Issue #2

INTEL WATCH

June 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

EXCLUSIVE INTELWATCH REPORTS & RESEARCH

TANZANIA'S REPRESSION OF DISSENT UNDER THE GUISE OF COUNTERTERRORISM

BY INTELWATCH

DOWNLOAD REPORT

Summary:

Months before the October 2025 elections, the government of President Samia Suluhu Hassan has begun a systematic, unrelenting and brutal clampdown on critics, opposition leaders, civil society and even foreign activists. This repression has silenced critical voices, with media and human rights activists self-censoring over the experienced violent suppression of civil and political liberties.

Impunity, untouchability and the perception of existential threats to the regime feed these authoritarian tendencies with few signs of abating. This report exposes the persistent use of repressive laws by Tanzania's government, under the ruling Chama Cha Mapinduzi (CCM), as a primary weapon for suppressing political dissent, targeting opposition, and maintaining political dominance. Colonial-era and post independence laws, including detention, treason, and anti-terrorism statutes, are systematically employed to undermine political freedoms and curtail opposition activities. Since independence in 1961, Tanzania's leadership has historically retained colonial-era laws, using them as tools of political control rather than amending them to protect civil liberties. Although past governments insisted that these laws would never be used arbitrarily, history has shown that authorities invoke them whenever the need arises to suppress dissent.

The enactment and subsequent amendments to counterterrorism legislation, often influenced by international pressure, have expanded state powers, enabling their misuse and frequent application beyond genuine security threats to target and punish opposition leaders, activists, and journalists, resulting in prolonged pre-trial detentions and miscarriages of justice. Muslim leaders and Muslim communities have been disproportionately targeted under terrorism laws, with high-profile cases like the prolonged detention of Uamsho clerics illustrating systemic abuses such as secret detentions, extrajudicial killings, and intimidation of families. The judiciary and prosecutorial systems often lack independence, evidenced by cases like that of opposition Chadema party leader Freeman Mbowe and more recently Tundu Lissu, which reveal political influence over legal proceedings. Judges face pressure, and state agencies routinely act on political directives, further eroding the rule of law.

Civil society advocacy for legislative reform remains weak, partly due to fear of reprisals and the perception that anti-terrorism laws primarily affect marginalised groups. The concentration of power in the executive, enabled by the 1977 Constitution and laws like the National Security Act, facilitates arbitrary detentions, restricts access to information, and curtails media freedoms. Recent legislative additions, such as the Cybercrimes Act of 2015, have further empowered authorities to target journalists and human rights defenders under vague provisions.

Precedents for these practices were set during earlier administrations, notably under President Jakaya Kikwete, whose government prosecuted opposition figures and activists under terrorism laws, often resulting in lengthy pre-trial detentions and judicial criticism of politically motivated prosecutions. The situation significantly deteriorated under the Presidency of John Magufuli. The security apparatus–including the police, intelligence services, and military– has consistently aligned with the ruling party, using covert taskforces to target perceived threats and suppress dissent. The misuse of counterterrorism laws, particularly against dissidents and human rights activists, evokes memories of past government repression, where repressive laws were weaponized to silence critics.

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE UPDATES

PREDATOR SPYWARE ACTIVITY RESURFACES IN MOZAMBIQUE USING NOVEL TECHNIQUES

IMAGE SOURCE: IT SECURITY NEWS

Recent research by the Insikt Group has uncovered the resurfacing of Predator spyware activity in Mozambique, marking the first time the sophisticated surveillance tool has been linked to operators in the country. Despite US sanctions imposed on its backers since July 2023, Predator continues to find new customers, with Africa now accounting for more than half of all known users. The investigation also established the first technical connection between Predator's infrastructure and corporate entities tied to the Intellexa Consortium, which has been sanctioned by the US. The findings stem from an inquiry into individuals associated with Intellexa, highlighting the ongoing proliferation of commercial spyware in African nations and raising concerns about surveillance, privacy, and the effectiveness of international sanctions in curbing the spread of such technologies - IT Security News

GHANAIANS URGED TO USE RTI LAW TO ASK GOVERNMENT TO DISCLOSE INFORMATION ON SPYWARE

IMAGE SOURCE: GHANA BUSINESS NEWS

Ghanaian authorities have reportedly spent about $184 million acquiring at least five types of spyware and surveillance technologies from various international companies, including Israeli, Taiwanese, Swiss, Greek, and Chinese firms, yet have remained silent about the details and purposes of these acquisitions. Despite constitutional protections against state interference in citizens' privacy, evidence suggests these tools are being used to monitor dissent, raising concerns about transparency, accountability, and potential rights violations. Experts and researchers highlight the secrecy surrounding spyware procurement and deployment, noting that weak privacy laws favor state agencies and make it difficult for citizens to demand accountability. Consequently, Ghanaians are being urged to use the Right to Information (RTI) law to request disclosure from the government regarding its use of spyware, as democratic oversight and judicial control are essential to prevent abuses and ensure that surveillance does not undermine democratic freedoms - Ghana Business News

MTN HITS BACK AT US CONGRESSWOMAN'S ACCUSATIONS OF COMPLICITY IN TERROR FINANCING

IMAGE SOURCE: DAILY MAVERICK

MTN Group is facing serious accusations from U.S. Congresswoman Elise Stefanik, who has called for an investigation into the telecom giant's alleged links to Iran, Hamas, and potential complicity in terror financing, urging Bank of New York Mellon to halt its role as MTN's ADR sponsor and cooperate with U.S. sanctions probes. These allegations are tied to a pending lawsuit in New York accusing MTN of terrorism financing under the U.S. Anti-Terrorism Act. MTN strongly denies these claims, emphasizing that no court has ruled against them and that the legal case is still in early stages. The company also refutes suggestions that South African President Cyril Ramaphosa, who chaired MTN two decades ago, benefited improperly, and clarifies it holds only a minority, non-operational stake in Iran's Irancell, complying with sanctions by not investing or extracting dividends since 2018. Despite ongoing litigation and political pressure, MTN asserts its commitment to human rights and advancing Africa's digital progress while navigating reputational challenges amid complex geopolitical scrutiny - Daily Maverick

