

THE DIGITAL AGENDA

— MONTHLY NEWSLETTER —

Insights

In This Issue

Digital IDs

03 THE YOUTH ARE SPEAKING:
Their Take on Digital IDs

07 UGANDA'S NEW TAX LAW: Your
National ID Will Now Be Your Tax ID

Digital Learning

09 RFK JR.'S PHONE BAN DEBATE:
Beyond Health Risks, Should
Children Have Smartphones in
Schools?

11 DIGITAL AGENT: Protecting
Uganda's Young Minds

Digital Lifestyle

12 Are You Being Programmed, Or
Are You Programming Your Life?

Cybersecurity and Privacy

14 CYBERSECURITY: No One is
Immune!

16 You Are Sharing Your Secrets
With The World! Your Prompts With
AI

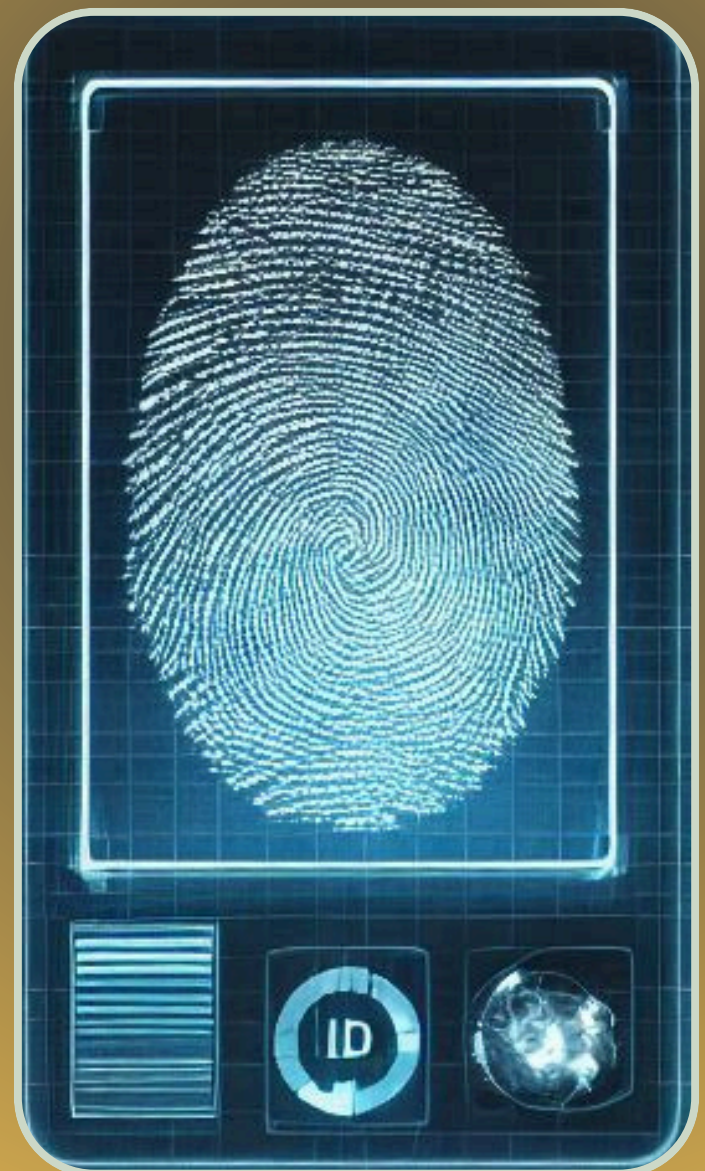
Faith & Religion in the Digital Era

18 IS TECHNOLOGY BAD OR GOOD?
Your Role As A Child Of God

Digital Tech Innovation

19 Harnessing AI Beyond Chatting
and Prompts?

20 Showcasing Digital Tech Innovators



Welcome to *The Digital Agenda Insights* - Monthly Newsletter

The talk today is one of a Digital Agenda. Digital ID has been placed at the centre of every service.

Healthcare = Digital ID

Financial Services = Digital ID

Food and Sustainability = Digital ID

Travel and Mobility = Digital ID

Humanitarian Response = Digital ID

E-commerce = Digital ID

Social Platforms = Digital ID

E-Government = Digital ID

Telecommunications = Digital ID

Employment and Workforce Management = Digital ID

Education and E-Learning = Digital ID

Energy and Utilities Access = Digital ID

Smart Cities and IoT Integration = Digital ID

Voting and Digital Democracy = Digital ID

Law Enforcement and Border Security = Digital ID

The concern is, where is this leading? Though sold as a matter of convenience and security, is it truly about that, or is it paving the way for centralised control?

At the Digital Agenda Forum, we scrutinise this global push of centralisation of identity and challenge any agenda that threatens to strip away privacy, rights, and dignity.

This is why ***The Digital Agenda Insights Newsletter*** brings you thought-provoking perspectives on the rapidly evolving digital world. Our aim is to spark critical thinking, encourage deeper questioning, and inspire informed action.

Together, we can shape innovation and policy to uphold privacy, transparency, and accountability, ensuring that technology serves not control.

Yet we don't stop there. Technology in its purest form is not the problem. It's how it's used that matters. We value innovation and understand how technology can ease life. That's why this platform also celebrates start-ups and innovators who are using tech to drive real progress.

Come with us to navigate these pressing issues through the pages of this newsletter.

If you like our work, don't hesitate to partner with us.

Warm regards,



Team Leader,
Digital Agenda Forum

Our Core Values

S Stewardship

P Purpose

A Authenticity

D Dignity

THE YOUTH ARE SPEAKING: Their Take on Digital IDs

By **DIGITAL AGENDA FORUM**

On 26th March 2025, the Digital Agenda Forum convened an insightful and spirited X Space discussion titled *“The Youth Are Speaking: Their Take on Digital IDs.”* This session uniquely centred the voices of youth – not just as users of technology, but also as builders, analysts, and advocates critically engaging with digital identification systems. The conversation explored whether digital IDs foster inclusion or deepen exclusion, particularly for marginalised populations.

The discussion featured a multidisciplinary youth panel:

- **Asha Wandulu** – Policy Analyst, CEO of Ashalumi Governance Network
- **Steven Bongomin** – Data Scientist and Youth Leader
- **Moses Businge** – Software Engineer and Technologist
- **Shanice Naisenya** – Lawyer and Certified Data Privacy Professional
- **Lynn Edinance Olepus** – Lawyer and Human Rights Advocate

1. Do Digital IDs Foster Inclusion or Deepen Exclusion?

Asha Wandulu began with a powerful reflection:

“When your identity is tied to a system you don’t trust or can’t even navigate, inclusion becomes a hollow promise.”

She questioned the assumption that digital IDs are inherently inclusive.

Drawing examples from India’s Aadhaar and Kenya’s Huduma Namba, she explained how biometric failures disproportionately affect manual labourers and elderly citizens, ultimately denying them basic services like healthcare and food subsidies.

Asha warned that centralised systems often “concentrate power in the hands of governments or private entities,” which can lead to surveillance and exclusion, especially of marginalised groups.

2. Are Digital IDs a Necessity for Development?

Responding to whether digital IDs are essential for achieving SDG 16.9, Asha argued:

“Meaningful development has happened for centuries without digital IDs.”

She cited historical examples like post-WWII Europe and Japan’s economic recovery using paper-based systems. Asha advocated for “community registries, paper certificates, and SMS-based systems” as viable alternatives, especially in Sub-Saharan Africa where digital infrastructure is still lacking.

She proposed blockchain-based self-sovereign identity systems and local-level documentation backed by trusted community leaders as safer, more inclusive solutions.

3. Challenges in Underserved Communities

Steven Bongomin, speaking from a remote area in Gulu, Uganda and frequently interrupted by network issues, highlighted poor infrastructure and limited access as major challenges.

"There's a digital divide; access divide, skill divide, and usage divide."

Steven stated that many youths in rural areas lack the smartphones, documentation, and digital literacy required to navigate these systems. He warned of exclusion and political misuse:

"Such centralised IDs give governments access to all your information, which can lead to surveillance or political persecution."

He questioned the push for digital IDs by global organisations, describing them as a "foreign agenda," and added:

"Digital ID isn't a pressing issue for Uganda's youth; education, healthcare, and roads are."

4. Vulnerability to Hacking and Surveillance

Moses Businge, from a technical standpoint, emphasised how digital IDs are inherently vulnerable:

"Whatever is online is really vulnerable to hacking."

He explained that once biometric data like fingerprints or facial scans are compromised, they cannot be changed, unlike passwords.

"Hackers only need to breach the system once to access all your personal data."

He also warned of mass surveillance and manipulation:

"A company or government could know where you are, what you're doing... that puts you at risk."

5. Consequences of System Failure

Moses provided scenarios of real-world harm:

"If you need emergency healthcare, and the system is down, you can die."

He likened it to a mobile money or banking outage, but on a national scale:

"Just imagine hundreds of thousands of people being locked out of vital services."

He also noted how disabilities or ageing could render biometric IDs unusable over time.

6. Government and Corporate Overreach

Shanice Naisinya from Nairobi, Kenya, addressed legal and privacy concerns:

"A centralised digital ID definitely gives governments and corporations too much control."

She referenced Kenya's Maisha Namba rollout, where data protection concerns were ignored:

"There were no data protection impact assessments... public trust was eroded."

She described how marginalised communities like the Kenyan Somalis and Nubians were disproportionately affected, with the digital ID rollout becoming a "revenue stream rather than a right."

7. Risks and Safeguards

Shanice highlighted key data risks: *Privacy violations, Mass surveillance, Exclusion, Cyberattacks, and Data misuse.*

She recommended:

- Strengthening data protection laws
- Independent oversight
- Practising data minimisation (“only collect what you need”)
- Ensuring purpose limitation (“use data only for the stated purpose”)

“Digital IDs can have benefits, but not with the current centralised models,” she concluded.

8. Faith and Human Dignity and Digital ID systems

Lynn Edinace Olepus addressed the spiritual and philosophical implications of digital identification systems. Speaking candidly from a Christian perspective, she raised theological concerns about how digital IDs may undermine the dignity and divine worth of human beings.

“We as humans are created in the image or likeness of God... when we get into the place of digital IDs, a lot more of our worth and freedom as humans is taken away.”

She emphasised that reducing one's identity to a biometric or ID number: *“Strips us of the autonomy we get to have as individuals... because every other thing about me is narrowed down to a fingerprint or face scan.”*

This, she argued, clashes with the scriptural understanding of human identity as being rich, multifaceted, and sacred.

9. The Prophetic Voice in the Digital Age

Lynn went on to reference a Ugandan prophetic voice, Prophet Elvis Mbonye, highlighting his earlier

prophecies that she believes are unfolding today:

“There's a man of God in this nation, Prophet Elvis Mbonye, who actually prophesied years ago about a global lockdown... and it happened in 2020 with COVID.”

She continued:

“He also spoke about the collapse of Silicon Valley, and if you've been observing the recent technological disruptions, it's clear those words are not in vain.”

Lynn suggested that the rise of digital surveillance, identity reduction, and centralised control had been foretold from a spiritual standpoint, and that Christians must pay attention to what the Spirit of God is saying through prophetic voices:

“We can't ignore that God, through His prophets, gives us direction... and some of these things we're seeing today are a fulfilment of that.”

She encouraged listeners, particularly people of faith, to remain vigilant and spiritually discerning:

“Yes, technology is advancing, but we must ask, does it align with God's will for how we live, how we govern, and how we identify ourselves?”

Her contribution framed digital ID as not just a legal or political issue, but a spiritual matter that challenges Christians to think deeply about sovereignty, trust, and freedom.

Recommendations

Concerning the implementation of Digital ID systems, the following came out as the recommendations.

- Adopt inclusive, decentralised digital ID models that account for

- Prioritise digital literacy and access before implementing mandatory digital ID systems.
- Strengthen legal and regulatory frameworks to ensure privacy, transparency, and accountability.
- Engage youth and grassroots voices in policymaking and system design.
- Explore alternatives to biometric dependency, such as zero-knowledge proofs and non-digital identity solutions.

Call to Action from the Youth Panel

- **To policymakers and development agencies:** Do not frame digital IDs as a one-size-fits-all solution. Reimagine inclusion beyond technological access; prioritise equity, accountability, and dignity. Avoid exporting systems that don't work for the local context.
- **To governments and national planners:** Close the digital divide before enforcing digital identity systems. Ensure that youth in rural areas have the infrastructure, literacy, and documentation required to meaningfully participate. Focus first on education, roads, and healthcare before digital ambitions.
- **To software engineers, developers, and tech institutions:** Acknowledge that digital systems can be hacked, manipulated, or misused. Build secure, decentralised alternatives that safeguard human identity. Remember: ethical design is as important as technical skill.


- **To fellow citizens, especially the youth:** Speak up. Get involved. The law is still in motion. Participate in policy-making, consultations, and civic conversations. Don't leave decisions about your data and identity to people who don't understand the digital world you live in.
- **To people of faith, spiritual leaders, and believers:** Be vigilant. Assess the spiritual and moral implications of digital control. Don't surrender your divine identity to systems that treat you as a number. Trust prophetic insight. Remember: faith must still lead, even in the digital age.

Conclusion

The youth panellists were clear: while digital IDs can offer convenience, the risks, especially for marginalised groups, are severe and under-addressed. They called for alternative systems grounded in community trust, local realities, and strong privacy safeguards.

There was consensus that digital transformation should not come at the cost of human dignity, access, and autonomy.

It was concluded that **“The future may be digital, but it must also be just.”**

Find the recorded full discussion on our **YouTube Channel** at <https://bit.ly/Youth-On-Digital-IDs> or on  at <https://x.com/DigitalAgendaT>

UGANDA'S NEW TAX LAW: Your National ID Will Now Be Your Tax ID

By **DIGITAL AGENDA FORUM**



Registration Authority under the Registration of Persons Act, in the case of an individual
(b) a registration number issued by the Uganda Registration Services Bureau, in the case of a person who is a non-individual
(c) a tax identification number issued by a foreign tax authority with whom Uganda has a tax treaty or agreement for the exchange of information

🧠 What Does That Mean?

The government of Uganda is changing how it identifies taxpayers. In a new law recently tabled before Parliament, ***the Tax Procedures Code (Amendment) Bill, 2025***, one of the biggest changes is that your National Identification Number (NIN) – the number on your National ID – will now serve as your Tax Identification Number (TIN).

📋 What the Law Actually Says

Here is what the law states in black and white:

📌 Clause 2: Amendment of Section 4 of the Principal Act

◆ Section 4 – Tax Identification Number

(1) For tax purposes, the following shall be used as tax identification numbers
(a) a national identification number issued by the National Identification

If you are a Ugandan citizen, your National ID number is now your tax number too. That means:

- You will not need to apply separately for a TIN
- The government can track who is paying taxes using your national ID

If you are a company, your registration number from URSB will be used instead. And if you are a foreigner with a tax agreement in Uganda, your foreign-issued TIN applies.

📌 Other Key Points in the Law

- ◆ Local authorities cannot give you business licences or register documents unless you have an NIN or registration number:
- (4) No government body shall issue a business licence unless the applicant has a national ID or a

registration number.

(5) No documents needing stamp duty will be accepted without these identification numbers

So if you are trying to start a business, register land, or apply for anything formal – and you do not have a National ID – you will hit a wall.

📌 **Clause 3: Tax Penalties Waived If You Pay Up Early**

◆ Section 47B – Waiver of Interest and Penalty

(1) Any interest and penalty outstanding as at 30th June 2024 shall be waived where the taxpayer pays the principal tax by 30th June 2026

This means if you owe URA taxes and have not paid, you can clear just the principal amount (the original tax) and avoid penalties and interest, but only if you pay by mid-2026.

🧬 **The Bigger Picture: Your Data, Biometrics, and Access to Services**

This shift to a single identification system does not end with taxes.

“The National ID is the backbone of our identification framework, from healthcare to banking, education to utilities, accessing health services, it will soon be the key to accessing everything.” ~ Brig Gen Johnson

Namanya Abaho, Commissioner of Citizenship and Passport Control, Ministry of Internal Affairs

This was said at a stakeholders’ meeting in Entebbe attended by leaders from NIRA, district security officers, and other government

representatives from across the Kampala Metropolitan area.

The National ID already contains your biometrics – fingerprint, photo, and soon even DNA and iris scans. The aim? ***To centralise all access to services – from getting medication to opening a bank account – under one number: your NIN.***

❓ **Is This Like China’s Social Credit System?**

Not exactly, but it is getting closer. In China, a person’s ID links to everything: income, spending, online behaviour, legal record, and even how polite you are. If you fall short, you could be banned from travel, denied loans, or locked out of services.

Uganda’s new setup, where access to nearly all services is tied to a centralised ID system that also tracks your tax compliance, mirrors the infrastructure of such systems.

It might start with taxes... but where does it stop?

🤔 **Final Thoughts**

This law sounds simple, but it has huge implications:

- The National ID becomes more than just identification – it is now tied to your economic, legal, and social life.
- Without it, you might not be able to open a business, register property, go to school, or access healthcare.
- The government gains a central view of your life – where you work, what you earn, and what you own.

Is this efficiency? Control? Or both? That is a question Ugandans will need to ask – and answer – very soon.

RFK JR.'S PHONE BAN DEBATE: Beyond Health Risks, Should Children Have Smartphones in Schools?

By **MARIAGORRETI BATENGA**, Director at Dopamine Ace Ltd., an incorporator and a writer.

Robert F. Kennedy Jr., the United States secretary of Health and Human services, has been advocating for banning phones in schools in the U.S., arguing that they can cause "neurological damage to kids" and "even cancer" due to electromagnetic radiation. While some share his concerns about the potential health risks, others argue that the scientific evidence is not strong enough to support these claims. Many reputable health organizations, including the National Cancer Institute, the Food and Drug Administration, and the Environmental Protection Agency, have also found no conclusive evidence that cellphone use is linked to cancer or other health problems. But even if we set aside the argument about health risks, should children ever be allowed to have phones in school or even at all?

In Uganda, banning such devices in schools including radios has been the norm for years now. At some point, I felt like this was a form of oppression, cutting children off from information beyond the classroom. However, after growing up and seeing the reality of the media, I strongly agree that these devices are a major distraction, especially for children who still need guidance in focusing on what is important.

Even outside of school, access to smartphones, without restriction is a



serious danger to children. Sadly, even adults struggle with the effects of smartphone addiction—so do children even stand a chance? Smartphones are not only addictive but also consume so much of our attention that we neglect vital tasks. People miss meals, let food burn, push work to extreme deadlines, and even destroy relationships because they are too absorbed in their screens. Ironically, these same adults, despite witnessing the negative impact of these smartphones in their own lives, argue that children should be allowed to have and use them in classrooms.

Some [parents and schools] argue that smartphones are necessary for research and learning, which is true. With Uganda's new curriculum, the

long-standing ban on phones in schools might soon be lifted for the same reason. However, this one positive doesn't weigh as much compared to the many negative effects of phone use among children. But is this one reason even worth exposing children to the unfiltered information on the internet? Should a child who has not yet developed critical thinking skills be left to navigate this grand pool of information including harmful content? If research means accessing information in this manner, perhaps there should be an age limit on when students can begin independent research, when they are mature enough to process and make informed decisions. Is this one reason enough for teachers to struggle for students' attention against the distraction of smartphones? Is it worth creating even another insecurity among students whose families cannot afford expensive devices? Should this become yet another reason for ridicule based on what kind of phone a child bears?

Should a child who has not yet developed critical thinking skills be left to navigate this grand pool of information including harmful content?

Another common argument from parents pushing for smartphones in schools is that they need to communicate with their children. However, why must this be done through smartphones when simpler, affordable communication devices designed purposely for calls exist?

If smartphones are trusted to parent and educate children, then why do we have schools and teachers at all? To battle constantly with the internet for a child's attention and deal with behaviors picked from there?

As education costs rise, why aren't schools investing in controlled research infrastructure on campus, similar to traditional libraries? This would filter student access to information and reduce unnecessary competition and comparison. Schools can also set up dedicated communication channels for students and parents without relying on smartphones in classrooms or on school premises.

The push for smartphones in schools is unnecessary, as all the concerns raised have simple solutions. Many parents advocating for this are simply engaging in parental politics, using their children as pawns. They are avoiding their responsibilities, and hoping that devices will do the parenting for them, just as has become the norm of late.

Before cancer or any neurological illness ever reaches these children, these basic but rampant negative effects of smartphone addiction and the information accessed there on, will have already caught up with them. While critics argue against RFK Jr.'s reasoning on health risks, the more immediate and obvious dangers that they are conveniently choosing not to see shouldn't be ignored.

DIGITAL AGENT: Protecting Uganda's Young Minds

By DEZY PAUL LUBOWA, Elementary School Teacher and Soccer Coach



Digital Agents are parents, educators, and policymakers actively working to protect and guide children in their use of digital technology, ensuring that digital tools are used responsibly and safely in schools and homes.

As a digital agent you are the force or presence in the digital space that promotes awareness, sets boundaries, and prevents harm to young users navigating the opportunities and risks of the digital world.

While technology can enhance education, it also poses risks to children's learning, development, and wellbeing. As we embrace the digital agenda in schools, we must watch out for excessive screen time, digital distractions, and their impact on academic and emotional growth.

I. Excessive Screen Time can lead to digital addiction, reduced attention spans, and diminished face-to-face interaction skills. It may also contribute to sleep disorders and physical health issues.

II. Online Harassment

(Cyberbullying) can cause deep emotional distress, affecting a child's self-esteem, mental health, and academic performance. Many victims suffer in silence.

III. Unfiltered Access to Information

may expose children to misinformation, confusion, and reduced critical thinking. There is also the risk of encountering explicit or harmful content online.

IV. Over-reliance on Digital

Communication can weaken interpersonal skills and emotional intelligence, leaving children less equipped for real-world social interaction and conflict resolution.

What Can Be Done?

Schools and parents must collaborate to create safe digital environments. Investing in filtered research tools, digital literacy, and clear communication can help children benefit from technology without harm.

Let us commit to being proactive Digital Agents, championing balance, protection, and purpose in the digital age.

Are You Being Programmed, Or Are You Programming Your Life?

By **EVELYNE NAIKOB**, *Governance and Strategy Specialist*

Most of us don't realize how often we scroll. We're on our devices when we're bored, when we want to relax, or when we feel the need to connect. Sometimes, we're not even sure why. That's the thing about media and tech in their current form. They don't just serve our needs. They shape them.



Modern media is not neutral. It delivers narratives. Every video, post, headline, and notification is engineered to influence how we think, what we value, and what we feel. Emotion is currency in the attention economy. The more charged a piece of content is, the more likely it is to spread.

Modern media is not neutral. It delivers narratives.

If you've watched *The Social Dilemma*, this will sound familiar. The documentary reveals how social media algorithms are not simply responding to our behavior. They are actively directing it. Built by some of the sharp minds in tech from Silicon Valley, these systems are designed to increase engagement, often by tapping into our most reactive emotions. The longer we stay on a platform, the more money it makes. The more predictable we become, the more valuable we are to advertisers.

There's a quote in the film that captures it well: "If you're not paying for the product, you are the product."

And that should make us pause. Why do we believe what we believe? Who decides what gets amplified, and what doesn't? How much of what we call truth or culture has actually been crafted by invisible systems designed to keep us watching?

Not long ago, I watched an interview where someone was asked to name the most cringeworthy trend they'd seen on TikTok. She mentioned a viral prank where parents ask their child to fetch tissue. When the child returns, the parent 'accidentally' smears chocolate on them, pretending it's something else. Some kids scream. Some even faint. Millions have watched.

That's more than just poor taste. It reflects a deeper issue. How does something like this rise to popularity? What kind of system rewards that kind of content? And why are we so comfortable calling it entertainment?

This isn't an argument against tech. It's a reminder of what tech can become when it's left unchecked. Tools are shaped by the hands that wield them. If the algorithm can reward humiliation, it can also reward integrity. If it can amplify outrage, it can also amplify wisdom and Godly values. But that shift won't happen on its own.

Some people are starting to push back. When Donald Trump found himself silenced on major platforms back in 2020, he didn't just complain. He created Truth Social. Whether or not you support him, the principle stands. He took the initiative. He built

a space for his message.

We may not all launch platforms, but we can still be intentional with the influence we have. We can pause before reposting, question before believing, and create with purpose rather than just reacting to trends. If we don't, we risk becoming conduits for systems we don't even fully understand.

Media is shaping society. Not just for us, but through us. And if we're going to participate in this space, let's do it consciously. Let's use these tools to build, not just scroll.

Because in the end, it's not about how advanced the technology is but who it serves. And make no mistake; it can only be either God or Satan. Nothing in between, no matter how casual some content might seem. It us up to us to awake while using it.

BE A PANELIST

Join Our Webinars and Town Hall Panel

Are you an expert or enthusiast in digital technology? The Digital Agenda Forum welcomes knowledgeable individuals (**Technology Experts, Policy Makers, Legal Experts, Regulatory Bodies, Academics and Researchers, Civil Society Representatives, International Organisations, Ethics Experts, Industry Associations and Data Protection Authorities**) to join our panel discussions during our online Webinars and Town Halls. Our focus is on exploring the latest advancements in digital tech, with a key emphasis on digital IDs.

As a panelist, you'll have the opportunity to share your insights, engage with thought leaders, and contribute to shaping a balanced and inclusive digital future.



Interested in being a panelist?
Reach us on e-mail at
info@thedigitalagenda.org

CYBERSECURITY: No One is Immune!

By **DIGITAL AGENDA FORUM**

Several cyberattacks occurred globally in March 2025, impacting critical infrastructure, government agencies, and private companies. Here are some notable incidents:

Ukraine: Cyberattack on National Railway System

In late March 2025, Ukraine's state railway operator, Ukrzaliznytsia, suffered a large-scale cyberattack that disrupted its IT systems. The attack was first reported on March 23, leading to the suspension of online ticket sales and forcing passengers to purchase tickets on-site or onboard. As of April 9, approximately half of the affected IT services had been restored. Ukrainian security officials suspect Russian involvement, given the ongoing conflict between the two countries.

Poland: Breach at the Polish Space Agency

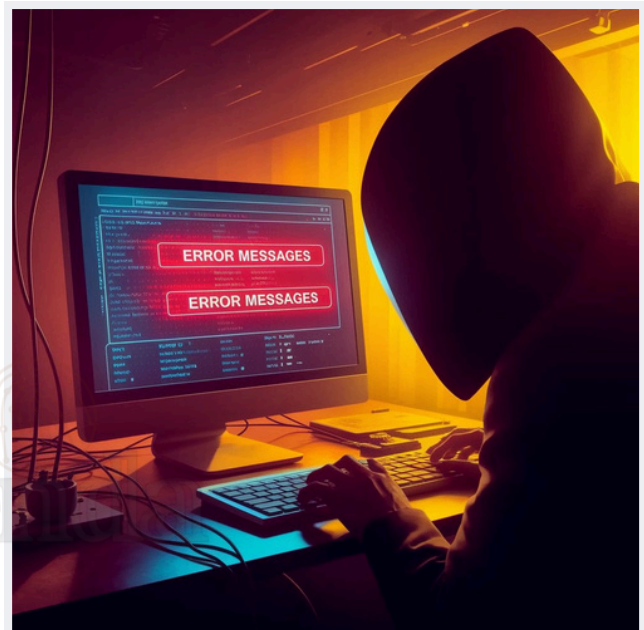
On March 2, 2025, Poland's Minister of Digitalization announced that unauthorized access had been detected in the IT infrastructure of the Polish Space Agency (POLSA). The agency's network was immediately disconnected from the internet to secure data while investigations were conducted. Polish authorities have previously accused Russia of attempting to destabilize the country due to its support for Ukraine.

United Kingdom: NHS Scotland Cyberattack

On March 20, 2025, NHS Scotland reported a major cyber incident that caused network outages across multiple health boards. The attack disrupted clinical systems, leading to delayed patient care and forcing staff to revert to paper-based processes. The incident has been linked to a suspected ransomware group, though official attribution is still pending. Investigations are ongoing with support from the National Cyber Security Centre (NCSC).

United States: Ransomware Attack in Pennsylvania

On March 13, 2025, Union County, Pennsylvania, discovered a ransomware attack on its government systems. Personal information from residents was stolen during the breach. Federal law enforcement was notified, and cybersecurity experts were hired to assist with the recovery process.



HACKER!

Global: DDoS Attack on Social Media Platform X

On March 10, 2025, the social media platform X (formerly Twitter) experienced a massive distributed denial-of-service (DDoS) attack, causing widespread outages. The hacktivist group Dark Storm Team claimed responsibility for the attack. Initial reports suggested the attack originated from IP addresses in the "Ukraine area," but cybersecurity experts have questioned this attribution.

Ireland: FBI Warns of Medusa Ransomware Threat

In March 2025, the FBI issued an urgent alert to Irish Gmail and Outlook users regarding a significant threat from the Medusa ransomware. The malware had obtained data from over 300 victims, particularly in critical infrastructure sectors like hospitals, schools, and large enterprises. Users were advised to

implement two-factor authentication, keep operating systems updated, and activate spam filters to mitigate the threat.

These incidents emphasise the increasing frequency and sophistication of cyberattacks worldwide, highlighting the need for robust cybersecurity measures across all sectors.

One click can cost a nation. Cybersecurity isn't optional, it's critical. Stay alert, stay secure.

**If one email can
cripple a lab, one
breach in a
centralised digital
ID system could
expose an entire
nation—proceed
with caution.**



PARTNER WITH US **Join Us in Shaping the Future of Digital Technology!**

At the Digital Agenda Forum, we believe in a digital future that protects individual rights, upholds ethical standards, and serves the common good. As a platform for dialogue, collaboration, and innovation, we are dedicated to bringing together visionaries, experts, and organizations committed to making technology work for everyone.

We invite you to partner with us as we explore the evolving landscape of digital technology. Together, we can lead conversations that matter, influence policy decisions, and create solutions that empower communities around the globe.

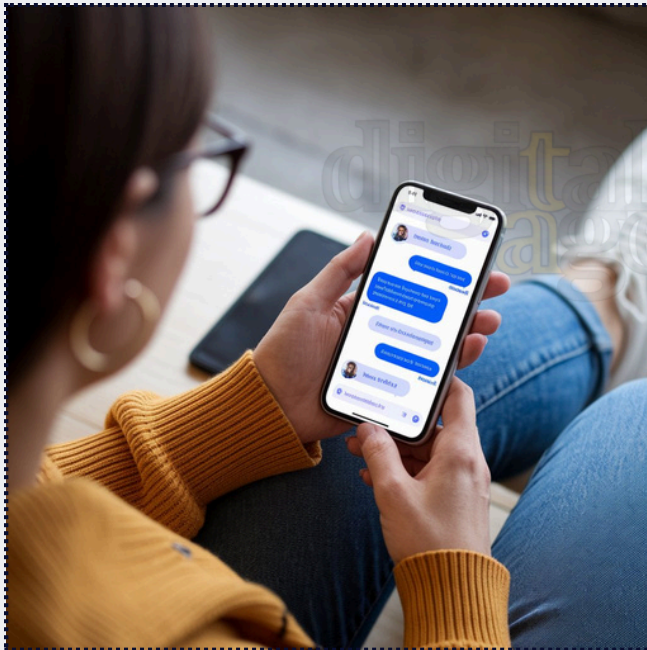
Let's work hand in hand to ensure that digital progress goes beyond innovation and truly aligns with human values. Whether you're a business, a nonprofit, a policymaker, or a tech enthusiast, there's a place for you at the Digital Agenda Forum. Partner with us today and be part of a movement that's shaping a digital future for all!

Like what we do? Partner with us.

Reach us on e-mail at
info@thedigitalagenda.org

You Are Sharing Your Secrets With The World! Your Prompts With AI

By Lilian Agaba Nabwebale, Information Scientist



Imagine this. You'd never walk up to a stranger on the street and confess your deepest, darkest secret. So why would you share it with an AI like ChatGPT?

If you're like most people, you might assume your prompts just vanish after you hit "send". But the truth is far more complex, and a bit unsettling.

Every time you type something into ChatGPT (or other AI tools like Claude, Groq, or DeepSeek), your words don't stay on your device. They are sent over the internet to powerful servers, usually hosted by companies like Amazon, Microsoft or Google. There, they're analysed, processed, and sometimes stored.

Even if a company says your data is deleted, there's usually a period when it still exists on their systems. During that time, your input can

potentially be seen, logged, or even used to train future versions of the model.

Some AI providers allow staff to review conversations, especially ones that are flagged for inappropriate or suspicious content. Others use real user data (yes, your prompts) to improve their systems – unless you take the extra step to opt out.

Take DeepSeek, for example. It's a fast-growing AI model developed in China. Unlike ChatGPT or Claude, DeepSeek often connects to Baidu – China's version of Google – during your chat. That means your data could be passing through Chinese servers, under Chinese data laws. And those laws aren't exactly known for putting users' privacy or consent first.

So even if you're asking innocent questions, your words may be stored, analysed, and used without your knowledge.

And it's not just overseas platforms doing this. Meta, the company behind Facebook and Instagram, trained its latest AI model, Llama 3, using millions of books and academic papers – many of which were illegally downloaded from sites like LibGen and Z-Library.

Reports say Meta's internal documents admitted they did this because of competition with OpenAI

They knew it was risky. They did it anyway.

One author even found their own book in the training set, used without permission, without payment.

You might be thinking, “Well, I trust Google. I trust Apple.” But even the most secure companies are run by people – and people make mistakes.

Think back to the private photos of celebrities like Jennifer Lawrence and Jeff Bezos being leaked. Most of those leaks weren’t high-tech hacks. They happened because of weak passwords, poor security settings, or insiders with access.

And what about governments? In the UK, officials recently asked Apple to weaken one of its strongest encryption features so that law enforcement could access user data more easily. That’s right. Even in a

democracy, your privacy can still be watered down.

So what should you do? You don’t have to quit AI completely. Just treat it like a public space.

If you wouldn’t post it on Facebook, Reddit, or X (formerly Twitter), don’t type it into ChatGPT. Avoid sharing sensitive personal info, private thoughts, or anything you wouldn’t want resurfacing.

AI tools are clever, helpful, and often entertaining. But they’re not your diary. They’re not your therapist. They’re not your best friend.

Once your words enter the system, you no longer control where they go, how long they stay, or who might see them.

AI is here to stay. But your right to privacy still matters. Take it seriously.

digital agenda
DIGITAL AGENDA FORUM

ON X SPACES
@DigitalAgendaT

WEDNESDAY
MARCH 26, 2025
7-9 PM EAT

**THE YOUTH ARE SPEAKING:
Their Take On Digital IDs**

CLAIRE BABIRYE
Data Scientist
MODERATOR

PANELISTS

 Lynn Edinace Olepus Advocate - Youth and Human Rights	 Asha Wandulu Policy Analyst, Founder and CEO - Ashalumi Governance Network	 Steven Bongomin Data Scientist, Youth Leader & Advocate	 Moses Businge Software Engineer, Photographer and Designer	 Shanice Naisenya Data Protection Specialist
---	--	---	--	---

www.thedigitalagenda.org

Did you miss this discussion?

Find the recording on our YouTube Channel at <https://bit.ly/Youth-On-Digital-IDs>

Or at <https://x.com/DigitalAgendaT>

IS TECHNOLOGY BAD OR GOOD? Your Role As A Child Of God

Technology itself isn't inherently bad or good. It's a tool, and how it's used is what really matters.

☀️ **The Good**

- Connection: Lets people stay in touch across the world.
- Access to Information: Anyone with a smartphone and internet can learn almost anything.
- Healthcare: Tech has revolutionised diagnosis, treatment, and research.
- Productivity: Makes work faster and more efficient in almost every field.

⚠️ **The Not-So-Good**

- Addiction & Mental Health: Social media and constant notifications can affect well-being.
- Job Displacement: Automation can replace certain types of work.
- Surveillance & Privacy: Tech can be used to track and exploit people.
- Misinformation: Fake news spreads faster than ever before.

It is like asking if a knife is bad. It depends if you're using it to cook or to harm someone. Same with tech: it's all about who's in control, what values guide its use, and how society regulates and adapts to it.

What are the children of God have to do in this aspect?

When we talk about technology and the responsibilities of the children of God, we are stepping into a space where faith meets innovation. Here are some ways children of God can approach it:

🙏 **1. Use Technology to Glorify God**

- Share truth, love, and hope online.

- Create or support tech that uplifts humanity, whether it's education, health, justice, or creativity.
- Be a light on the internet, just as in the real world. (Matthew 5:14-16)

🌱 **2. Guard Your Heart and Mind**

- Not all content is healthy. Some tech platforms encourage comparison, lust, greed, or distraction.
- Philippians 4:8 gives a filter: whatever is true, noble, right, pure, lovely, think about those things.

💡 **3. Discernment is Key**

- Not every trend is worth following. Christians are called to test everything (1 Thessalonians 5:21).
- Ask: Does this tech draw me closer to God or pull me away?

🤝 **4. Use It to Serve Others**

- Tech can help feed the hungry, reach the lost, teach the Word, or support the brokenhearted.
- From Bible apps to online ministries to platforms for advocacy, tech can be a tool for serious Kingdom work.

🗣️ **5. Advocate for Ethical Tech**

- