovers, and targeted cyberattacks worldwide. Although access to the database was eventually restricted, it remains unclear how long it was exposed or whether malicious actors accessed it, highlighting the persistent threat of credential-stealing malware, the challenges of attribution, and the urgent need for strong cybersecurity practices such as unique passwords and multi-factor authentication - Winbuzzer

ADIDAS IS HIT BY A CYBERATTACK: CUSTOMERS' PERSONAL INFORMATION STOLEN

IMAGE SOURCE: DAILY MAIL

Adidas has confirmed that a cyberattack on a third-party customer service provider resulted in the theft of customer contact information, such as names, email addresses, and phone numbers, primarily affecting individuals who previously contacted Adidas's customer service helpdesk. No passwords, credit card details, or payment information were compromised. Upon discovering the breach, Adidas immediately launched an investigation with cybersecurity experts and began notifying affected customers and authorities. The company has not disclosed how many people were impacted or which regions were affected, but it has warned customers to be vigilant against potential phishing attempts using their stolen contact details. This incident follows a wave of similar cyberattacks targeting major UK retailers, highlighting the growing risks associated with third-party service providers in the retail sector - Daily Mail

INTEL WATCH

Watching the watchers. Guarding the guardians.

INDIA'S ALARM OVER CHINESE SPYING ROCKS THE SURVEILLANCE INDUSTRY

IMAGE SOURCE: REUTERS

India has imposed stringent new security regulations requiring all manufacturers of internet-connected CCTV cameras–including Chinese firms Hikvision, Xiaomi, and Dahua, as well as South Korea's Hanwha and the U.S.'s Motorola Solutions–to submit their hardware, software, and source code for government testing before selling in India. This move is driven by growing concerns over Chinese espionage risks, especially after revelations that around one million cameras in Indian government facilities were sourced from Chinese companies and potentially transmitted sensitive video data abroad. The regulations, effective from April 2025, aim to secure India's rapidly expanding surveillance infrastructure amid fears that Chinese state security laws compel companies to cooperate with intelligence activities. While manufacturers have protested the rules, citing supply chain disruptions and slow approvals, India remains firm, reflecting broader geopolitical tensions and a push to safeguard national security against sophisticated foreign surveillance threats. China has condemned the measures as discriminatory, but India insists on rigorous checks, particularly for devices originating from countries sharing a land border with it - Reuters

RUSSIA'S FANCY BEAR SWIPES A PAW AT LOGISTICS, TRANSPORT ORGS' EMAIL SERVERS

IMAGE SOURCE: THE REGISTER

A coalition of 21 Western governments has issued a warning that Russia's military intelligence unit, known as Fancy Bear (APT28), has been conducting a widespread cyber-espionage campaign since 2022 targeting logistics providers, technology companies, and government organizations involved in supporting Ukraine. The attacks have affected nearly all modes of transportation–air, sea, and rail–and even targeted internet-connected cameras at Ukrainian border crossings to monitor aid shipments. Fancy Bear's tactics include spear-phishing, credential guessing, exploiting vulnerabilities in email services and Microsoft tools, and deploying malware such as the Headlace and Masepie backdoors. Once inside, the hackers conduct reconnaissance to identify key personnel and gather sensitive data like train schedules and shipment manifests. The advisory urges organizations in logistics and tech sectors to heighten their cyber defenses, monitor for known indicators of compromise, and assume they are potential targets of ongoing Russian cyber operations - The Register

APPLE SENDS NEW SPYWARE WARNING, JOURNALISTS AND ACTIVISTS AMONG THOSE TARGETED

IMAGE SOURCE: THE MIRRROR UK

The TSA has issued a major warning to travelers about the security risks of using USB charging ports at airports, cautioning that hackers can install malware on these public ports to compromise devices. The agency advises passengers to avoid charging phones and laptops through airport USB ports and instead use their own chargers plugged into power outlets or carry portable power banks to reduce the risk of cyberattacks. This alert comes amid growing concerns over airport cybersecurity vulnerabilities and aims to protect travelers' personal data and devices during increasingly busy travel periods. - The Mirror UK

GOVERNMENT ISSUES URGENT CYBERSECURITY ALERT FOR CHROME AND FIREFOX USERS

IMAGE SOURCE: ALSADAT MARKETING

The National Computer Emergency Response Team (NCERT) has issued an urgent cybersecurity alert warning users of Mozilla Firefox and Google Chrome about newly discovered zero-day vulnerabilities that are actively being exploited by hackers. These security flaws–CVE-2025-4918 and CVE-2025-4919 in Firefox, and CVE-2025-4664 in Chrome–can allow cybercriminals to run malicious code, steal personal data and passwords, hijack browser sessions, and install malware or spyware on users' devices. The vulnerabilities affect both desktop and mobile versions of the browsers, posing a significant risk to millions. NCERT strongly advises all users to immediately update their browsers to the latest versions, avoid suspicious websites and downloads, and remain vigilant to prevent hacking, identity theft, and data loss. - Alsadat marketing

INTEL WATCH

Watching the watchers. Guarding the guardians.

COCOSPY STALKERWARE APPS GO OFFLINE AFTER DATA BREACH

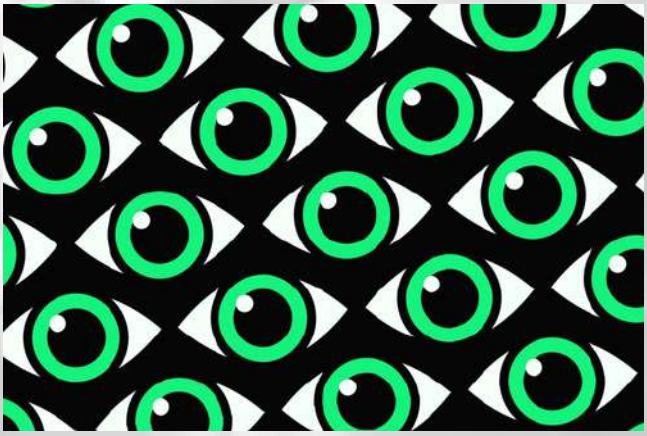

IMAGE SOURCE: TECHCRUNCH

Three widely used stalkerware apps–Cocospy, Spyic, and Spyzie–have gone offline following a major data breach that exposed the personal data of millions of people being secretly monitored, as well as the email addresses of 3.2 million customers who planted the spyware. These apps, which secretly harvested messages, photos, call logs, and real-time locations from victims' phones, were found to share a security flaw that allowed anyone to access the stolen data. After TechCrunch reported on the breach, the apps' websites and Amazon-hosted storage disappeared, and the services stopped working, though it's unclear if this was due to legal fears or reputational damage. The incident highlights a broader trend of consumer-grade spyware operations shutting down after hacks, and serves as a warning about the dangers of stalkerware, which is often disguised as parental control software but is widely misused for illegal surveillance. Victims are urged to check for and remove these apps, which may appear as "System Service" on devices, and seek support if they suspect their privacy has been violated - Techcrunch

LIGHT SENSORS IN SMARTPHONES ALLOW SPYING ON USERS - MIT STUDY

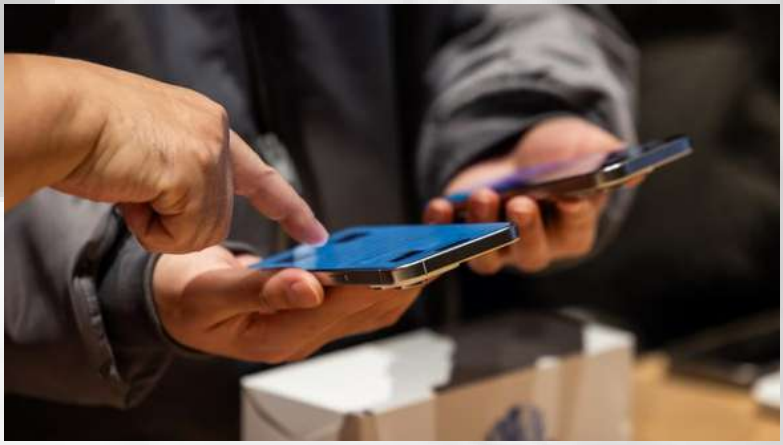

IMAGE SOURCE: DEV UA

A new MIT study reveals that the ambient light sensors (ALS) found in nearly all modern smartphones, tablets, and laptops can be exploited for covert surveillance, even if users disable their microphones, cameras, or use VPNs. Researchers developed an attack method called "LightSpy," which uses data from the ALS to track and reconstruct a user's on-screen actions–such as swipes, clicks, and text entry–by analyzing subtle changes in light detected by the sensor. Unlike cameras or microphones, the ALS cannot be disabled or restricted through system permissions, making it a persistent privacy risk. The attack can be executed via malicious JavaScript in a web browser, allowing hackers to monitor user interactions without their knowledge. The study urges operating system and browser developers to introduce new controls and permissions for ALS access to protect user privacy against this emerging threat. - Dev UA

U.S. SPY AGENCIES ARE GETTING A ONE-STOP SHOP TO BUY YOUR MOST SENSITIVE PERSONAL DATA

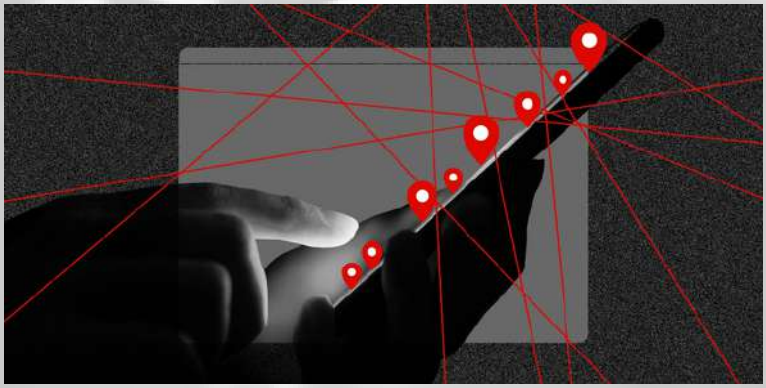

IMAGE SOURCE: THE INTERCEPT

U.S. intelligence agencies are developing an AI-driven centralized data portal called the Intelligence Community Data Consortium (ICDC) to streamline the purchase, linking, and analysis of commercially available personal data (CAI) from data brokers. This portal will allow 18 federal agencies, including the NSA, CIA, and FBI, to access sensitive information–such as location data and social media activity–more quickly and efficiently, bypassing traditional legal restrictions on surveillance of Americans. While the government claims to implement controls to protect privacy, the extensive use of purchased data raises serious concerns about constitutional rights, oversight, and potential misuse, as this data can reveal intimate details of individuals' lives. Critics, including Senator Ron Wyden, argue that current policies fail to safeguard Americans' privacy and call for stronger legislation to regulate both government purchases and private data brokers, highlighting the urgent need for reform in how personal data is collected and used by intelligence agencies. - The Intercept

AUSTRALIA FACES MOUNTING CYBER THREATS TO VITAL INFRASTRUCTURE

IMAGE SOURCE: SECURITY BRIEF AUSTRALIA

Australia is facing a rapidly escalating cyber threat to its critical infrastructure, with foreign state actors–often linked to espionage and sabotage–conducting persistent campaigns to infiltrate and map essential services like power, water, and healthcare. These sophisticated intrusions are designed to establish covert, long-term access, allowing attackers to disrupt vital systems during times of geopolitical tension, often by planting dormant malware that can be activated later for maximum impact. The convergence of operational and information technology, along with legacy systems lacking modern security, has increased vulnerabilities, as shown by a 23% rise in cyberattacks on critical infrastructure. In response, the Australian government has launched a comprehensive Cyber Security Strategy for 2023–2030, emphasizing stronger regulations, intelligence sharing, and mandatory cybersecurity standards for infrastructure operators. Success depends on collaboration between government, industry, and cybersecurity specialists, as well as practical measures like risk assessments and secure-by-design technologies, to ensure the resilience and protection of Australia's essential digital infrastructure. - Security Brief Australia

REPRESSION MONITOR

OPEN GOVERNMENT: EMANCIPATION FOR SOME, EXCLUSION FOR OTHERS

IMAGE SOURCE: THE TAHRIR INSTITUTE

Across the Middle East and North Africa, governments are rapidly adopting digital governance tools like biometric IDs and AI-driven surveillance, often promoting them as ways to boost efficiency and transparency. However, the article argues that without strong legal protections, independent oversight, and inclusive design, these technologies frequently reinforce existing inequalities, enable state surveillance, and marginalize vulnerable groups such as refugees, the displaced, and those lacking digital access. Case studies from Lebanon and Tunisia illustrate how outdated data protection laws, underfunded regulatory bodies, and rushed tech rollouts can expose citizens' sensitive information to breaches, erode public trust, and even incite violence. International donor-driven technology transfers, while well-intentioned, often fail to adapt to local contexts or ensure robust safeguards, as seen in the mass data leak of Syrian refugees in Turkey. The article calls for a rights-based approach to digital governance–prioritizing privacy, transparency, and accountability–through independent oversight, modernized legal frameworks, and meaningful engagement with affected communities, warning that without these reforms, digital tools risk becoming instruments of exclusion and repression rather than empowerment and equitable development - The Tahrir Institute

TRUMP'S IMMIGRATION CRACKDOWN IS BUILT ON AI SURVEILLANCE AND DISREGARD FOR DUE PROCESS

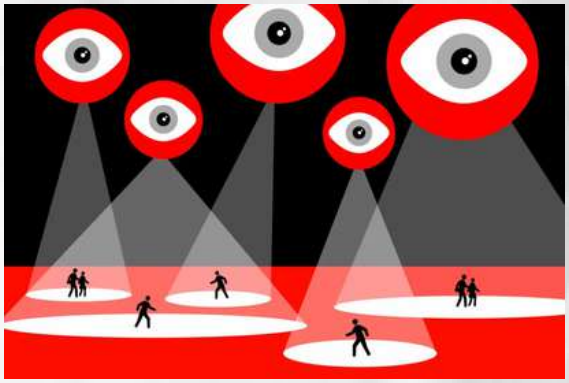

IMAGE SOURCE: BULLETIN OF THE ATOMIC SCIENTISTS

Donald Trump's latest immigration crackdown is being driven by the widespread use of AI-powered surveillance technologies, including facial recognition, predictive analytics, and expansive data-sharing between government agencies and private companies, to monitor and target undocumented immigrants. The article highlights how these high-tech tools are being deployed with little regard for due process, resulting in increased deportations and the erosion of civil liberties for immigrant communities, who often face surveillance and enforcement actions without fair hearings or legal recourse. Critics warn that this approach not only disproportionately harms minorities and vulnerable populations but also sets a dangerous precedent for the broader use of AI surveillance in law enforcement, raising serious concerns about privacy, accountability, and the undermining of constitutional protections in the U.S. immigration system. - Bulletin of the Atomic Scientists

FEARS EXPLODE OVER NEW TSA FACE SCAN TECH AS PRIVACY WATCHDOGS SOUND ALARM OVER 'SURVEILLANCE'

IMAGE SOURCE: IRISH STAR

The TSA has implemented facial recognition technology at select U.S. airports to enhance security by verifying that travelers are the same individuals shown on their identification documents, improving both safety and operational efficiency while maintaining privacy protections. Participation is voluntary, with travelers able to opt out without delay or penalty, and photos are not stored after verification except in limited testing scenarios. The technology uses advanced algorithms with high accuracy rates–better than 99% in matching faces to IDs under controlled conditions–and is designed solely for identity verification at checkpoints, not for surveillance or law enforcement purposes. The TSA also employs Credential Authentication Technology (CAT-2) scanners to verify IDs and flight status, including digital IDs, across many airports. While the system has received positive assessments for effectiveness and civil liberties safeguards, experts suggest TSA could enhance transparency and consider integrating watchlist data to further improve security. Overall, the TSA emphasizes traveler privacy, respect, and the use of cutting-edge technology to protect the transportation system without compromising civil rights. - Irish Star

NEW ORLEANS POLICE SECRETLY USED PROHIBITED FACIAL RECOGNITION SURVEILLANCE FOR YEARS

IMAGE SOURCE: REASON

The New Orleans Police Department (NOPD) secretly used real-time, AI-driven facial recognition alerts from a network of 200 cameras across the city for two years, despite a city ordinance prohibiting generalized public surveillance through such technology. This system automatically notified officers of possible matches to wanted suspects, raising serious concerns about privacy, civil liberties, and the potential for wrongful arrests due to software errors. Although the ordinance passed in 2022 allowed some surveillance tools for criminal investigations, it specifically banned the use of broad facial surveillance systems, limiting data collection to narrowly defined purposes. After the practice was exposed, NOPD's superintendent paused the automatic alerts in April 2025 pending legal review, though facial recognition technology and camera footage are still being used for investigations, including tracking escaped inmates. The case highlights ongoing debates over the balance between public safety and privacy rights, as well as the lack of clear accountability and oversight in the deployment of advanced AI surveillance tools by law enforcement - Reason

PROJECT NOLA'S FACIAL RECOGNITION PUSH RAISES LEGAL AND CIVIL RIGHTS QUESTIONS

IMAGE SOURCE: BIOMETRIC UPDATE

Project NOLA, a New Orleans-based nonprofit managing a vast network of privately owned surveillance cameras, has sparked intense debate by integrating real-time facial recognition into its system and sharing alerts with law enforcement, despite limited public oversight and unclear legal authority. Originally intended to help neighborhoods monitor crime, Project NOLA's network has expanded into a decentralized, AI-powered surveillance web, with thousands of cameras feeding footage to a central hub and facilitating dozens of arrests. Critics, including civil rights groups and city officials, warn that the program operates in a regulatory gray area–outside direct municipal control and without the procedural safeguards, transparency, or audit requirements mandated for public-sector facial recognition. Concerns include potential violations of New Orleans' surveillance ordinance, risks of racial profiling, algorithmic bias, and warrantless, proactive surveillance. The controversy has led the city council to consider new regulations and prompted the NOPD to pause its use of Project NOLA's facial recognition pending legal review, while calls grow for independent audits and federal investigations into the project's compliance and impact on civil liberties - Biometric Update

TSA SAYS NEW CONTROVERSIAL TECHNOLOGY IS 'KEY' FOR AIRPORT SECURITY. CAN YOU OPT OUT?

IMAGE SOURCE: NJ

The TSA has deployed facial recognition technology at 84 airports nationwide, with plans to expand to 400 airports, aiming to enhance security by verifying travelers' identities more accurately and efficiently through real-time photo matching against their IDs. Participation is voluntary–travelers can opt out by informing a TSA agent and undergo traditional ID checks without delays or penalties. The TSA states that images captured during the process are typically deleted immediately after identity verification, except in rare cases for system accuracy assessments, with passengers notified if data is retained. Despite these assurances, privacy advocates raise concerns about potential data retention, misuse, and the security of biometric information, especially given the lack of transparency and risks of misidentification. The TSA emphasizes that opting out will not affect travel or cause delays, and the technology is intended solely to improve security and streamline screening, not for surveillance purposes - NJ

BURMA JUNTA ADOPTS CHINA'S DIGITAL BLUEPRINT FOR REPRESSION

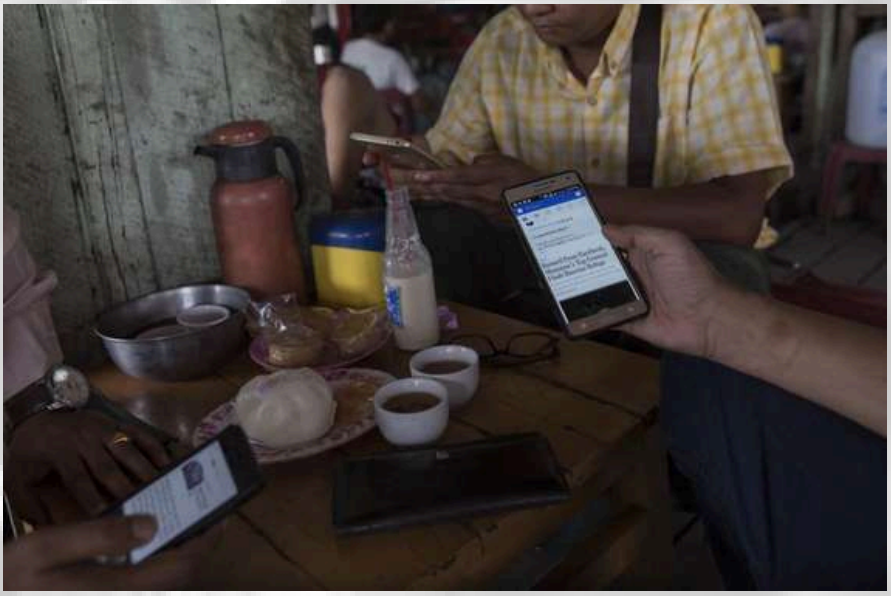

IMAGE SOURCE: MIZZIMA NEWS

Burma's military junta has established one of the world's most oppressive digital control systems, heavily influenced and enabled by Chinese surveillance technology and biometric infrastructure. Following the 2021 coup, the regime expanded surveillance across telecom networks using Chinese-modeled systems to eavesdrop on communications, track locations, and monitor citizens in real time, facilitating arrests and repression. High-level cooperation with China has included training on biometric enrollment and the rollout of a nationwide Unique Identification (UID) system that collects extensive personal and biometric data, linking it to essential services and enabling the junta to control access and punish dissenters. This system mirrors China's digital authoritarianism, including the social credit model used to monitor and restrict citizens' freedoms. Alongside biometric surveillance, the junta has imposed frequent internet shutdowns–over 329 in four years–especially in conflict zones, severely restricting communication and resistance efforts. International calls for sanctions on military-linked telecoms and an end to technology transfers aim to curb this digital repression, but as long as China continues exporting these tools, Burma's digital authoritarianism and suppression of opposition are likely to intensify - Mizzima News

INTELLIGENCE AGENCIES

GOOGLE EXPANDS ADVANCED PROTECTION IN ANDROID 16 TO TACKLE SPYWARE THREATS

IMAGE SOURCE: TECHWEEZ

Google has significantly upgraded its Advanced Protection feature in Android 16 to address the growing threat of spyware and sophisticated surveillance attacks, particularly those exploiting zero-day vulnerabilities. Announced on May 13, the enhanced security mode is tailored for high-risk users and anyone vulnerable to targeted cyberattacks, introducing robust safeguards such as blocking zero-click exploits, disabling 2G networks, restricting USB data connections, and preventing unauthorized app installations. Key innovations include a forthcoming intrusion logging feature for secure forensic analysis, hardware-based Memory Tagging Extension (MTE) to thwart memory corruption attacks, and tamper-resistant settings that require user authentication to modify. Advanced Protection also limits sensitive permissions during calls and ensures consistent security across Google and third-party apps. These measures, many of which are available immediately with more rolling out later in 2025, represent Google's most comprehensive mobile security response yet to the escalating risks posed by commercial spyware and advanced cyber threats - Techweez

UK FRAUD BILL TARGETS BENEFIT CLAIMANTS FOR MASS SURVEILLANCE

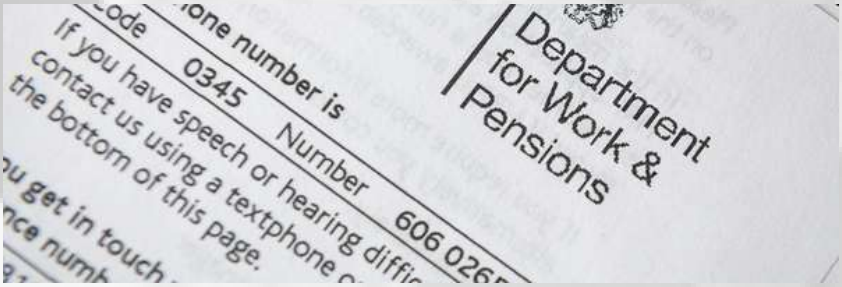

IMAGE SOURCE: COMPUTER WEEKLY

The UK's proposed Public Authorities (Fraud, Error and Recovery) Bill aims to combat benefit fraud and error but has sparked major concerns over privacy and human rights due to its sweeping surveillance powers. The Bill would allow the Department for Work and Pensions (DWP) to routinely and covertly monitor the bank accounts of millions of benefit claimants, enter private homes, and seize assets, all without requiring reasonable suspicion of wrongdoing. Critics warn that this mass surveillance approach treats all claimants as potential fraudsters, undermines the presumption of innocence, and risks significant harm to vulnerable individuals, especially as overpayments often result from DWP's own errors. The Bill's lack of robust safeguards, transparency, and human oversight–especially with the rise of automated decision-making–raises fears of wrongful investigations, financial hardship, and the normalization of invasive state surveillance. The finance industry and rights groups argue that the measures are disproportionate, likely ineffective against organized fraud, and set a dangerous precedent for broader government surveillance of the population. - Computer Weekly

OPEN GOVERNMENT: EMANCIPATION FOR SOME, EXCLUSION FOR OTHERS

IMAGE SOURCE: THE TAHRIR INSTITUTE

Across the Middle East and North Africa, governments are rapidly adopting digital governance tools–such as biometric IDs, AI surveillance, and data-driven migration policies–often under the banner of efficiency and transparency, but with insufficient legal safeguards and oversight, these technologies frequently reinforce existing inequalities, enable state surveillance, and exclude marginalized groups like refugees and the digitally underserved. Case studies from Lebanon and Tunisia reveal how outdated data protection laws, under-resourced regulatory bodies, and rushed tech rollouts expose citizens' sensitive data to breaches and erode public trust, while international donor-driven technology transfers can worsen vulnerabilities if not adapted to local contexts or accompanied by robust safeguards. High-profile incidents, like the mass data leak of Syrian refugees in Turkey, illustrate the dangers of poorly protected humanitarian data. The article calls for a rights-based approach to digital governance, emphasizing independent oversight, modern legal frameworks, community engagement, and privacy-by-design principles to ensure that digital tools empower rather than repress, warning that without such reforms, digital technologies risk becoming instruments of exclusion, surveillance, and elite control - The Tahrir Institute

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

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

Global Dialogue

Funded by the European Union

We are grateful for the support of our donors!