ZIMBABWE MARKS RISE IN DIGITAL SURVEILLANCE

IMAGE SOURCE: BULAWAYO 24 NEWS

Zimbabwe is witnessing a significant rise in digital surveillance by government authorities, which is severely undermining civil liberties and intensifying repression against journalists and human rights defenders, according to a report by Unwanted Witness. The Cyber and Data Protection Act, enacted under the guise of national security, grants the government sweeping powers to monitor citizens' digital communications and access personal data with minimal judicial oversight, enabling mass surveillance targeting activists, independent media, and political opponents. The report highlights cases like journalist Blessed Mhlanga's prolonged detention under this law, illustrating its chilling effect on press freedom. Surveillance activities have escalated notably amid political tensions, including debates over constitutional amendments to extend President Emmerson Mnangagwa's tenure, with increased CCTV deployment and spyware use to monitor dissent. The report calls for urgent reforms to establish independent oversight and protect fundamental freedoms, warning that without such measures, digital surveillance will further erode free expression, political activism, and journalistic integrity in Zimbabwe - Bulawayo 24 News

KENYA DIGITAL TRANSFORMATION PROGRESS: RUTO'S 1,000 DAYS OF GROWTH AND CONTROL

IMAGE SOURCE: TECH TRENDS

Kenya's digital transformation under President William Ruto has seen rapid expansion in digitized government services, with the eCitizen platform growing from fewer than 400 services in 2022 to over 22,500 by mid-2025, and registered users more than doubling to 30 million, resulting in a tenfold increase in government revenue collection. The country has also invested heavily in ICT infrastructure, digital innovation hubs, and youth digital skills programs, positioning itself as a leading digital hub in Africa. However, these advances are shadowed by increasing incidents of internet shutdowns, social media throttling, mass surveillance, and suppression of online dissent, raising concerns about digital rights and authoritarian tendencies. Notably, the High Court declared prior internet shutdowns unlawful in May 2025, highlighting the tension between technological progress and fundamental freedoms. The article concludes that while Kenya's digital transformation is remarkable, its ultimate success depends on balancing innovation with robust protections for privacy, free expression, and independent oversight to prevent digital repression - Tech Trends

POLICE, FEDERAL VIDEO SURVEILLANCE OF ANTI-ICE PROTESTS IN LOS ANGELES RAISE ALARMS

IMAGE SOURCE: BIOMETRIC UPDATE

In response to anti-ICE protests in Los Angeles, the LAPD and federal agencies have deployed extensive video surveillance, including aerial footage from helicopters and drones, facial recognition technology, Ring camera footage, and social media monitoring to identify and track demonstrators. A controversial incident involved an LAPD officer warning protesters from a helicopter that they were being recorded and could be located at home, raising serious concerns about intimidation and suppression of constitutional rights. Civil liberties groups like the ACLU and EFF condemned these practices as authoritarian and a threat to free speech, highlighting the risks of long-term data retention and the potential for political retribution. The surveillance disproportionately affects communities of color and immigrants, exacerbating existing biases. Despite public outcry, Los Angeles lacks robust oversight compared to other cities, and federal agencies like ICE operate with fewer restrictions, using powerful facial recognition tools such as Clearview AI. This convergence of surveillance technologies creates a chilling effect on protest participation and underscores the urgent need for transparency and accountability in law enforcement's use of digital monitoring tools - Biometric Update

IN THIS ERA OF SPYWARE, PARLIAMENT MUST CODIFY SAFEGUARDS IN SURVEILLANCE LAW

IMAGE SOURCE: DAILY MAVERIVK

The article argues that South Africa's ongoing reform of the Regulation of Interception of Communications Act (Rica) presents a critical opportunity to establish robust legal safeguards against surveillance abuses, especially given the rise of sophisticated spyware technologies. Despite the Constitutional Court declaring the existing law unconstitutional in 2021 and setting a 36-month deadline for reform, Parliament's slow and minimalist approach has delayed effective changes, leaving the country vulnerable. Key flaws in the Rica Bill include a weak notification system that allows indefinite suspension of informing surveillance targets, undermining accountability and remedy; a one-sided warrant application process lacking adversarial safeguards, which risks authorizations based on false claims; and inadequate transparency about the use of intrusive spyware that can erase traces and is often operated by private vendors. The article emphasizes that international human rights law requires timely notification of surveillance to enable effective remedies, and it advocates for the introduction of a public advocate system—an independent legal representative to challenge surveillance warrants in secret hearings—as a proven mechanism to enhance oversight and protect privacy rights. Without these reforms, surveillance abuses will continue unchecked, threatening constitutional freedoms and South Africa's potential to set a global example in surveillance law - Daily Maverick

RESEARCHERS UNCOVER POSSIBLE IPHONE SPYWARE CAMPAIGN INSIDE U.S

IMAGE SOURCE: AXIOS

Researchers from iVerify have uncovered what they believe to be the first evidence of an active spyware campaign targeting iPhones in the U.S. and European Union, focusing on six high-profile devices linked to government officials, political campaigns, media, and AI companies. The spyware exploited a vulnerability in iOS's "Nickname" feature, causing unusual crashes indicative of tampering, with one EU official receiving an Apple threat notification about a month after such an event. Apple has since fixed the vulnerability in iOS 18.3 but disputes that it was exploited in targeted attacks, describing the issue as a conventional software bug and stating no credible evidence supports claims of hacking. The investigation highlights circumstantial evidence suggesting sophisticated zero-click attacks, possibly by state-linked actors previously known to target these individuals. iVerify urges high-risk users to keep devices updated and enable Apple's Lockdown Mode to guard against such spyware, emphasizing the need for further research and public discussion on mobile security threats - Axios

