July 2025 Issue

THE DIGITAL AGENDA Insights

Monthly Newsletter

In This Issue

Digital ID

Digital Lifestyle

Artificial Intelligence

Faith & Religion in the Digital Era

Tech Should Serve Not Control

Welcome to The Digital Agenda Insights Monthly Newsletter

Governments worldwide are rushing to implement national identity systems under the banner of the Global Digital Agenda. What started as simple ID cards has switched into vast databases of permanent biometric markers. What started with fingerprints has rapidly advanced into high-resolution iris scans, packaged as “secure” and “unique identification.”

At the same time, Central Bank Digital Currencies (CBDCs) are being pushed forward, with the National Identification Number (NIN) positioned as the key to every essential service. This is clearly a tightly woven system of surveillance and control, marketed as innovation, but designed to centralise power and limit freedom.

At the Digital Agenda Forum, we believe **the true digital agenda** should serve God’s higher purposes for humanity. Innovation should serve humanity, not rule it.

That’s why the Digital Agenda Insights Newsletter exists, to cut through the noise of relentless digitisation. While the world races ahead without pausing, we slow down to ask: Whose interests are being served? What freedoms are being traded away? With sharp analysis and bold commentary, we uncover the deeper struggles for privacy, dignity, and democratic control.

We value innovation and we spotlight technologies that genuinely ease life without compromising humanity. This is not about rejecting progress, but about insisting on progress with purpose.

Join us in navigating these urgent questions. Through these pages, we invite you to stay awake, stay informed, and stay fully human.

If our work resonates with you, consider partnering with us.

Our Core Values

- **S** **Stewardship**
- **P** **Purpose**
- **A** **Authenticity**
- **D** **Dignity**

Warm regards,

Lilian Agaba Nabwebale

For **Digital Agenda Forum**

POLICY BRIEF

Data Overcollection in Uganda's National ID: Balancing Function and Privacy

Issue Summary

Uganda's National Identification Number (NIN) system has evolved from a basic identifier into a central node for accessing nearly all public and private services. However, the scope of biometric and personal data collected during NIN registration and renewal has significantly expanded, raising constitutional, legal, and ethical concerns.

Current practices violate principles of necessity, proportionality, and purpose limitation as required by Uganda's own Data Protection and Privacy Act (2019).

Key Concerns

1. Excessive Biometric Collection

On top of full demographic data, NIRA collects ten fingerprints, facial images plus iris scans, without publishing a risk-benefit justification.

2. Lack of Legal Safeguards

- No published Data Protection Impact Assessment (DPIA)
- No clear retention, deletion, or purpose-limitation policies
- No opt-out or consent mechanisms for sensitive data
- Undefined access protocols for third-party institutions (banks, telecoms, etc.)

3. Security and Surveillance Risks

- Centralised storage of sensitive data increases the risk of breach
- Function creep enables surveillance, political profiling, and misuse.
- Biometric errors lead to service exclusion, especially for vulnerable groups.

4. Unchecked Powers and Lack of Oversight in NIRA's Data Collection

The current Registration of Persons Act, 2015 grants NIRA sweeping powers to collect and process personal data without clear limits or oversight. Schedule 3, enabled by Sections 55 and 85, lists extensive data categories and allows NIRA to demand "any other information" it deems necessary.

Further, the Minister of Internal Affairs is empowered under Section 85 of the Act to make regulations for the implementation of the Act. Under these powers, the Minister enacted the Registration of Persons Regulations, 2015, which delegate the authority to the NIRA Board to determine what categories of personal data should be collected, stating:

""biometric" includes DNA, fingerprint, eye retina, iris, voice pattern, facial pattern, hand measurements and any other thing as may be determined by the Board;"

This means that enormous discretion over citizens' personal and biometric data is handed to the NIRA Board, without any mandatory public consultation, technical justification, or independent oversight.

