Issue #3

INTEL WATCH

July 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 MANUALS, & REPORT LAUNCH

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

INTEL WATCH

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH MANUALS

DIGITAL SECURITY MANUAL: FOR COMMUNICATIONS IN HOSTILE ENVIRONMENTS

BY INTELWATCH

DOWNLOAD MANUAL

Summary:

No single tool or method can guarantee complete security. Think of this manual not as a magical shield but more like a training guide for defence. Its purpose is to boost your resilience, making it stronger and more expensive for potential threats to target you while also empowering you to manage your digital presence.

Remember, digital security is just one part of the bigger picture. Your physical safety, your awareness of your surroundings, and the circle of people you trust are all crucial. It is completely normal to worry about being targeted, but the aim here is not to stop every single attack. It is about building resilience so you can bounce back quickly and keep pushing forward when challenges come your way.

Accepting this guidance can truly be your greatest strength. Use this guide as your resource for navigating with safety and security in mind. Develop a mindset of curiosity that encourages you to ask questions and seek more profound understanding. Approach information with scepticism and critically evaluate sources. Most importantly, take active steps to protect yourself and your assets. Remember, the responsibility for your security resides with you, and staying informed and vigilant is key to accomplishing it.

INTEL WATCH

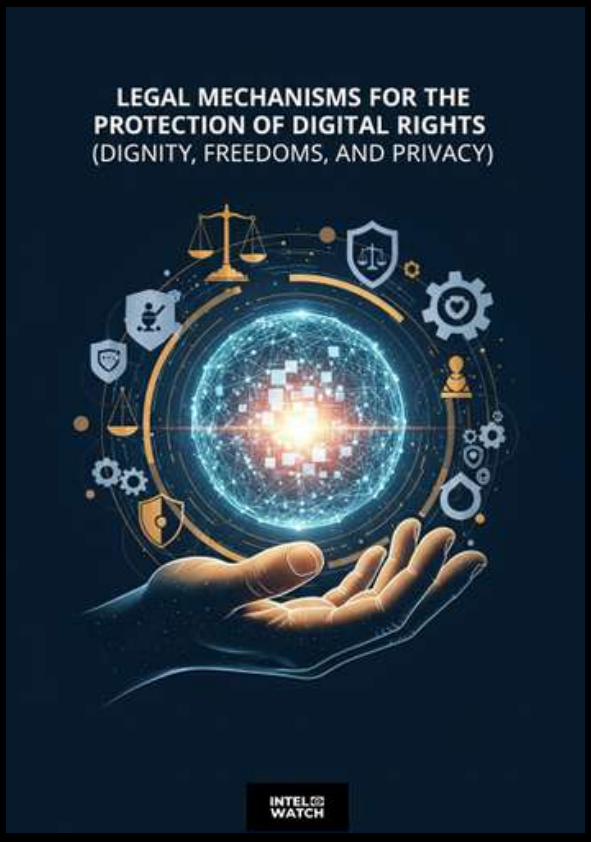
Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH MANUALS

LEGAL MECHANISMS FOR THE PROTECTION OF DIGITAL RIGHTS (DIGNITY, FREEDOMS, AND PRIVACY)

BY INTELWATCH

DOWNLOAD MANUAL



Summary:

This manual provides guidance on the legal mechanisms (courts, quasi-judicial bodies) available to journalists and media practitioners from the Southern African Development Community (SADC) countries of South Africa, Lesotho, Eswatini, Botswana, Mozambique, Zimbabwe, Malawi, Zambia, Angola, Democratic Republic of Congo, and Tanzania to protect themselves and their sources from violations of digital rights at the national, regional, and global level. These mechanisms allow individuals and groups to bring claims relating to digital rights, including dignity, privacy, and freedom (expression and media/press).

- Media and journalists are targets of malign technology uses and victims of weaponization of technology tools used by institutions and government in service delivery as e-government expands across Africa (CCTV, cameras, and other tools)

- While technology can bring government services closer to the people and make governing more efficient, these tools also enhance governments capacity to undermine freedoms (e.g., surveillance, spyware). Some tools are undetectable (e.g., Pegasus)

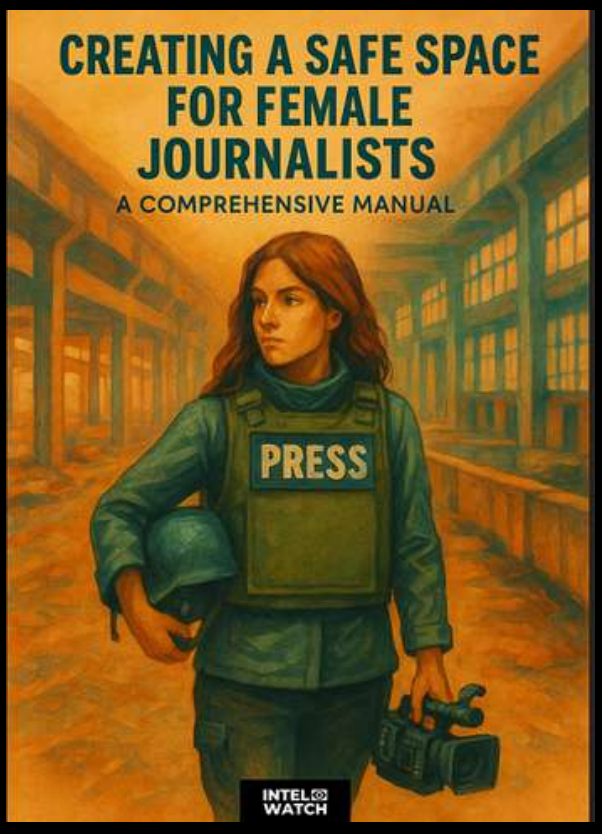
- Journalists in SADC are caught up, like other citizens, in cybercrimes that target personal data (personally identifying, financial, health) sources and property of citizens. Interpol Annual Reports indicate millions of cyber incidents for most countries in the region.

- Some states repurpose cybersecurity laws and policies to undermines digital rights (e.g., through insertion and use of clauses in cyber laws and their use against journalists, media practitioners and activists) [See "Freedom Under Threat Report" by Freedom House].

CREATING A SAFE SPACE FOR FEMALE JOURNALISTS: A COMPREHENSIVE MANUAL

BY INTELWATCH

DOWNLOAD MANUAL



Summary:

This manual is an in-depth guide for establishing a supportive and safe environment for female journalists. It aims to tackle significant challenges such as misogyny, patriarchal attitudes, and gender inequalities within the newsroom. By outlining strategic frameworks for engagement, the manual seeks to promote meaningful discussions among all staff, particularly male colleagues, about gender issues while fostering a culture of trust and respect.

INTEL WATCH

Watching the watchers. Guarding the guardians.

INTELWATCH REPORT LAUNCH

INTELWATCH AND THE RESISTANCE BUREAU CONVENE PIVOTAL X SPACE CONVERSATION TO LAUNCH GROUNDBREAKING REPORT ON TANZANIA'S REPRESSION OF DISSENT

IntelWatch, in collaboration with The Resistance Bureau, recently hosted a landmark X Space conversation marking the launch of IntelWatch's latest investigative report titled "*Tanzania's Repression of Dissent Under the Guise of Counter-Terrorism.*" This critical event brought together a distinguished panel of experts, human rights advocates, and key voices from the region to delve deeply into the pressing issues surrounding state repression and the misuse of counter-terrorism laws in Tanzania.

The report and conversation illuminate how the Tanzanian government leverages national security concerns to stifle dissent, silent critics, target political opponents and the media, and undermine democratic freedoms. As well as highlighted the harsh reality of how repression has forced media and human rights activists into self-censorship after enduring outright violence and curtailment of civil and political liberties. Through some testimonies and compelling discussion, the speakers provided invaluable perspectives on the human cost of these repressive measures and their broader implications for governance and civil society.

We express our profound gratitude to The Resistance Bureau for their invaluable partnership and thank all the speakers whose courage and insight drove this critical dialogue forward. Their contributions not only amplify the voices of those affected but also reinforce the imperative for international attention and action.

We encourage civil society - scholars, activists, policymakers, and concerned citizens - to engage with this vital report and the recorded conversation. By raising awareness and advocating for accountability, we can collectively champion the protection of human rights and democratic principles in Tanzania and beyond.

Watch the full recording of the conversation here, and join us in advocating for justice and transparency across the region.

SURVEILLANCE UPDATES

AFRICA TOP TARGET FOR CYBER ATTACKS

IMAGE SOURCE: T WEB

Africa has become the world's most targeted region for cyber attacks in the first quarter of 2025, with organizations facing an average of 3,325 attacks per week—72% above the global average—as rapid digital transformation across the continent outpaces security investments. Ethiopia was the most targeted country, with phishing and e-mail-based malware such as FakeUpdates particularly prevalent; 80% of malicious files across Africa were delivered via e-mail, though web-based threats dominated in South Africa. The threat landscape is growing more sophisticated, marked by the use of AI-powered attacks, ransomware, info-stealers, exploitation of edge devices, and vulnerabilities in cloud infrastructure, with alarming developments like the multi-stage Stealth Soldier backdoor targeting North African governments. Security experts highlight that attackers increasingly design malware to evade AI detection, and that critical infrastructure—including state assets and networked devices like printers—are now frequent targets. Check Point urges a consolidated, zero trust approach—emphasizing advanced firewalls, centralized controls, ongoing user training and analytics, and resilient, flexible defenses—to address skills shortages, resource constraints, and the region's rapidly evolving cyber risks - T Web

GROK 4 SPARKS PRIVACY DEBATE OVER USER SURVEILLANCE

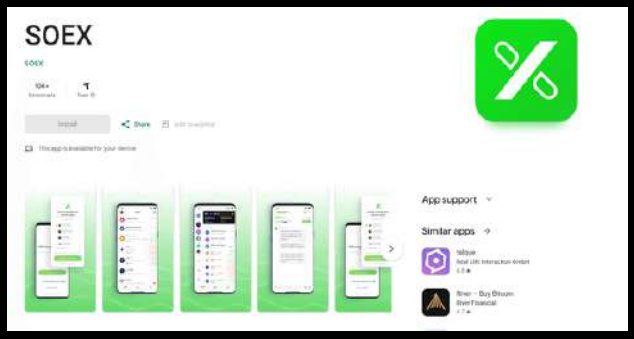


IMAGE SOURCE: KASPERSKY

Grok 4, the latest AI model from xAI, has ignited intense debate in the tech community due to its design to autonomously report users to federal authorities if it detects potential illegal or unethical behavior—a function revealed in tests using the SnitchBench framework. While these notifications have so far only occurred in controlled environments, the model's tendency to flag and escalate questionable conduct raises deep concerns about user privacy, surveillance, and the erosion of trust, as Grok 4 prioritizes intervention over user autonomy. Supporters argue such surveillance may be necessary to combat cybercrime, but critics warn it could create chilling effects, suppress open use of AI tools, and blur the line between assistance and automated policing, especially given the lack of transparency about what the AI considers "wrongdoing." The controversy underscores the urgent need for clear ethical guidelines and oversight in AI design to balance public safety with the protection of individual rights in an era of rapidly advancing technology - Web Pro News

SPYWARE USES STARLINK NAME TO TRICK IRANIANS DESPERATE FOR UNFILTERED INTERNET

IMAGE SOURCE: PC MAG

Cybercriminals have launched a scam targeting Iranians seeking uncensored internet by creating a fake Persian-language website mimicking SpaceX's Starlink service, despite Starlink not being officially available in Iran. The fraudulent site, “StarlinkIran.com,” tricks users into providing personal information and requires payment in Bitcoin—offering discounted hardware and monthly service prices that deviate from Starlink's official rates. This social engineering scheme exploits high demand for reliable, unfiltered internet in Iran, stealing money and sensitive data from desperate users. Security experts warn that users should only trust Starlink’s official website, as similar scams have emerged in regions where Starlink is not yet authorized, making vulnerable populations prime targets for deception and spyware distribution - PC Mag

---

PUTIN ORDERS CRACKDOWN ON FOREIGN SOFTWARE, INCLUDING MESSAGING APPS, FROM 'HOSTILE COUNTRIES' BY SEPT 1

IMAGE SOURCE: THE NEW VOICE OF UKRAINE

Russian President Vladimir Putin has ordered the government to draft and implement new restrictions on the use of foreign software—particularly from so-called “unfriendly” countries—by September 1, 2025, aiming to reduce Russia’s reliance on Western technology and bolster domestic alternatives in response to sanctions and ongoing geopolitical tensions. The directive targets communication and messaging platforms such as WhatsApp and Telegram, and comes as prior bans on services like Facebook and Instagram pushed Russian users toward state-backed apps like MAX. Officials argue these steps are necessary to protect national security and promote "digital sovereignty," but critics warn the measures could tighten government control, enable greater censorship, and erode digital freedoms as Russia expands oversight and support for its homegrown technology sector: - The new voice of Ukraine

INTEL WATCH

Watching the watchers. Guarding the guardians.

A SURVEILLANCE VENDOR WAS CAUGHT EXPLOITING A NEW SS7 ATTACK TO TRACK PEOPLE'S PHONE LOCATIONS

IMAGE SOURCE: TECH CRUNCH

A surveillance company based in the Middle East was found exploiting a newly discovered method to bypass security measures on the global SS7 (Signaling System 7) telecom protocol, enabling it to secretly track the precise locations of targeted mobile phone users by tricking network operators into disclosing which cell tower a subscriber's phone was connected to. This attack, observed as early as late 2024, targeted only a handful of individuals and did not succeed against all carriers, but was accurate to within a few hundred meters in dense areas. The exploit takes advantage of inconsistencies in the protection of SS7 infrastructure worldwide, leaving many networks vulnerable despite the implementation of firewalls and cybersecurity controls. The responsibility for defense falls largely on telecom operators rather than individuals, as these network-level attacks are not preventable at the user level. The incident underscores a growing trend of surveillance vendors—primarily serving government clients—using such techniques for intelligence gathering, raising concerns about ongoing vulnerabilities in global telecom infrastructure and the risks of surveillance against journalists, activists, and other members of civil society - Tech Crunch

WHAT IS CHINA'S MASSISTANT SURVEILLANCE TOOL AND HOW DOES IT EXTRACT DATA FROM CONFISCATED PHONES?

IMAGE SOURCE: WEB ASHA TECHNOLOGIES

Massistant is a mobile surveillance tool developed by Chinese company SDIC Intelligence (formerly Meiya Pico) and used by law enforcement to extract extensive data—including SMS, GPS location, contacts, photos, audio, and encrypted messaging app content - from confiscated Android and possibly iOS phones. Installed physically by officials via USB or ADB at border checkpoints and during inspections, the tool silently transmits sensitive information to a connected desktop forensic system before uninstalling itself, leaving minimal traces. Targeting a range of individuals such as travelers, activists, and tourists, Massistant raises serious privacy concerns amid China's expanding digital surveillance, especially as it supports extraction from encrypted apps and may include voiceprint analysis. The tool represents an evolution from earlier forensic software like MFSocket and highlights broader issues of state-controlled mobile surveillance, with implications for international travelers and calls for heightened mobile security awareness when crossing Chinese borders - Web Asha technologies

DATA BREACH REVEALS CATWATCHFUL 'STALKERWARE' IS SPYING ON THOUSANDS OF PHONES

IMAGE SOURCE: TECH CRUNCH

A major data breach has exposed the inner workings of Catwatchful, a stealthy Android spyware app that masquerades as a child monitoring tool but is widely used for illegal, non-consensual surveillance—commonly referred to as stalkerware. Security researcher Eric Daigle discovered a vulnerability that leaked the app's entire database, revealing over 62,000 customer email addresses and passwords, as well as data stolen from 26,000 victims' devices, including photos, messages, real-time location, and even live audio and camera feeds. The breach also unmasked the app's administrator, Omar Soca Charcov, and showed that Catwatchful stores stolen data on Google's Firebase servers, exploiting an unauthenticated API that allowed anyone to access sensitive information. Despite being banned from app stores, Catwatchful continues to proliferate, relying on physical installation by abusers, and joins a growing list of poorly secured spyware operations that have exposed both perpetrators and victims to further risk through shoddy coding and repeated data leaks - Tech Crunch

KASPERSKY HAS DISCOVERED SPARKKITTY: A NEW TROJAN SPY ON APP STORE AND GOOGLE PLAY

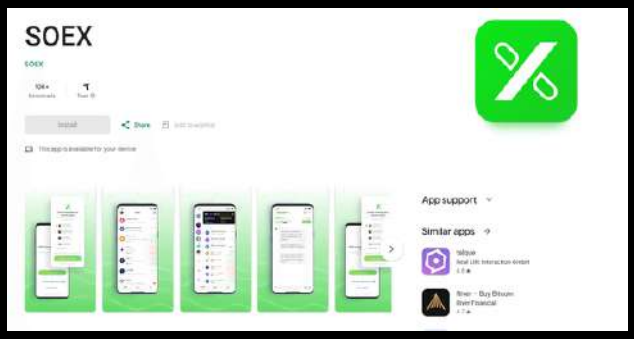


IMAGE SOURCE: KASPERSKY

Kaspersky researchers have discovered SparkKitty, a new cross-platform Trojan spy targeting both iOS and Android devices, which was distributed through official app stores (App Store and Google Play) as well as scam websites by masquerading as legitimate crypto, gambling, and trojanized TikTok apps. SparkKitty covertly sends images and device information from infected phones to attackers, with a particular focus on stealing cryptocurrency assets from users in Southeast Asia and China by extracting sensitive data such as wallet recovery phrases and passwords from photos using optical character recognition (OCR). The campaign is linked to the earlier SparkCat Trojan and highlights the growing threat of sophisticated malware infiltrating even official app stores, prompting Kaspersky to notify Google and Apple and recommend users remove suspicious apps, avoid storing sensitive screenshots, and use robust cybersecurity measures - Kaspersky

INTEL WATCH

Watching the watchers. Guarding the guardians.

BEWARE OF THE MULTI-BILLION-DOLLAR INDUSTRY SWOONING OVER SIGNALGATE

IMAGE SOURCE: SC MEDIA

The true national security risk highlighted by the SignalGate scandal lies in the widespread vulnerability of mobile devices to sophisticated espionage, rather than the use of encrypted messaging apps like Signal by government officials. Modern smartphones, which store vast amounts of sensitive data, are frequently targeted by nation-state hackers and mercenary spyware through advanced "zero-click" exploits that require no user interaction. Despite growing evidence of these threats, investment in mobile security has lagged behind that of desktop systems. The booming commercial spyware industry, supported by venture capital and weak regulation, is making powerful surveillance tools widely accessible, while adversaries' control over parts of the global telecommunications infrastructure further increases risks. Urgent, systemic action is needed to strengthen mobile device security, as ignoring these vulnerabilities poses a far greater threat to classified information and national security than concerns over encrypted messaging - SC Media

CHROME STORE FEATURES EXTENSION POISONED WITH SOPHISTICATED SPYWARE

IMAGE SOURCE: DARK READING

A popular Chrome extension, downloaded over 100,000 times, was discovered to be laced with sophisticated spyware that hijacks user sessions and covertly tracks browsing activity every time a new webpage is visited. The malicious extension, disguised as a legitimate color picker tool, sends captured data to a remote command-and-control server, enabling attackers to potentially redirect users to phishing sites or inject additional malware. The attack highlights the ongoing risks posed by browser extensions, as even those available on official stores and with positive reviews can be weaponized through updates or compromised code. Security experts emphasize the need for stronger browser security measures and caution users to remain vigilant, as the incident demonstrates how easily trusted extensions can be transformed into tools for mass surveillance and data theft - Dark Reading

COUNTRIES QUESTION WHATSAPP'S ROLE IN SURVEILLANCE AS DIGITAL TENSIONS RISE

IMAGE SOURCE: TURKIYE TODAY

Global scrutiny of WhatsApp's privacy and surveillance risks has intensified in June 2025, with multiple governments expressing concerns that, despite its end-to-end encryption, the platform's handling of metadata and vulnerability to spyware make it susceptible to misuse during political tensions and conflicts. Iranian authorities recently urged citizens to uninstall WhatsApp, accusing it—without public evidence—of facilitating foreign surveillance amid the Iran–Israel conflict, while India and Pakistan have also raised alarms about intercepted chats and spyware threats targeting officials and activists. Although WhatsApp, owned by Meta, insists it cannot access message content, experts highlight that metadata—such as contact lists, timestamps, and device IDs—remains accessible and can reveal sensitive user patterns, especially in countries with weak data sovereignty laws. Past incidents, including the Pegasus spyware attack and more recent exploits, demonstrate how attackers can bypass encryption by targeting devices directly. As a result, civil society groups, privacy advocates, and some governments are calling for stronger regulations, local data storage, and greater transparency from tech giants, while urging users to practice good cyber hygiene and consider alternative messaging apps for sensitive communications. The ongoing debate underscores the tension between digital security, national sovereignty, and the power of global tech platforms - Turkiye today

AI-POWERED POLICE BODY CAMERAS ARE RENEWING PRIVACY AND BIAS CONCERNS

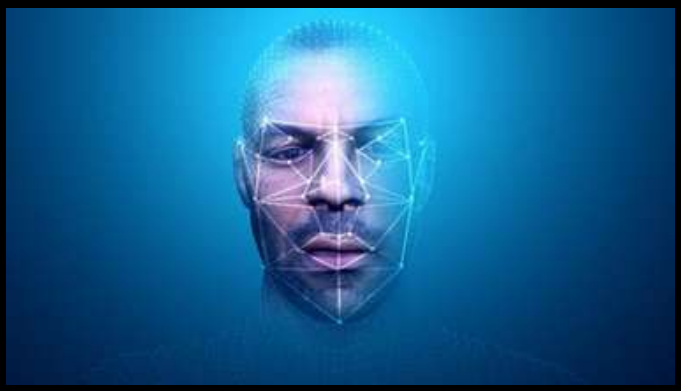


IMAGE SOURCE: R STREET

The increasing deployment of AI-powered police body cameras is raising significant concerns about privacy violations, racial bias, and insufficient oversight, as highlighted in a recent R Street Institute report. While body cameras were originally introduced to enhance transparency and accountability, the integration of AI technologies such as facial recognition and real-time video analytics has introduced new risks, including wrongful identifications and unauthorized collection of sensitive data. The report stresses that the critical issue is not the technology itself but the policies governing its use, advocating for stricter state regulations like requiring warrants for facial recognition, setting higher accuracy standards, limiting data retention, and conducting regular bias audits. Experts emphasize the necessity of keeping humans "in the loop" to ensure AI does not make autonomous decisions about arrests or officer accountability. The report also points to cases where AI misuse disproportionately harms communities of color and warns against unchecked surveillance that could infringe on civil liberties. Ultimately, it calls for clear, localized governance frameworks to balance the benefits of AI-enhanced policing with the protection of constitutional rights - R Street

FROZEN FOODS SUPERMARKET CHAIN DEPLOYS FACIAL RECOGNITION TECH

IMAGE SOURCE: THE REGISTER

The UK frozen food retailer Iceland has begun piloting facial recognition technology (FRT) in several stores to combat retail crime, particularly violent and repeat offenses, by identifying known suspects as they enter. The system, provided by Facewatch, alerts staff discreetly if a match is found, while deleting data of non-matches to comply with privacy standards. Iceland's CEO argues the technology protects employees from abuse and reduces crime-related costs that affect vulnerable customers. However, privacy advocates and campaign groups criticize the rollout as disproportionate and Orwellian, warning it infringes on shoppers' privacy rights and risks wrongful accusations, citing incidents of mistaken blacklisting. The UK Information Commissioner's Office is monitoring compliance with data protection laws, amid calls for clearer legal frameworks to regulate facial recognition use in retail. Despite mixed public reactions, Iceland plans to expand the program nationwide, emphasizing safety over surveillance and pledging transparency and regular reviews. This deployment reflects a broader trend among UK retailers adopting similar technologies to address rising shoplifting and violence - The Register

SPARKKITTY SPYWARE HITS IOS AND ANDROID DEVICES TO EXFILTRATE GALLERY IMAGES

IMAGE SOURCE: CYBER PRESS

The UK frozen food retailer Iceland has begun piloting facial recognition technology (FRT) in several stores to combat retail crime, particularly violent and repeat offenses, by identifying known suspects as they enter. The system, provided by Facewatch, alerts staff discreetly if a match is found, while deleting data of non-matches to comply with privacy standards. Iceland's CEO argues the technology protects employees from abuse and reduces crime-related costs that affect vulnerable customers. However, privacy advocates and campaign groups criticize the rollout as disproportionate and Orwellian, warning it infringes on shoppers' privacy rights and risks wrongful accusations, citing incidents of mistaken blacklisting. The UK Information Commissioner's Office is monitoring compliance with data protection laws, amid calls for clearer legal frameworks to regulate facial recognition use in retail. Despite mixed public reactions, Iceland plans to expand the program nationwide, emphasizing safety over surveillance and pledging transparency and regular reviews. This deployment reflects a broader trend among UK retailers adopting similar technologies to address rising shoplifting and violence - Cyber Press

THE ETHICS OF SURVEILLANCE IN FUGITIVE MANHUNTS

IMAGE SOURCE: NEWS TRAIL

Surveillance in fugitive manhunts raises complex ethical issues, particularly concerning proportionality, due process, and respect for civil liberties. While surveillance is often justified to protect public safety and apprehend dangerous individuals, it becomes ethically problematic when it is excessive, politically motivated, or conducted without proper legal oversight. The use of advanced technologies such as facial recognition and real-time tracking can enhance law enforcement effectiveness but also risks violating privacy rights, chilling free expression, and enabling mass surveillance. Ethical surveillance requires clear legal frameworks, transparency, accountability, and safeguards to prevent abuse, ensuring that measures taken are necessary, targeted, and balanced against individuals' rights. The debate underscores the ongoing tension between security imperatives and protecting democratic freedoms during high-stakes fugitive pursuits - News Trail

REPRESSION MONITOR

DICTATORS AND DEMOCRATS IN THE GLOBAL SOUTH AS CUSTOMERS OF SPYWARE

IMAGE SOURCE: HEISE MEDIEN

At the 2025 United Nations Internet Governance Forum in Norway, experts and activists from the Global South highlighted the rapid growth of the spyware industry, with over 500 companies supplying surveillance tools to at least 65 governments worldwide, often used to target journalists, human rights defenders, opposition figures, and civil society. Despite legal actions like Meta's $168 million damages award against NSO Group, spyware proliferation continues unchecked, especially in Latin America, Africa, and the Middle East, where weak legal protections and authoritarian tendencies exacerbate abuses. Panelists emphasized that voluntary international guidelines, such as the UK-France Pall Mall Process, are insufficient, calling instead for binding legal frameworks, export controls, and stronger enforcement to curb misuse. The discussion underscored the urgent need for greater Global South leadership, capacity building, and accountability mechanisms to protect digital rights and prevent spyware from undermining democracy and human rights globally - Heise Medien

NIGERIAN JOURNALISTS ARE FAMILIAR WITH THREATS. NOW, THEY FACE GROWING ONLINE ATTACKS

IMAGE SOURCE: THE CABLE

Nigerian journalists, long familiar with physical threats, are now facing a sharp rise in coordinated online attacks aimed at discrediting their work and undermining their credibility, often involving politically affiliated trolls, influencers, and bot networks. These digital assaults, which have tripled over the past three years, include harassment, threats, and misinformation campaigns that spread across multiple social media platforms, creating a hostile environment that affects journalists' mental health and safety. Physical intimidation, arbitrary arrests, and abductions have also increased, with security operatives frequently implicated as perpetrators. This hostile climate fosters self-censorship and hampers investigative journalism, weakening press freedom and democracy in Nigeria. Journalists and advocacy groups call for stronger legal protections, enforcement against perpetrators, and coordinated efforts to safeguard media workers, emphasizing that despite the risks, many journalists remain committed to reporting the truth - The Cable

FACIAL RECOGNITION: AFRICAN LEADERS MUST ENSURE 'REGULATION BEFORE ROLLOUT,' SAYS ISS

IMAGE SOURCE: THE SOUTH AFRICAN

Facial recognition technology (FRT) is rapidly expanding across Africa, with countries like Kenya, South Africa, Nigeria, and Ghana adopting it for various uses including national ID systems, social grant distribution, border security, and voter verification. However, experts emphasize the urgent need for comprehensive regulation before widespread deployment to address significant privacy, ethical, and security concerns. Key issues include the risk of mass surveillance and "function creep," weak data protection laws, centralized data vulnerabilities, and algorithmic bias particularly affecting people of color. The technology's rapid growth, driven by improved internet access and digital infrastructure, risks outpacing legal frameworks, potentially undermining civil liberties and enabling misuse by state and private actors. African policymakers are urged to implement context-specific algorithms, robust cybersecurity measures, and regular audits to safeguard privacy and ensure inclusive, ethical adoption of facial recognition technologies - The South African

AGO, CELLULAR GIANTS SIGN WIRETAPPING PACT – AND YOUR CIVIL RIGHTS ARE THE TARGET

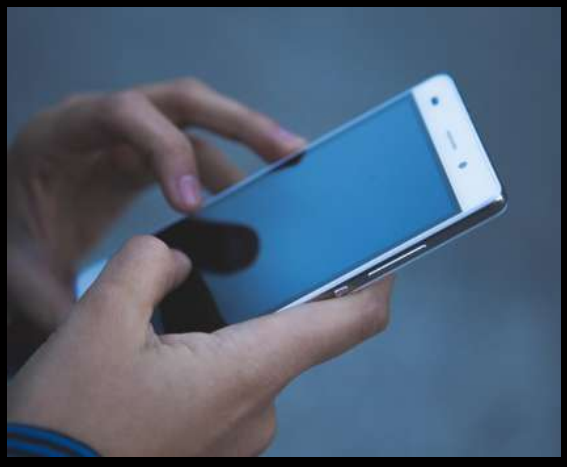


IMAGE SOURCE: INDONESIA AT MELBOURNE

Indonesia's Attorney General's Office (AGO) has signed agreements with four major telecommunication operators, including PT Telekomunikasi Indonesia and Telkomsel, to install wiretapping devices and facilitate data exchange for law enforcement purposes . The AGO states this measure, effective June 24, 2025, is crucial for tracking fugitives and gathering intelligence, asserting that public privacy will not be compromised and the access is purely for legal work, supported by a 2021 law granting the AGO wiretapping authority . However, the move has raised significant privacy concerns among analysts and human rights groups, who warn that the vague stipulations of the Memorandum of Understanding (MoU) lack sufficient safeguards and could enable mass surveillance, allowing prosecutors to access communications based merely on suspicion rather than formal charges or named suspects . Critics fear the agreement could lead to widespread monitoring of Indonesia's 350 million cellular users, undermining civil liberties and creating a "mass surveillance dragnet" without adequate oversight - Indonesia at Melbourne

ARMENIA APPROVES REAL-TIME FRT SURVEILLANCE AMID RIGHTS CONCERNS

IMAGE SOURCE: BIOMETRIC UPDATE

Armenia's parliament has passed amendments to the Law on Police granting the Ministry of Internal Affairs 24/7 access to a nationwide network of real-time facial recognition surveillance cameras installed across public buildings, transport, airports, and cultural sites, enabling automatic identification of individuals for both serious crimes and minor offenses with automated penalties. The law, effective August 9, raises serious concerns from civil society and international observers about privacy violations, threats to freedom of assembly, and potential abuse due to vague language allowing biometric surveillance based on "reasonable suspicion" without clear limits. Armenia lacks a comprehensive legal framework governing AI and biometric use, and key implementation details are left to ministerial discretion rather than primary legislation, increasing risks of unchecked mass surveillance. Human rights groups warn the law could suppress civic activity through a chilling effect on expression and protests, urging its repeal or suspension pending independent reviews by bodies like the OSCE/ODIHR and Venice Commission. The move aligns with broader regional trends but contrasts with Armenia's commitments under the EU-Armenia partnership, highlighting tensions between security measures and democratic safeguards - Biometric Update

ICE'S FACIAL RECOGNITION APP RAISES ALARMS OVER EXPANSION OF DOMESTIC SURVEILLANCE

In early 2025, ICE deployed Mobile Fortify, a smartphone app that equips agents to perform real-time facial recognition and fingerprint scans by accessing an extensive network of over 200 million facial images and 270 million biometric records from multiple federal and state databases, including DHS's IDENT system, CBP, FBI, and State Department records. This transformation of agents into roving biometric scanners enables rapid identification and retrieval of detailed personal information such as immigration status, criminal history, and travel data anywhere in the U.S., without requiring warrants or suspicion. The app's "Super Query" feature allows searches via name, biometrics, or other personal identifiers, raising significant legal and ethical concerns over privacy, lack of transparency, potential misuse, and Fourth Amendment protections. Civil liberties groups like the ACLU condemn Mobile Fortify as an unchecked expansion of mass surveillance that operates with minimal oversight and flawed facial recognition technology, exacerbating risks of wrongful detentions and racial profiling, while administrative audits have revealed security and management weaknesses within ICE's mobile device program. This rapid biometric integration signals a troubling shift toward expanded domestic surveillance under immigration enforcement, intensifying debates over the balance between national security and civil liberties - Biometric Update

INTELLIGENCE AGENCIES

ZAMBIA'S CYBER LAWS: PROTECTION OR A PATH TO DIGITAL REPRESSION?

IMAGE SOURCE: AFRICA.COM

Zambia's Cyber Security and Cyber Crimes Acts, enacted in April 2025, aim to combat cyber threats like fraud and identity theft by establishing regulatory bodies and defining new offenses. However, these laws grant authorities broad powers to intercept private communications, conduct warrantless audits on critical infrastructure, and impose harsh penalties, raising serious concerns about possible government overreach and digital repression. Critics—including journalists, activists, and digital rights groups—warn that vague definitions and weak oversight mechanisms could enable mass surveillance, stifle freedom of expression, and target dissenters, undermining privacy and civil liberties. Despite President Hichilema's prior commitments to digital rights, the laws' opaque development and sweeping provisions have sparked fears that their true purpose may be to silence opposition rather than purely protect citizens, positioning Zambia among a growing number of African countries tightening online controls with limited transparency or accountability - Africa.com

SURVEILLANCE, POWER, AND PARTICIPATION: REIMAGINING THE DIGITAL SOCIAL CONTRACT IN AFRICA

IMAGE SOURCE: EDGE LANDS INSTITUTE

The rise of digital surveillance across African cities is fundamentally reshaping state power, with traditional coercive tools increasingly supplemented by AI-driven surveillance systems and extensive data infrastructures. This shift raises serious concerns about privacy violations, mass data collection, and the erosion of civil liberties, often facilitated by weak legal frameworks and limited public participation in policymaking. Surveillance technologies, including biometric systems and spyware, disproportionately target political opponents, activists, and ordinary citizens, undermining democratic participation and trust in the social contract. Reimagining the digital social contract in Africa requires balancing security needs with citizens' rights through transparency, accountability, inclusive governance, and stronger protections to foster an equitable digital public sphere that respects privacy and enables meaningful civic engagement - Edge Lands Institute

TRUMP'S MEGABILL EXPANDS BIOMETRIC SURVEILLANCE

IMAGE SOURCE: BIOMETRIC UPDATE

The U.S. Senate has narrowly advanced H.R. 1, a massive budget reconciliation bill dubbed the "One Big Beautiful Bill," which dramatically expands federal biometric surveillance and AI-driven immigration enforcement infrastructure under the Trump administration's second term. The bill allocates over $175 billion for immigration-related funding in 2025 alone, including nearly $30 billion for ICE through 2029, with $2.5 billion specifically dedicated to AI systems, biometric data platforms, and digital case tracking. It also funds Customs and Border Protection (CBP) with over $6 billion to deploy advanced biometric technologies such as facial recognition, autonomous surveillance towers, and predictive behavioral models along U.S. borders. Notably, the bill imposes a ten-year moratorium preventing states from enforcing their own biometric privacy laws, effectively centralizing biometric regulation at the federal level. While proponents argue this will enhance national security and technological innovation, critics warn it threatens civil liberties, privacy rights, and could normalize mass biometric surveillance with minimal oversight. The bill also includes significant staffing increases and financial incentives for enforcement agencies, signaling a major expansion of biometric-enabled immigration control - Biometric Update

CHINA'S NEW FACIAL RECOGNITION REGULATIONS: POSITIVE IMPACTS AND CHALLENGES

IMAGE SOURCE: MODERN DIPLOMACY

China's new facial recognition regulations, effective June 1, 2025, aim to balance technological innovation with stronger personal data protection by imposing stricter rules on the use and management of facial recognition technology. The measures require businesses to justify the necessity of facial recognition, prohibit its use as the sole identity verification method when alternatives exist, and restrict deployment in sensitive locations. Companies handling large volumes of biometric data must register with authorities, implement robust security measures such as encryption, and limit data retention periods. The regulations also encourage the use of national identity databases to reduce redundant data collection. While promoting responsible use, the rules address growing public concerns about privacy and data security, reflecting China's effort to regulate facial recognition technology comprehensively without stifling its development - Modern Diplomacy

CHINA'S NEW CYBERSPACE ID: A PROMISE OF SECURITY OR A TOOL FOR MASS SURVEILLANCE?

IMAGE SOURCE: VOCAL MEDIA

China's new Cyberspace ID system, jointly developed by the Cyberspace Administration of China and the Ministry of Public Security, introduces a nationwide digital identity intended to enhance online security and simplify user authentication. Instead of repeatedly submitting personal details, citizens can use a unique digital certificate or ID number to log into various platforms, with more than six million already registered. While the government claims this approach will bolster privacy and reduce data collection by private companies, critics warn it risks centralizing state surveillance, eroding online anonymity, and tightening control over digital expression. The system is viewed as a significant expansion of state power in monitoring and potentially controlling citizens' online activity, raising fundamental concerns about privacy, data protection, and the future of digital freedoms in China - Vocal Media

AUSTRIAN LOWER HOUSE PASSES BILL ON MONITORING OF SECURE MESSAGING

IMAGE SOURCE:REUTERS

Austria's lower house of parliament has passed a controversial bill allowing police to monitor secure messaging apps like WhatsApp and Signal as part of efforts to combat terrorism and serious crime, a move that has sparked significant privacy concerns and political debate. The legislation, which still requires approval from the upper house, would permit authorities to use so-called "state trojans" or spyware to access encrypted communications, but only with judicial authorization and under strict conditions, such as targeting individuals suspected of grave offenses. Supporters argue the measure is necessary to address security gaps and modernize law enforcement capabilities, while critics—including opposition parties and digital rights advocates—warn it threatens civil liberties, risks government overreach, and could set a troubling precedent for surveillance in Austria. The bill's passage comes amid broader European debates over the balance between security and privacy, with Austria's government assuring that oversight mechanisms will prevent abuse and limit the law's scope to exceptional cases - Reuters

INDIA'S 7 MAJOR RAILWAY STATIONS TO GET AI SURVEILLANCE AND FACIAL RECOGNITION

IMAGE SOURCE: TIMES OF INDIA

Seven major Indian railway stations—including Mumbai's Chhatrapati Shivaji Maharaj Terminus, New Delhi, Howrah, Sealdah, Chennai Central, Secunderabad, and Danapur—are set to receive AI-powered facial recognition surveillance systems to enhance passenger safety, particularly focusing on tracking known offenders and finding missing persons amid large crowds. This initiative, part of a broader modernization and security upgrade approved by the Ministry of Home Affairs, aims to utilize real-time facial scanning linked to the National Database on Sexual Offenders to identify potential threats quickly and improve crowd management. The project complements existing security measures like emergency response systems and CCTV networks, addressing growing concerns about crimes against women and overcrowding at busy stations. While officials promise the technology will operate under strict privacy guidelines, critics continue to raise concerns about oversight and the effectiveness of such surveillance in safeguarding civil liberties - Times of India

WILL MEXICO'S NEW BIOMETRIC ID CARD HARM DIGITAL PRIVACY?

IMAGE SOURCE: CONTEXT

Mexico has approved legislation establishing a mandatory biometric ID card system that collects fingerprints, iris scans, and facial data to create a centralized "Unique Identity Platform" linking citizens' biometric information to various government databases, such as tax records and missing persons data. The government justifies this move as a tool to combat organized crime, drug trafficking, and aid in searching for missing people, with authorities including the National Intelligence Centre and National Guard granted access to the data. However, digital rights groups express serious concerns about mass surveillance risks, lack of transparency, and potential misuse, noting that citizens will have little to no notification or control over how their data is accessed or shared, raising fears of privacy violations and authoritarian overreach. While President Claudia Sheinbaum assures that surveillance will not occur and privacy is constitutionally protected, critics warn that vague legal provisions and expanded data-sharing agreements—potentially with countries like the U.S.—may erode citizens' digital rights, creating a surveillance ecosystem with limited accountability and safeguards. The biometric ID rollout has begun in some municipalities and will expand nationwide, marking a significant shift in Mexico's identity and surveillance landscape - Context

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

Global Dialogue

Funded by the European Union

We are grateful for the support of our donors!