INSIDE THE PHONE-SPYING SCANDAL ROCKING ITALY'S JOURNALISM COMMUNITY

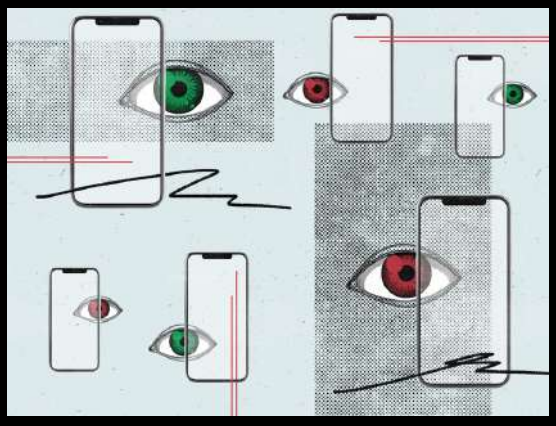

IMAGE SOURCE: COLUMBIA JOURNALISM REVIEW

Italian investigative journalists from the digital outlet Fanpage, including editor-in-chief Francesco Cancellato and Naples bureau chief Ciro Pellegrino, have been targeted with military-grade spyware called Graphite, developed by Israeli company Paragon Solutions, sparking a major national scandal. Citizen Lab researchers confirmed that the spyware silently infected their iPhones, granting full access to calls, messages, photos, and activating microphones and cameras without detection. The attacks likely occurred via malicious files sent through WhatsApp, and the journalists only discovered the breaches after receiving Apple's security alerts. While the Italian government denies authorizing surveillance on journalists, acknowledging only monitoring of migrant-rights activists, suspicions remain high since Graphite is sold exclusively to state agencies. The scandal has prompted investigations by Italian prosecutors, condemnation from press freedom groups, and calls for accountability amid fears that state secrecy is being used to cover up illegal spying on the media, threatening press freedom and democratic oversight. Italy has since cut ties with Paragon amid growing political backlash - Columbia Journalism Review

GRAPHITE CAUGHT FIRST FORENSIC CONFIRMATION OF PARAGON'S IOS MERCENARY SPYWARE FINDS JOURNALISTS TARGETED

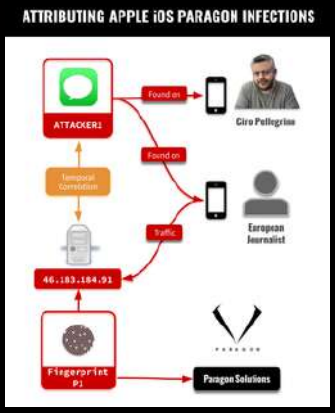

IMAGE SOURCE: THE CITIZEN LAB

Citizen Lab's forensic analysis has provided the first high-confidence confirmation that Paragon Solutions' Graphite mercenary spyware targeted at least two journalists—a prominent European journalist and Italian journalist Ciro Pellegrino—using sophisticated zero-click iMessage attacks exploiting a vulnerability later patched in iOS 18.3.1 (CVE-2025-43200). Both infections are linked to the same Paragon operator infrastructure, indicating coordinated targeting. This spyware silently compromised the devices, granting extensive access without the users' knowledge. The investigation also connects these attacks to a broader cluster involving other journalists at the Italian news outlet Fanpage.it, raising concerns about state or state-like actors using mercenary spyware against the press. Despite the Italian government acknowledging some use of Paragon spyware, it denies responsibility for targeting these journalists and has declined Paragon's offer to assist in investigations, citing national security concerns. The case highlights ongoing risks to journalists in Europe from advanced spyware and underscores the urgent need for transparency, accountability, and stronger protections against digital surveillance abuses. The analysis and monitoring of Paragon's operations continue - The Citizen Lab

APPLE FIXES ZERO-CLICK EXPLOIT UNDERPINNING PARAGON SPYWARE ATTACKS

IMAGE SOURCE: THE REGISTER

Apple has confirmed and publicly documented a zero-click vulnerability (CVE-2025-43200) in its Messages app that was exploited to deploy Paragon Solutions' Graphite spyware on iPhones of at least two European journalists in early 2025. The flaw, involving a logic error when processing maliciously crafted photos or videos shared via iCloud Link, allowed remote code execution without any user interaction, making the attacks stealthy and difficult to detect. Apple patched the vulnerability in iOS 18.3.1 released in February 2025 but only recently added details to its security advisory. Citizen Lab's forensic analysis linked the infections to Paragon's mercenary spyware infrastructure, highlighting a targeted campaign against journalists, including Italian reporter Ciro Pellegrino. The spyware grants extensive access to device data while leaving minimal traces, raising serious concerns about state-sponsored surveillance and digital privacy. Following public exposure, the Italian government ended its contract with Paragon amid the scandal. Security experts advise users to keep devices updated and enable Lockdown Mode for enhanced protection against such sophisticated spyware - The Register

FACIAL RECOGNITION ERROR SEES WOMAN ACCUSED OF THEFT

IMAGE SOURCE: BBC

Danielle Horan was wrongly accused of shoplifting about £10 worth of toilet paper after her image was mistakenly added to a facial recognition watchlist used by Home Bargains stores in Greater Manchester. She was removed from two stores in May and June without explanation, causing her significant distress and anxiety. The retail security company Facewatch, which supplies the technology, acknowledged the error and said the retailer has since improved staff training. A review confirmed Horan had purchased the items in question. Civil liberties groups warn that such facial recognition errors wrongly label innocent people as criminals, undermining the presumption of innocence and calling for stricter regulation or bans on the technology in retail. The UK government emphasizes that biometric data use must be lawful, fair, and transparent to prevent such incidents - BBC

THE DANGEROUS RISE OF MILITARY-GRADE SPYWARE – A GLOBAL DAY OF ACTION

IMAGE SOURCE: BDS MOVEMENT

The article exposes the widespread use of military-grade spyware, particularly highlighting Israel's deployment of such technology in Gaza to surveil and target civilians, contributing to severe human rights violations. It explains how Israeli companies like NSO Group and Candiru developed spyware tools such as Pegasus and Predator, initially tested on Palestinians before being sold globally, allowing various governments to suppress dissent, monitor journalists, and violate privacy. The piece underscores high-profile abuses, including the hacking of associates of murdered journalist Jamal Khashoggi and the targeting of activists, while criticizing the failure of international bodies like the European Council to effectively regulate spyware. Despite these challenges, the article points to growing resistance through legal actions in Colombia, Spain, and the US, as well as advocacy efforts in Ghana, culminating in a call for a Global Day of Action to demand bans on spyware, corporate accountability, and stronger protections for human rights and democracy - BDS Movement

IRAN CLAIMS WHATSAPP HARVESTS DATA FOR ISRAEL

IMAGE SOURCE: SCROLL IN

Iranian state media has urged citizens to delete WhatsApp, alleging without evidence that the app collects user data and shares it with Israel, which purportedly uses this information for military targeting, including airstrikes on Iranian officials. WhatsApp, owned by Meta, strongly denies these claims, emphasizing its end-to-end encryption that prevents anyone—including WhatsApp itself—from accessing message content or precise location data, and stating it does not provide bulk user data to any government. While independent verification of Iran's allegations is impossible due to lack of evidence, historical precedents exist of Israeli-linked cyber operations exploiting WhatsApp vulnerabilities via spyware like Pegasus to target specific individuals through spearphishing attacks. Experts caution that despite WhatsApp's strong security features, no system is entirely impenetrable, and users should remain vigilant against targeted cyberattacks. The controversy arises amid heightened Israel-Iran tensions and ongoing internet restrictions in Iran, raising broader concerns about digital privacy, state surveillance, and misinformation in conflict zones - Scroll in

REPRESSION MONITOR

ZIMBABWE MARKS RISE IN DIGITAL SURVEILLANCE, REPRESSION ON JOURNALISTS AND HUMAN RIGHTS DEFENDERS

IMAGE SOURCE: NEW ZIMBABWE

Zimbabwe has seen a significant rise in digital surveillance and repression targeting journalists, human rights defenders, and activists, with the government increasingly deploying spyware and other intrusive technologies to monitor and intimidate dissenting voices. This escalation is part of a broader crackdown on freedom of expression and civil liberties, facilitated by expanded state surveillance capabilities often justified under national security pretexts. Human rights organizations warn that these practices undermine democratic freedoms and create a climate of fear, calling for greater transparency, accountability, and legal safeguards to protect privacy and uphold fundamental rights amid growing authoritarian control - New Zimbabwe

ALARMING REPORT SUGGESTS CHINA MAY BE SPYING ON YOUR VPN BROWSING DATA

IMAGE SOURCE: HOT HARDWARE

Several reports reveal that numerous VPN apps available on Apple's App Store and Google Play Store have undisclosed ties to Chinese companies, raising serious privacy and national security concerns. Despite Apple and Google's policies requiring transparency and prohibiting the sale or misuse of VPN browsing data, many Chinese-owned VPNs operate under China's national security law, which can compel them to share user data with the Chinese government without consent. Investigations have identified about 17 to 24 such VPN apps linked to Chinese firms, including those connected to Qihoo 360, a Chinese cybersecurity company under U.S. sanctions. Users of these VPNs risk having their browsing histories, IP addresses, and encrypted communications exposed to Chinese authorities, undermining the core privacy purpose of VPNs. Although some apps have been removed following earlier reports, many remain available, with developers often obscuring their Chinese ownership through offshore registrations. Experts warn that using these VPNs is effectively surrendering sensitive online activity to Beijing, emphasizing the need for users to choose reputable VPN providers with strict no-logs policies and servers located in privacy-friendly jurisdictions to avoid surveillance risks. Apple and Google have yet to take comprehensive action to remove all implicated apps, prolonging user exposure to potential data harvesting by China - Hot Hardware

CITY OF SEDONA'S SPY CAMERAS ARE A THREAT TO OUR PRIVACY AND RIGHTS

IMAGE SOURCE: SEDONA RED ROCK NEWS

The City of Sedona has installed a dozen automated license plate readers (ALPRs) around the city without public consultation, meetings, or adequate notice, sparking outrage over privacy violations and government overreach. These cameras indiscriminately track and store data on residents' and visitors' movements, associations, and locations, creating extensive surveillance databases that threaten fundamental rights and freedoms by enabling mass monitoring without individualized suspicion or warrants. The city's claim that ALPRs pose no privacy threat is contradicted by its refusal to disclose camera locations, undermining public trust. Technical flaws in ALPRs also risk misidentifying innocent drivers, leading to wrongful police stops. The surveillance disproportionately targets minority neighborhoods and raises concerns about "pre-crime" monitoring, chilling lawful activities and eroding civil liberties. Data management by private company Flock Safety further jeopardizes transparency and data protection, as private firms are not bound by constitutional safeguards. Critics argue that Sedona's secretive implementation of ALPRs resembles authoritarian surveillance practices, demanding public accountability and legal oversight to protect privacy and democratic rights - Sedona Red Rock News

HAZARDS OF THE SURVEILLANCE STATE AND PRIVATIZING NATIONAL SECURITY

IMAGE SOURCE: GEOPOLITICAL INTELLIGENCE SERVICES

Private tech companies have overtaken traditional defense contractors as central players in national security, providing governments with advanced AI-driven surveillance tools, facial recognition, and big data analytics that blur the lines between military defense and domestic security. While these innovations have improved efficiency and reduced costs, they operate with little transparency or accountability, often shielded by confidentiality and intellectual property protections, leaving citizens unaware that their data is collected and analyzed by private firms in partnership with governments. This shift has enabled extensive government surveillance of populations without meaningful oversight or the ability for individuals to opt out, resulting in significant violations of privacy and civil liberties. The profit motives of these companies, combined with governments' expansive powers, create a moral hazard where basic rights are sacrificed to maintain lucrative contracts. Potential future scenarios include public backlash demanding greater oversight, or, less likely, private contractors gaining enough power to challenge government authority. Overall, the privatization of national security surveillance represents a dangerous transfer of power away from democratically accountable institutions toward profit-driven entities, threatening individual freedoms and democratic governance - Geopolitical Intelligence Services

J&K POLICE CONFIRMS USE OF FACE RECOGNITION TECH IN DETENTION OF CARPENTER AT PAHALGAM

IMAGE SOURCE: THE WIRE

Jammu and Kashmir police have, for the first time, officially confirmed the use of facial recognition technology to detain a suspected overground worker (OGW) linked to militants near Pahalgam, following a terror attack in the area. The system, deployed at security checkpoints along the route to the Amarnath Yatra pilgrimage, uses a pre-fed database of hundreds of suspects named in militancy-related FIRs to flag individuals for detention, often without clear legal safeguards. While authorities emphasize the technology's role in enhancing security, especially during sensitive events like the pilgrimage, human rights groups and legal experts criticize the system for privacy violations, lack of transparency, and potential misuse, noting that India's facial recognition software has low accuracy and is implemented without adequate legal oversight. The deployment raises concerns about mass surveillance, systemic bias against marginalized communities, and the erosion of fundamental rights protected under India's constitution - The Wire

ALLEGED ITALIAN PHONE HACKING INVOLVES POLITICAL GOSSIP WEBSITE, SOURCES SAY

IMAGE SOURCE: MILWAUKEE JOURNAL SENTINEL

In Milwaukee, growing public opposition is challenging the police department's interest in deploying facial recognition technology, amid concerns over privacy, racial bias, and lack of transparency. Civil rights advocates and community members argue that the technology disproportionately targets Black and minority communities, exacerbating systemic injustices and risking wrongful identifications. Despite police claims that facial recognition aids crime-solving, critics highlight its documented inaccuracies and potential to erode civil liberties without proper oversight. The debate reflects broader national conversations about balancing public safety with protecting individual rights, with calls for stricter regulations or outright bans on law enforcement's use of facial recognition in Milwaukee and beyond - Milwaukee Journal Sentinel

SPYWARE AND STATE ABUSE: THE CASE FOR AN EU-WIDE BAN

IMAGE SOURCE: EUROPEAN DIGITAL RIGHTS

The European Digital Rights (EDRi) position paper calls for a comprehensive EU-wide ban on spyware, arguing that the widespread, unregulated use of commercial spyware by at least 14 EU countries poses severe threats to fundamental rights, democracy, and collective security. Spyware covertly infiltrates devices to extract data and monitor individuals, disproportionately targeting journalists, activists, politicians, and human rights defenders, thereby undermining democratic norms and chilling civic space. The EU has become a hub for spyware development and export due to permissive legal loopholes and weak oversight, enabling spyware vendors to profit despite documented abuses. EDRi urges lawmakers to prohibit the development, production, marketing, sale, export, and use of spyware, including banning the commercial trade of software vulnerabilities that facilitate spyware creation. Additionally, the paper calls for legal remedies and accountability mechanisms to support victims of unlawful surveillance and to ensure state and political responsibility, emphasizing that only a full ban can effectively safeguard human rights and democratic institutions in Europe - European Digital Rights

ALLEGED ITALIAN PHONE HACKING INVOLVES POLITICAL GOSSIP WEBSITE, SOURCES SAY

IMAGE SOURCE: REUTERS

Italian prosecutors are investigating the alleged hacking of seven phones, including that of Roberto D'Agostino, head of the political gossip website Dagospia, as part of a wider surveillance scandal involving spyware from the Israeli firm Paragon. The inquiry follows earlier revelations that Italian intelligence agencies used Paragon's Graphite spyware, authorized by prosecutors, primarily to monitor migrant rescue activists and combat crime, though the government denies targeting journalists despite forensic evidence showing infections of journalists from Fanpage.it. The scandal has sparked political controversy and demands for transparency, with opposition figures and press freedom groups condemning the surveillance as an attack on democratic rights. Italy has since terminated its contract with Paragon amid public backlash, while investigations continue into unauthorized phone intrusions linked to political and media figures - Reuters

INTEL WATCH

Watching the watchers. Guarding the guardians.

HEADED TO A PROTEST? YOU MIGHT WANT TO LEAVE YOUR CELL PHONE AT HOME

IMAGE SOURCE: DEMOCRAT AND CHRONICLE

Attending protests with a cell phone poses significant privacy and security risks due to advanced surveillance techniques used by law enforcement, such as Stingrays and IMSI catchers that can track location and intercept communications without user knowledge. Experts recommend turning off or putting phones in airplane mode to minimize tracking, disabling biometric locks like Face ID or fingerprint recognition to better protect against forced unlocking, and considering the use of burner phones or Faraday bags to block signals. While phones are valuable for safety, coordination, and documenting events, carrying them can lead to data extraction if confiscated, potentially exposing protest participation and contacts. Protesters are advised to weigh these risks carefully, use encrypted messaging apps like Signal, disable unnecessary services (e.g., location, AirDrop), and back up data before attending. Overall, balancing communication needs with digital security precautions is essential to safeguard privacy and avoid surveillance abuses during protests - Democrat and Chronicle

TELEGRAM MESSENGER'S TIES TO RUSSIA'S FSB REVEALED IN NEW REPORT

IMAGE SOURCE: NEWS WEEK

An investigation by the Russian outlet IStories revealed that Telegram's server infrastructure is managed by companies with ties to Russia's Federal Security Service (FSB), including Global Network Management (GNM) owned by Vladimir Vedeneev, who also serves as Telegram's CFO. These companies, linked to Russian intelligence contractors like Electrontelecom, provide thousands of IP addresses and maintain infrastructure potentially enabling FSB access to Telegram user data. While Telegram denies any unauthorized access or cooperation with Russian authorities, emphasizing its encryption and global server distribution, experts warn that Telegram's default chats are not end-to-end encrypted and that unique device identifiers could facilitate user surveillance if accessed by intelligence agencies. Human rights groups have reported the FSB using Telegram communications as evidence in treason cases, suggesting possible undisclosed surveillance methods. The revelations cast doubt on Telegram's security claims and raise concerns about privacy, government monitoring, and the platform's role in authoritarian regimes. Telegram's founder Pavel Durov, now based outside Russia, maintains the platform's commitment to privacy but faces growing scrutiny over these alleged links - News Week

CHINA PART OF CONCERN INDIAS CCTV CRACKDOWN OVER SPYING FEARS HITS GLOBAL GIANTS LIKE HIKVISION XIAOMI

IMAGE SOURCE: BUSINESS TODAY

India has implemented stringent new cybersecurity rules effective April 9, 2025, requiring all internet-connected CCTV cameras—both domestic and imported—to undergo mandatory certification involving hardware inspections, firmware testing, source code submission, and factory audits before sale. This crackdown primarily targets Chinese surveillance giants like Hikvision, Dahua, and Xiaomi, which dominate India's CCTV market and raise national security concerns due to China's National Intelligence Law compelling companies to cooperate with state intelligence. Indian officials emphasize the risk of espionage through internet-connected cameras, citing global precedents of tech equipment misuse for spying. Despite pushback from manufacturers over testing capacity and compliance costs, the government insists on strict enforcement to secure national surveillance infrastructure. The policy has caused significant delays in product approvals, disrupted the CCTV market, and intensified India's efforts to reduce reliance on Chinese technology amid broader geopolitical tensions - Business Today

---

HOW THE US IS TURNING INTO A MASS TECHNO-SURVEILLANCE STATE

IMAGE SOURCE: EL PAISE

Since Donald Trump's return to the White House, the U.S. government has rapidly expanded a vast techno-surveillance state using AI-powered tools to monitor and persecute thousands, primarily immigrants, foreigners, and students, often without judicial authorization. This system includes unauthorized scanning of social media, biometric and health data analysis, phone communication interception, geolocation tracking, and license plate readers, supported by large contracts with private companies like Palantir. Programs such as Babel X and SocialNet aggregate data from hundreds of sources to profile individuals, influencing decisions like asylum denial based on social media activity. The Department of Government Efficiency, led by Elon Musk, collects sensitive citizen data for use in deportation platforms. Surveillance infrastructure also includes drones, facial recognition, and spyware from firms like NSO Group. Critics warn this surveillance disproportionately targets marginalized groups, threatens fundamental rights, and risks normalizing authoritarian practices, with concerns that once accepted, such systems can be used against anyone. Similar surveillance expansions are noted in Europe, raising global alarms about privacy and democratic freedoms - El Pais

EUROPEAN JOURNALISTS TARGETED WITH PARAGON SOLUTIONS SPYWARE, SAY RESEARCHERS

IMAGE SOURCE: THE GUARDIAN

Citizen Lab has forensically confirmed that Paragon Solutions' mercenary spyware, Graphite, was used to target at least three European journalists, including two Italians—Ciro Pellegrino and Francesco Cancellato of the investigative news outlet Fanpage.it—via sophisticated zero-click iMessage attacks exploiting a critical iOS vulnerability. These infections link to the same Paragon operator infrastructure, deepening concerns about unlawful surveillance of journalists critical of political powers, notably the Italian government under Prime Minister Giorgia Meloni, which denies illegal spying despite mounting evidence. The revelations highlight the ongoing misuse of commercial spyware in democratic countries, sparking calls from press freedom organizations and the European Commission for transparency, accountability, and stronger protections against digital surveillance abuses. The scandal has led to Italy terminating its contract with Paragon, though the exact responsible parties and legal authorizations remain unclear, underscoring the broader risks spyware poses to press freedom and civil society in Europe - The Guardian

GOVT ALLOCATES MILLIONS TO BOOST STATE SURVEILLANCE USING SPYWARE

IMAGE SOURCE: CAPITAL NEWS

Kenya's 2025/26 supplementary budget allocates significant funds to expand state surveillance capabilities, including Sh150 million specifically for the acquisition and operation of Optimus 3.0, an advanced spyware system designed to infiltrate devices, decrypt encrypted messages, and monitor social media activity. The Directorate of Criminal Investigations (DCI) receives increased funding for forensic labs and digital monitoring, while the police and security sectors see broader budget boosts, including Sh800 million for police operations and Sh150 million for upgrading communication equipment. These allocations coincide with the upcoming debate on the controversial Kenya Information and Communication (Amendment) Bill, which would grant the government sweeping powers to access private digital data without court orders, raising serious privacy and civil liberties concerns. Critics argue the government is prioritizing surveillance and control over citizens' digital freedoms without adequate public consultation or legal safeguards, while also cutting funds for essential social services, intensifying fears of authoritarian overreach - Capital News

CHINA COVERTLY USING CHATGPT FOR PROPAGANDA POSTS ON SOCIAL MEDIA, SAYS OPENAI

IMAGE SOURCE: 9TO5MAC

OpenAI researchers have uncovered multiple covert operations, including four likely originating from China, using ChatGPT to generate propaganda posts and comments on social media platforms such as TikTok, Reddit, Facebook, and X in various languages including English, Chinese, and Urdu. These operations, dubbed "Sneer Review," produced both original posts and engagement content on politically sensitive topics like the dismantling of the U.S. Agency for International Development and criticism of a Taiwanese game opposing the Chinese Communist Party. Remarkably, the perpetrators also used ChatGPT to create detailed internal performance reviews of their propaganda efforts, providing insights into their tactics. Additionally, ChatGPT was employed to draft emails targeting journalists, analysts, and politicians for intelligence gathering. OpenAI has blocked ten such operations globally, with China, Russia, Iran, and North Korea identified as key abusers, highlighting a growing trend of state-linked actors exploiting AI tools for disinformation, influence campaigns, and surveillance - 9to5mac

ITALY ADMITS HACKING ACTIVISTS WITH ISRAELI SPYWARE PARAGON

IMAGE SOURCE: HAARETZ

Italy has admitted that its intelligence agencies legally used Israeli-made Paragon spyware to hack phones of migrant rescue activists linked to the Mediterranea charity, with authorization from prosecutors, but denies targeting journalists despite forensic evidence showing infections of at least two Italian journalists, including Ciro Pellegrino of Fanpage.it. The parliamentary oversight committee report revealed that the spyware was employed mainly to combat illegal immigration, terrorism, and organized crime, and that the contract with Paragon was initially suspended and later terminated amid public and political backlash. While the government insists surveillance was lawful and limited, critics and press freedom advocates condemn the use of mercenary spyware against civil society and demand transparency and accountability. The scandal has led Italy to sever ties with Paragon and intensified scrutiny over state surveillance practices and potential abuses of digital spying tools - Haaretz

THE ZIONIST AI EMPIRE: HOW ISRAEL WEAPONIZED SURVEILLANCE TO CONTROL THE WORLD

IMAGE SOURCE: EASTERN HERALD

An investigation by Eastern Herald reveals that Israel, through military tech firms like NSO Group, Cellebrite, Verint Systems, and AI startups such as AnyVision and Toka, has built a global AI surveillance empire that extends far beyond its borders. These companies have developed intrusive technologies—including spyware, facial recognition, predictive policing, and behavioral analytics—that were first tested in occupied Palestinian territories, particularly Gaza, and then exported to Western democracies and allied nations under the guise of counterterrorism. Israeli firms have deep partnerships with major tech giants like Google, Amazon, and Meta, embedding surveillance tools and personnel with intelligence backgrounds into global digital infrastructures. This surveillance apparatus disproportionately targets marginalized groups worldwide, normalizing authoritarian control and digital apartheid. The report warns that BRICS nations risk importing this oppressive model if they do not establish sovereign AI systems free from Israeli-linked technologies, advocating for transparency, open-source development, and AI focused on social good rather than repression. Ultimately, Israel's AI empire represents not just technological dominance but an ideological export of control, surveillance, and racial profiling on a global scale - Eastern Herald

EUROPE'S GROWING FEAR: HOW TRUMP MIGHT USE U.S. TECH DOMINANCE AGAINST IT

IMAGE SOURCE: THE NEW YORK TIMES

A recent incident involving Microsoft's suspension of the International Criminal Court (ICC) chief prosecutor's email account, following a Trump executive order targeting the ICC over its investigation into alleged Israeli war crimes, has alarmed European policymakers and highlighted the geopolitical risks of U.S. tech dominance. The executive order barred American companies from providing services to the ICC prosecutor, leading Microsoft to swiftly comply and cut off digital communications—just after the ICC issued an arrest warrant for Israeli Prime Minister Benjamin Netanyahu. This move disrupted the ICC's work and underscored how U.S. administrations can leverage control over key technology providers to enforce foreign policy, even against institutions in allied countries. European officials now fear that such dominance could be weaponized in future disputes, prompting calls for greater European digital sovereignty and less reliance on U.S.-based tech infrastructure - The New York Times

INTEL WATCH

Watching the watchers. Guarding the guardians.

PARAGON MUST ANSWER FOR SPYWARE USE AGAINST CIVIL SOCIETY AND JOURNALISTS

IMAGE SOURCE: ACCESS NOW

Recent investigations by Citizen Lab have confirmed that Paragon Solutions' Graphite spyware has been used to target journalists, humanitarian workers, and civil society actors in Italy, raising serious concerns about the misuse of surveillance technology by democratic governments. Despite Paragon's claims of selling only to responsible state actors, evidence shows that Italy deployed this spyware against individuals engaged in legitimate humanitarian and journalistic work without providing transparency or remedies to victims. The Italian government has refused to allow independent verification of the spyware's use, and Paragon's contract with Italy was terminated only after public exposure, highlighting systemic failures in oversight, accountability, and victim support. Human rights organizations urge Paragon and its investors to implement robust safeguards, conduct independent audits, provide reparations to those harmed, and ensure compliance with international human rights standards, emphasizing that voluntary frameworks are insufficient to prevent abuses of such intrusive technologies. - Access Now

ISRAEL SAYS IRAN IS HACKING SECURITY CAMERAS FOR SPYING

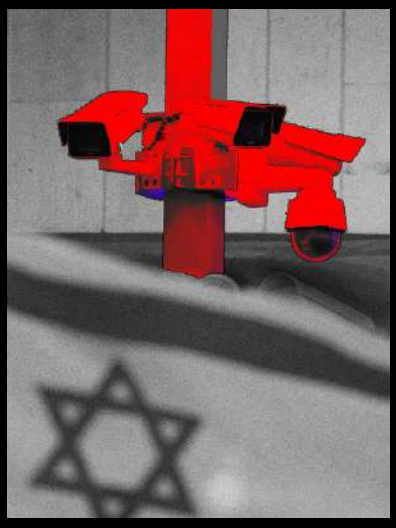

IMAGE SOURCE: WIRED

Iran has been actively hacking into private home security cameras across Israel to gather real-time intelligence on missile impact sites and improve targeting accuracy amid ongoing hostilities, according to Israeli cybersecurity officials. This tactic, which mirrors methods previously used by Hamas and Russia in other conflicts, exploits vulnerabilities in internet-connected cameras—often due to weak passwords or outdated software—turning everyday surveillance devices into tools of war. Israeli authorities have urged citizens to enhance their camera security by changing passwords and enabling two-factor authentication, while also imposing media blackouts on images of missile damage to limit intelligence leaks. The cyber espionage campaign highlights the growing risks of interconnected devices in modern warfare and the challenges of protecting civilian infrastructure from being weaponized - Wired

INTELLIGENCE AGENCIES

GOVT ALLOCATES MILLIONS TO BOOST STATE SURVEILLANCE USING SPYWARE

IMAGE SOURCE: CAPITAL NEWS

Kenya's 2025/26 supplementary budget allocates over Sh150 million specifically for the acquisition and deployment of Optimus 3.0, a sophisticated spyware tool designed to infiltrate devices, decrypt encrypted messages, and monitor social media activity, significantly expanding state surveillance capabilities without public consultation or legal safeguards. The Directorate of Criminal Investigations (DCI) receives substantial funding increases, including Sh400 million for operations and Sh150 million for upgrading communication equipment, while the police get an additional Sh800 million to bolster security infrastructure. These budgetary moves coincide with the upcoming debate on the controversial Kenya Information and Communication (Amendment) Bill, which would grant the government sweeping powers to access private digital data without court orders, raising serious privacy and civil liberties concerns. Critics warn that the government is prioritizing surveillance and control over citizens' digital freedoms, potentially legalizing existing intrusive practices, and undermining democratic rights amid limited transparency and accountability - Capital News

SH100M SPYWARE BUDGET SPARKS OUTRAGE AHEAD OF CONTROVERSIAL ICT LAW DEBATE

IMAGE SOURCE: EASTLEIGH VOICE

Kenya's 2025/26 national budget, totaling 4.29 trillion shillings, controversially allocates 100 million shillings to fund "Optimus 3.0," a powerful spyware tool aimed at monitoring internet activities, sparking public outrage amid ongoing debates over a contentious ICT law. The spyware budget raises concerns about privacy, government surveillance, and the potential misuse of digital monitoring technologies, especially as Kenya pursues expanded digital infrastructure and security measures. While the overall budget emphasizes economic recovery, job creation, and fiscal discipline without new taxes, critics warn that increased investment in surveillance tools threatens civil liberties and calls for greater transparency and regulation of state surveillance powers. The controversy highlights tensions between national security priorities and protecting citizens' digital rights - Eastleigh voice

ITALIAN SENATE APPROVES CONTROVERSIAL SECURITY LAW

IMAGE SOURCE: ECRE

Italy has terminated its contract with Israeli spyware firm Paragon Solutions following a major scandal in which Paragon's military-grade spyware, Graphite, was used to target journalists, migrant rescue activists, and government critics, sparking widespread political backlash and calls for investigation. The Italian parliamentary intelligence oversight committee (COPASIR) revealed that Italy's intelligence agencies initially suspended and later ended the use of Paragon's spyware amid public outcry. While the government insists that surveillance was lawful and conducted under prosecutorial oversight, it rejected Paragon's offer to assist in investigating alleged abuses, citing national security concerns. The controversy has intensified scrutiny over digital surveillance practices, press freedom, and human rights in Italy, with international organizations demanding transparency and accountability. Additionally, the Italian Senate approved a controversial security law amid these tensions, further fueling debate over civil liberties and state surveillance in the country - ECRE

AUSTRIAN GOVERNMENT AGREES ON PLAN TO ALLOW MONITORING OF SECURE MESSAGING

IMAGE SOURCE: REUTERS

Austria's coalition government has approved a plan to allow police to monitor suspects' secure messaging apps like WhatsApp and Signal to prevent militant attacks, addressing a significant intelligence gap previously filled by relying on foreign allies such as the UK and the US. The new framework requires prior approval from a three-judge panel and is expected to be used sparingly, targeting around 25 to 30 individuals annually, with parliamentary oversight in place to prevent mass surveillance. This move aims to enhance national security by making potential terrorists feel less secure while increasing public safety. The legislation is set to be implemented by 2027, following a tender process for the necessary monitoring technology. Although security officials hail the plan as a critical step in counterterrorism efforts, privacy advocates express concerns about potential infringements on civil liberties and the risk of government overreach - Reuters

INTELWATCH

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!