Legal Frameworks Breached

1. ***Data Protection and Privacy Act, 2019:*** *Overcollection without consent or necessity*

***2. Constitution of Uganda (Article 27):** Right to privacy compromised*

***3. International Standards (e.g., ID4D, GDPR):** Lack of transparency, redress, or proportionality.*

Policy Recommendations

Short-Term

- Publish the full DPIA before collecting any further biometric data
- Suspend iris scan collection until a legal and scientific justification is provided
- Mandate disclosure of all data-sharing agreements with public and private entities

Medium-Term

- Amend the Registration of Persons Act (ROPA) to restore checks and balances:

To address this, the Act must be amended to:

- Limit the categories of data NIRA is legally permitted to collect, tied to strict necessity for identification only.
- Mandate clear data retention and deletion schedules aligned with global best practices.
- Prohibit the repurposing of collected data for surveillance, profiling, commercial use, or political ends.
- Establish a multi-stakeholder oversight board to improve accountability and transparency. This oversight body should include experts from civil society, technology, law, and academia. Its mandate should include:
  - Reviewing and approving data collection practices
  - Monitoring compliance with legal safeguards.
  - Advising Parliament and the Data Protection Office on risks and reforms.

Long-Term

- Reform and empower the Personal Data Protection Office (PDPO) with independence, budgetary autonomy, and enforcement power. (The PDPO currently operates under NITA-U, which compromises its autonomy. It should be relocated to an independent constitutional or parliamentary body.)
- Enact a standalone Biometric Data Protection Law to:
  - Define and Classify biometric data as high-risk and designate it as a special category of personal data due to its sensitivity and potential for misuse.
  - Introduce consent, opt-out, erasure, and data minimisation rights.

Conclusion

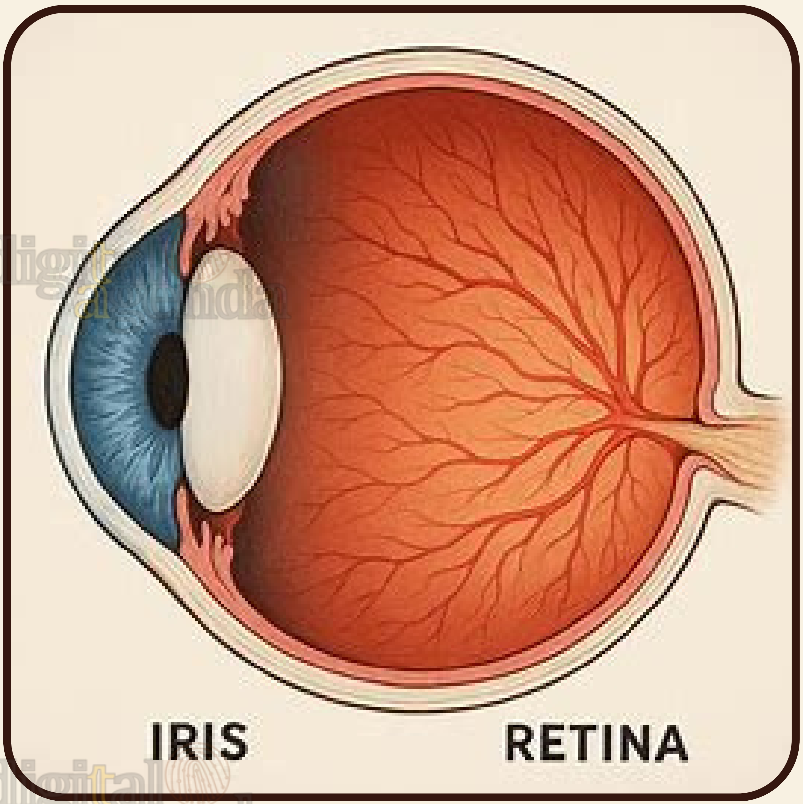
Uganda's ID system must not become a surveillance tool disguised as innovation. Overcollection of personal data not only violates fundamental rights but also erodes public trust in national digital systems. The government must act to realign the NIN system with constitutional protections, international norms, and the dignity of its people.

Prepared by:

Digital Agenda Forum
📩 info@thedigitalagenda.org
🌍 www.thedigitalagenda.org
X/Twitter: @DigitalAgendaT

The hidden cost of iris scans in Uganda's National ID system

Article in the Daily Monitor, Tuesday, July 08, 2025



Imagine if a system could detect your stress levels, emotional triggers, or cognitive weaknesses. Imagine it could infer your political leaning, mental stability, or truthfulness, and monitor when you are likely to resist, comply, or panic.

Now, combine that with facial analysis, voice tone decoding, social media metadata, and National ID systems. You get psychopolitical profiling.

This is a method used by those in power to understand, anticipate, and even influence the behaviour of individuals or entire populations. It can determine who is likely to protest, who is persuadable, and who is considered a "threat".

Whoever controls the biometric system does not just verify you. They own your identity and intent. If you are a citizen, you can be tracked across borders and systems. Even your mood or stress response at checkpoints can be flagged. Your data might be sold or shared with foreign powers or private firms without your knowledge. You could be denied services based on predicted behaviour.

If you are a leader, such as a president, your scans can be stored, copied, and reused. If accessed by hostile insiders or foreign agencies, AI could be trained on your biometric responses to predict how you might react in a crisis, or to manipulate you using tailored psychological tactics. Even your family's biometrics could be used for leverage, coercion, or blackmail.

With the rapid advancement of AI, it is likely that such data could be used to impersonate a person. It could be used to unlock phones, log into bank accounts, or access confidential systems.

We are entering the world of data weaponry. Forget the science fiction you have seen in films. This is a quiet reality, steadily creeping in to control us through biometric systems. We must understand the power involved and expose what is happening in the real world.

Biometric systems, when abused, can turn democracies into digital prisons. The infrastructure is being quietly built. A system of control is emerging, one scan at a time.

We gave away our fingerprints. Now our eyes are needed because, apparently, all ten fingers are no longer readable after five years. It is claimed that iris scans are needed to uniquely identify us. It sounds noble. However, what if iris data does more than just identify us? What if it can also be used to profile, manipulate, and control us?

Scientifically, the iris is not part of the brain, but it is controlled by the autonomic nervous system. This system is closely linked to stress, emotion, attention, and neurocognitive responses. Pupil dilation, for example, is already used in psychology and marketing to measure deception (pupils dilate when lying), arousal, cognitive load (mental effort), and fear or threat response.

AI systems trained on high-resolution iris and eye movement data have started to infer personality traits, emotional states, and risk factors for mental disorders. Deep learning models have reached up to 85 percent accuracy in identifying early Alzheimer's signs from retinal scans, according to a 2021 study in *The Lancet Digital Health.*

> **BIOMETRIC SYSTEMS, WHEN ABUSED, CAN TURN DEMOCRACIES INTO DIGITAL PRISONS. THE INFRASTRUCTURE IS BEING QUIETLY BUILT. A SYSTEM OF CONTROL IS EMERGING, ONE SCAN AT A TIME.**

Your iris scan does not just verify you. It predicts you. It profiles how your brain reacts under pressure, fear, or stress. It estimates your "threat level", your "obedience index", and even your potential to resist. When AI meets your iris scan, it becomes a new form of control. This is the path we are on when biometric data is fed into AI systems trained on behavioural psychology and neurological datasets.

In China's smart surveillance state for example, facial recognition combined with gait analysis and mood detection is used to score behaviour and predict "untrustworthy" actions. AI models flag individuals based on stress signals, microexpressions, and surveillance history, including participation in protests or religious gatherings.

In Israel, emotion-detection AI firms such as Corsight claim to detect intent, arousal, and deception through facial and eye analysis. These tools are used at airports and checkpoints.

In the United Kingdom, the NHS and

DeepMind use eye scans to detect signs of neurological degeneration. The data is held by Google's DeepMind, raising ethical concerns about future profiling power.

Is predictive governance the future we want for our nation? If not, then we must not open the door to it by allowing the unchecked overcollection of unchangeable personal information through the National ID registration process.

In Uganda, the National Identification and Registration Authority (NIRA) is conducting a mass National ID renewal exercise. This now includes iris scans, reportedly because some Ugandans no longer have readable fingerprints. Does this truly justify subjecting the entire population to such an intrusive process?

Where is the assessment that NIRA conducted to reach this conclusion, and where are the supporting figures? NIRA has not clearly explained how it arrived at this decision. Yet, it has made iris scans mandatory for all citizens, regardless of whether their fingerprints are readable. What is the real purpose behind this?

We must also remember that Uganda issues an expiring National ID. Does this mean that by the time each ID expires, the fingerprints of the entire population will also have expired? This sounds like someone buying everything in a shop, whether they will use it or not.

Why is NIRA not handling this on a case-by-case basis? When is it determined that a person's fingerprints have failed? This only becomes apparent when they try to access a service. So far, the only known instance that requires fingerprint validation in the National ID, is during SIM card activation, where telecoms use your NIN and fingerprint to retrieve your ID data.

Clearly, biometric use in Uganda is still limited. How many services require biometric readings? Besides, NIRA already has a process that allows individuals to update or change their ID details. If someone's fingerprints are unreadable at the time of seeking a service, they can go to NIRA to update them or provide an alternative form of identification such as an iris scan.

Subjecting the entire population to the collection of such sensitive biometric data is inappropriate, especially given the risks already discussed.

At some point, one begins to wonder; Is this data really being collected for Uganda's benefit, or is someone planning to profit from it? Who actually gains from this massive overcollection of personal data?

Even though NIRA has claimed to be putting cybersecurity measures in place, experiences from other countries show that no system is unhackable. India’s Aadhaar, Argentina’s RENAPER, and the Philippines' voter database were all breached, exposing millions of citizens' personal and biometric data.

Collecting vast amounts of unchangeable biometric data from the entire population increases the risk of a breach by state-level hackers. If high-resolution iris data is linked to names, family details, locations, and records of access to online services, it can be used to track, profile, and predict individual behaviour in deeply invasive ways. It becomes a weapon of mass control.

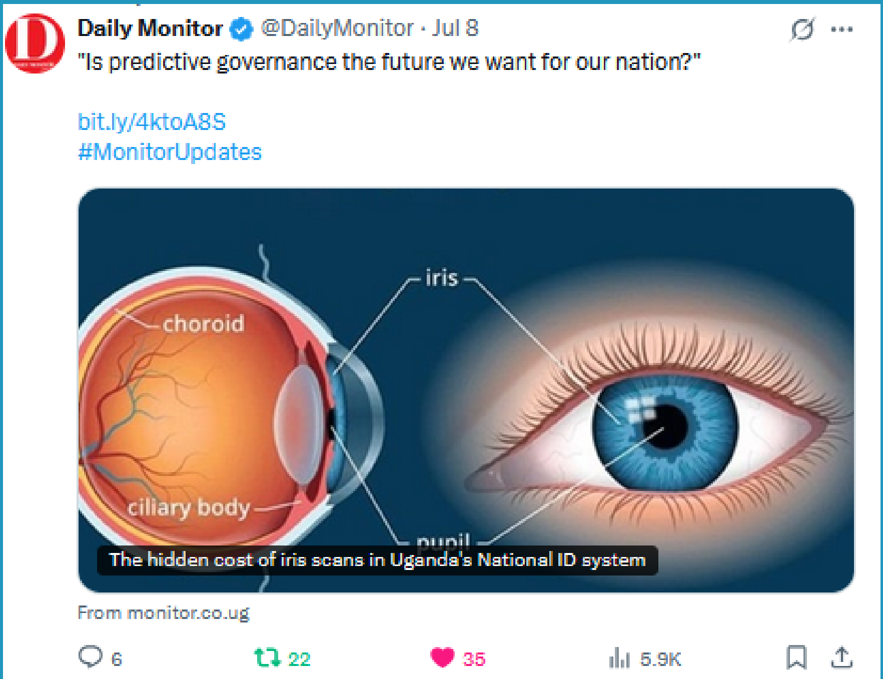
The consequences could be political targeting, intimidation, or psychological manipulation.

If this iris data is exported, it could be used to train AI systems to profile African populations. Uganda risks becoming a testing ground for predictive policing or emotion-driven propaganda.

Is predictive governance the future we want for our nation? If not, then we must not open the door to it by allowing the unchecked overcollection of unchangeable personal information through the National ID registration process. Let iris scans be done on only those without fingerprints.

*By **Lilian Agaba Nabwebale and Stephen Semigabo, Concerned Ugandan Citizens.***

IN THE NEWS



Daily Monitor @DailyMonitor · Jul 8

"Is predictive governance the future we want for our nation?"

bit.ly/4ktoA8S
#MonitorUpdates

The hidden cost of iris scans in Uganda's National ID system

From monitor.co.ug

6 22 35 5.9K

Read article at https://www.monitor.co.ug/uganda/oped/letters/open-letter-to-pdpo-ug-on-national-id-personal-data-risks-in-uganda-5086658

The Illusion of Free Services

*By **Mariagorreti Batenga,** Director at Dopamine Ace Ltd., an incorporator, and a writer*

For years, businesses have made us believe that we are the most important people to them. We have been told “the customer is always right” and “your satisfaction is what matters to us” to make us feel like we matter even more than the business itself. These slogans sound sweet, but the truth is that no business exists without making profit at its core of goals. Your importance ends where their ability to make money from you ends.

It is not different in the technology world. We are given “free” things; free email accounts, free social media, free cloud storage, free Wi-Fi at certain restaurants, even free mobile apps. We sign up thinking these companies are privileged to have us, carrying the cost out of generosity. But the uncomfortable truth is that you are only as important as the value they can squeeze out of you.

The reason these services feel free is because you are not paying in shillings. You are paying with something much more personal; your data, your attention, your behaviour. Every click, every like, every photo upload, and every Google search tells a story about you. And that story is worth money.

Right here in Uganda, examples are everywhere. When you use that “free” Wi-Fi at the cafe in Kampala, your browsing patterns can be tracked and linked to your phone’s unique ID. When you signed up for a social media account, you agreed (probably without reading the terms) that your activity can be monitored and used for targeted ads. Even big names like Gmail have, in the past, scanned emails to target advertising. Facebook tracks your movements online, even when you’re not on Facebook. Some “free” VPN apps have been caught selling browsing history to advertisers.

And it’s not just private companies. Governments are also in the game. NIRA’s mass collection of biometric data; your fingerprints, facial scans, and other personal details is said to be for national identification and service delivery. But in the wrong hands, such data could be used for surveillance, profiling, or even control. Remember, you can change a password, but you can't change your fingerprints.

Free is rarely free especially if it is coming from someone who doesn't even know you personally.

Tech companies and institutions quietly build what's known as a "digital dossier" about you, a detailed profile containing your age, education level, location history, political leanings, spending habits, and even your health concerns. Your activity on one app is linked to others. Your Facebook likes can be tied to your Google searches, your Instagram follows, even your MoMo transactions. This information can be sold to advertisers, insurance companies, and sometimes governments.

The hidden costs are huge. You are never truly anonymous online. Your decisions can be influenced by targeted ads or specific news feeds, shaping your beliefs and purchases without you realizing it. You can be discriminated against like in pricing because an algorithm has profiled you as "willing to pay more". And if hackers breach these databases, your personal information can end up in criminal hands.

We keep using these "free" services because they are convenient, fast, and easy. We tell ourselves, "It's free, so I can't complain". We trust brand names, the government, and assume they will not misuse our data, even though history shows they already have.

Good enough, there are options. You can use paid email services like Proton Mail that don't sell your data. You can support open-source tools where you can see exactly how they work. And you can be more mindful about what you share because once it's out there, you can't take it back.

Free is rarely free especially if it is coming from someone who doesn't even know you personally. No sane business wakes up and says, "You know what? Let's give away our stuff to random strangers for absolutely no reason." There's always a price tag; sometimes it just doesn't come in shillings. In this case, the currency is your personal information, your autonomy, and probably your security. In Uganda, just like everywhere else, the real question isn't whether you should stop using the 'free' services but whether you understand the deal you are making. Because in today's digital world, you're not just using the product, you are the product. And trust me, you're selling at wholesale prices.

WHEN YOUR TV OUTSMARTS YOU: The Screen That Listens

*By **Mariagorreti Batenga,** Director at Dopamine Ace Ltd., an incorporator, and a writer*

As more homes in Uganda proudly mount smart TVs on their walls, there is a shift taking place. It goes beyond streaming Netflix or watching Bukedde in high definition. These shiny internet-connected screens promise more convenience, clearer pictures, and endless entertainment but behind all this, do you ever wonder if your TV could be listening to you without your consent?

Modern Smart TVS are not just viewing devices, they listen too. They come with voice recognition features which help you “talk” to your TV, asking it to change channels, play music, or search for content. However, while you are doing so, the microphone that listens to your commands may also record small clips of what they hear and send them to servers for analysis. These can be private conversations, arguments, prayers, or even business ideas shared during supper.

For example, you might be at home, chatting with friends about a surprise birthday party for one of you. Just moments later, you start seeing YouTube ads for party décor, catering services, video suggestions of new birthday party trends, none of which you had searched for online. This means that your smart TV, had voice activation switched on. The conversation you had triggered background listening. It can feel like a coincidence but even manufacturers have admitted that collected voice data can be used to “improve services,” and this often includes ad targeting.

You can know that your TV may be quietly gathering more than just dust when there is a sudden rise in personalized ad recommendations, slow performance when the microphone is triggered, or when new privacy terms are popping up after software updates.

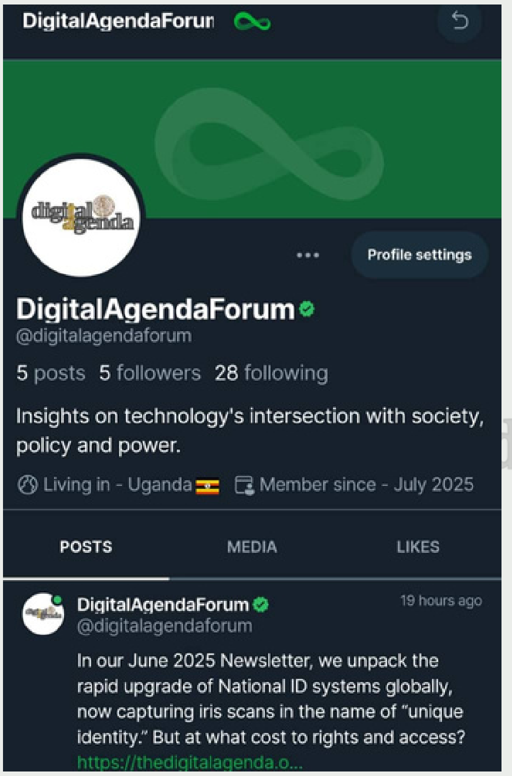
Some users have reported that there are instances where their TVs turn on by themselves or react to nearby conversations with unintended actions. Sadly, it is more likely that these settings are enabled by default.

It is more concerning especially in Uganda where digital literacy is still very low. Only a few customers are taught how to work around privacy settings. Many buyers pick up smart TVs from electronics shops in downtown or from online marketplaces, excited to enjoy the upgrade but ignorant or less concerned about the data exposure risks that come with them. The country's Data Protection and Privacy Act (2019) is supposed to protect people's personal data, but it has not kept up with how fast technology is changing. Many Ugandans don't know their rights or how to speak up when devices invade their privacy.

Smart technology is not evil in itself, but when it is smarter than its users, the imbalance becomes dangerous. We must approach every innovation not just with excitement but also with wisdom.

So, before you sit back to enjoy the evening news or your favourite show, take a moment to review your TV's privacy settings. Ask yourself, is the screen looking at you too? And even more important, could it be listening to what you're saying?

Digital Agenda Forum is on DopaNite



DigitalAgendaForun

Profile settings

DigitalAgendaForum
@digitalagendaforum

5 posts 5 followers 28 following

Insights on technology's intersection with society, policy and power.

Living in - Uganda 🇺🇬 Member since - July 2025

POSTS MEDIA LIKES

DigitalAgendaForum @digitalagendaforum 19 hours ago

In our June 2025 Newsletter, we unpack the rapid upgrade of National ID systems globally, now capturing iris scans in the name of "unique identity." But at what cost to rights and access?
https://thedigitalagenda.o...

Have you created your account today on DopaNite?

AI Can Remix, But Humans Bring the Real Ideas

*By **Lilian Agaba Nabwebale,** Information Scientist*

Artificial Intelligence is now everywhere. It writes text, makes pictures, creates music and videos that fill the internet. Because it works so fast and so well, many people are asking whether AI can actually create something truly new, or whether it is only repeating what humans have already made.

The truth is that AI can produce things that feel new. It can join ideas from many different subjects in ways that surprise us. For example, scientists at DeepMind built a system called AlphaFold that predicted the shapes of millions of proteins, something that would have taken researchers many years. In mathematics, AI has pointed out connections between different areas of study that experts later confirmed. In art and music, AI can generate work that seems original because it mixes styles in unusual ways.

Even with all this, AI cannot create knowledge on its own. It does not watch the world, run experiments or live human lives. It lacks the real experience. Let us simply say that AI is reported speech. It cannot decide if something is true or false. Every new piece it produces comes from material that people have already created. Without a steady supply of new human research, stories, and experiences, AI will eventually only repeat itself.

This is why the future of knowledge is at risk if humans stop creating. At first, AI would still look impressive and helpful. Gradually, mistakes would grow, all its content would start to sound the same, and the freshness of new ideas would fade. After many years, AI would no longer reflect the real world. It would only reflect itself.

A simple way to picture this is to think of a chef and a farm. AI is like the chef, able to cook endless meals, but depends on farmers, to grow new ingredients. As long as the farms keep producing, the chef can make new dishes. If the farms stop, the chef will only have the same old ingredients, and every meal will begin to taste the same.

So, AI can look creative, but it is humans who bring in the real, fresh knowledge. The best future is not where AI replaces people, but where it works alongside them. People keep discovering and creating, and AI helps make those discoveries easier to share, connect, and build upon.

Increased Deception in the Digital Age

*By **Lilian Agaba Nabwebale,** Information Scientist and Minister of the Gospel*

Technology is all around us. Artificial intelligence, social media, and countless digital platforms shape how we work, learn, and even worship. These tools bring amazing opportunities. They make communication easier, connect communities across the globe, and provide access to knowledge and learning that was once impossible. AI can generate helpful content, and digital platforms allow people to share ideas and faith in ways that were unimaginable just a few decades ago.

However, with all these advances, the Digital Age has also opened the door to deception like never before. AI now produces huge amounts of content, from news articles to social media posts and educational material. Much of it looks real but is completely artificial. The Bible warns us about this kind of deception. In 2 Corinthians 11:14 it says that "Satan himself masquerades as an angel of light." In a world where algorithms can make anything appear true, discernment has never been more critical. Technology can bring convenience and connection, but it can also encourage pride, greed, and dependence on human systems instead of God.

Believers have a clear responsibility. Technology should help us live out our faith, not replace it. Even at their best, digital tools need the guidance of spiritual wisdom. Prophet Elvis Mbonye's prophecy of Silicon Valley collapse reminds us that even the most powerful human innovations are not more powerful than God.

https://www.prophetelvis.com/here-is-the-prophecy-silicon-valley-collapse

He warned on where our reliance should be, whether in Silicon Valley or in God. The rise of AI content shows that human tools cannot secure truth or protect society. Technology can fail, but faith endures.

We must be careful, especially when raising children. Technology can educate and entertain, but it cannot take the place of faith, moral teaching, and the personal guidance that shapes character and wisdom. Children cannot learn integrity, compassion, or discernment from screens or algorithms. They learn these qualities through relationships, example, and the guidance of scripture.

In this age of growing digital deception, the message is simple. Use technology wisely and keep your life and your children's upbringing rooted in faith. Even Silicon Valley, a symbol of human achievement, is not beyond failure. True wisdom and protection come from God. Believers must stay vigilant, discerning, and committed to putting faith first instead of relying on technology.

FOR MORE FROM THE DIGITAL AGENDA FORUM

FOLLOW US ON X

@DigitalAgendaT

Following

Digital Agenda

@DigitalAgendaT

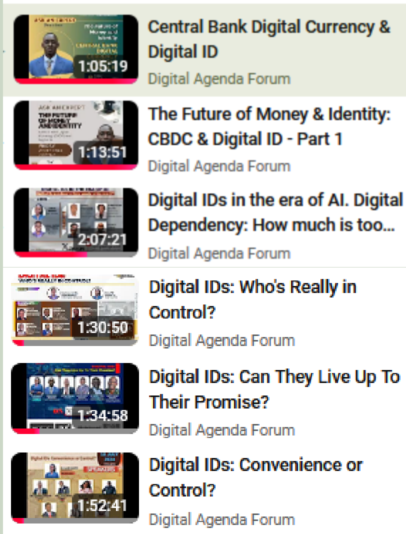
Insights on developments in the Tech industry

thedigitalagenda.org Joined July 2024

196 Following 232 Followers

at https://www.youtube.com/@DigitalAgendaT

Subscribe to our YouTube Channel



1:05:19 Central Bank Digital Currency & Digital ID
Digital Agenda Forum

1:13:51 The Future of Money & Identity: CBDC & Digital ID - Part 1
Digital Agenda Forum

2:07:21 Digital IDs in the era of AI. Digital Dependency: How much is too...
Digital Agenda Forum

1:30:50 Digital IDs: Who's Really in Control?
Digital Agenda Forum

1:34:58 Digital IDs: Can They Live Up To Their Promise?
Digital Agenda Forum

1:52:41 Digital IDs: Convenience or Control?
Digital Agenda Forum

Follow us on TikTok

@digitalagendat

Visit our Website at

www.thedigitalagenda.org

LinkedIn at digital-agenda-forum

Radio interviews on the digital agenda!
www.thedigitalagenda.org/radio

This is a publication of the Digital Agenda Forum.

Contact Us

For further inquiries and information

Digital Agenda Forum
📍 Munyonyo, Kampala, UG
📞+256 782 408607
📧 *info@thedigitalagenda.org*
✉ P.O BOX 172431, Kampala
🌍 www.thedigitalagenda.org