



# Atar

Sudan in Perspective

Issue 48, Monday, March 30, 2026

## OPINION

### **Connected, but not protected:** *Africa's place in the global surveillance web*

✉ **Mohamed Eldaby**



Artwork by: Mohamed Osman "Gaki"

*Deep in a tunnel under a pineapple field—a subterranean Pearl Harbor-era former airplane factory—I sat at a terminal from which I had practically unlimited access to the communications of nearly every man, woman, and child on earth who'd ever dialed a phone or touched a computer.*  
- Edward Snowden, *Permanent Record*

**T**hat moment revealed the true scale of modern surveillance: that governments may hold records on nearly everyone on the planet. What Snowden exposed, however, may have only scratched the surface.

As artificial intelligence begins to re-define surveillance, it does not simply expand its reach; it transforms what can be done with it. It introduces the possibility that systems once used to observe could now be used to decide, shaping not only information, but action.

Questions follow naturally: How is our private data being used? And more importantly, what law, if any, protects it from being used by foreign or domestic governments without our consent?

After the Pentagon designated **Anthropic** as a “supply chain risk,” its CEO, **Dario Amodei**, addressed the growing tension between artificial intelligence and military use. In his official statement, he noted that AI systems such as Claude have already been used in military analysis supporting operations. At the same time, he warned of clear limits: “We believe AI can undermine, rather than defend,

democratic values. Some uses are also simply outside the bounds of what today’s technology can safely and reliably do.”

Two such uses, he argued, should remain off-limits: mass domestic surveillance and fully autonomous weapons. The warning echoes Snowden’s earlier revelations, only now, the concern is no longer just access to information, but what is done with it. If surveillance defined the last decade, the integration of AI into these systems may define the next—where observation begins to merge into decision, and data into action.

While some countries have laws to protect their citizens’ privacy, such as **FISA (Foreign Intelligence Surveillance Act)** in the United States or the United Kingdom’s Investigatory Powers Act 2016 (IPA), the rest of the world’s privacy remains uncertain. As Snowden noted, much of this data is “stored at some server somewhere, waiting to be analyzed.”

Furthermore, the very country that controls many of the leading compa-

*“AI can undermine, rather than defend, democratic values.”*  
— **Dario Amodei**

nies in AI and the Internet applies legal frameworks differently to those outside its borders. As Snowden explained, Section 702 of the FISA Amendments Act allows the Intelligence Community (IC) to target non-U.S. persons located abroad who are deemed likely to possess “foreign intelligence information,” a broad category that can include journalists, corporate employees, academics, aid workers, and many others with no connection to wrongdoing. This authority has been used to justify major Internet surveillance programmes such as PRISM and upstream collection.

PRISM allows the National Security Agency to collect data from major technology platforms where users hold accounts, including companies like Google and Facebook, gathering information such as communications and metadata. With the growing role of artificial intelligence, the potential use of such data extends further, raising questions not only about where individuals are, but how their behaviour may be interpreted or anticipated.

Professor Shoshana Zuboff describes this as “behavioral surplus”, the idea that human behaviour is continuously collected, analyzed, and used by third parties, often for purposes that extend beyond the awareness or control of the individuals involved.

Snowden’s disclosures demonstrated that this system was not theoretical, but already operational at a global scale.

With the existence of programmes such as PRISM, this was no longer a possibility but a documented and routine practice. Major networks and platforms were shown to be part of a system through which large volumes of data could be accessed and analyzed.

This shifted the understanding of surveillance from something exceptional to something structural. It suggested that the infrastructure of the Internet itself had become intertwined with mechanisms of observation. And if that system already exists at a global scale, artificial intelligence does not introduce it, it extends its capabilities.

Recent discussions around the use of AI systems such as Anthropic’s Claude, and the broader conflict over control between technology companies and the Pentagon, raise deeper concerns about the expanding role of artificial intelligence within existing surveillance systems. These debates are not simply about which company provides the technology, but about how much control should be granted, and under what limitations.

This raises a more fundamental question: what new capabilities are being added to an already extensive surveillance infrastructure? Artificial intelligence enhances the ability to process, interpret, and act on vast amounts of data. In this context, concerns emerge about how such systems might influence military decision-making, particularly when applied to large-scale data drawn from everyday digital platforms.

This is not only a U.S. issue. As discussed in *Digital Democracy, Analogue Politics*, [Nanjala Nyabola](#) highlights how digital platforms such as Twitter and WhatsApp played a role in amplifying information during the 2016 collapse of [Chase Bank Kenya](#). While not an example of surveillance in the traditional sense, it demonstrates how digital systems can rapidly shape real-world outcomes at scale.

As these systems become more integrated into governance, security, and intelligence frameworks, the boundary between observation and action becomes less clear. The concern is no longer only about what is collected, but how it is interpreted and used.

The introduction of artificial intelligence into surveillance systems marks a significant shift in how data is processed and used. As one CentCom commander noted, processes that once took days can now be completed in seconds.

Rather than simply collecting information, AI systems are now capable of identifying patterns, detecting anomalies, and organizing data in ways that were previously impossible at scale. Platforms such as the Maven system, used by the U.S. military, integrate advanced data analytics with AI models to process satellite imagery and drone footage, enabling the rapid classification of objects and activities.

Similarly, systems such as Israel's Lavender programme analyze communica-

tion patterns and social networks to map relationships and assign relevance scores based on proximity to known actors.

These capabilities demonstrate how surveillance is evolving from observation to interpretation. The concern is not only the amount of data being collected, but the increasing ability to process it in real time and generate actionable outputs.

The revelations of NSA documents by [Edward Snowden](#) exposed the scale at which data could be collected and analyzed without public awareness. At that time, around 2013, often referred to as the Snowden era, surveillance largely followed a sequence: data was collected, then analyzed, sometimes with limited automation, and the results were passed to human decision-makers who remained responsible for final actions.

What is changing now is not the existence of this system, but its speed and its role in decision-making. With the integration of artificial intelligence, data from multiple sources, including communications, imagery, and live feeds, can be processed and interpreted in near real time. Instead of simply informing human analysis, these systems increasingly contribute to identifying patterns, highlighting potential targets, and supporting operational decisions.

This raises a deeper concern. As the Pentagon's pressure on [Anthropic](#) to loosen safeguards suggests, there is a growing interest in expanding the role of AI within these processes. The question is

no longer only about access to data, but about how far automation should extend within the decision chain.

Even within the industry, concerns have been raised about the unpredictability of such systems. [Alex Karp](#) has pointed to the complexity of deploying AI in high-stakes environments, where speed and scale may outpace full human understanding. While AI can compress processes that once took days into seconds, the challenge lies in ensuring that faster decisions do not come at the cost of accuracy or responsibility.

Africa, more than many other regions, has limited control over the systems its citizens are connected to. As more Africans become integrated into global digital platforms, many of the same companies previously linked to large-scale data collection, such as Google, Meta (Facebook, WhatsApp, and Instagram), and X.

The question of control becomes more significant. These platforms operate across borders, yet the data they collect may be stored and processed in jurisdictions beyond the reach of African governments and users.

At the same time, many African governments are investing heavily in so-called “smart city” technologies and AI-enabled surveillance systems, often sourced from foreign providers, mainly [Chinese companies](#). These systems are presented as tools for security and development, but they have also raised concerns about their potential use in monitoring activists, journalists, and political opposition. In such cases, questions not only about how data is collected, but also where it is stored, how it is processed, and who ultimately has access to it.





**Atar**  
**Sudan in Perspective**

From

**FACTSD**  
FACTS CENTER FOR JOURNALISM

Journalists Working on Sudan,  
anywhere.

---



To receive a pdf copy of Atar magazine,  
you can subscribe via Email or WhatsApp:

[atar@sudanfacts.org](mailto:atar@sudanfacts.org)

+254115438212

     @atarnetwork

[www.atarnetwork.com](http://www.atarnetwork.com)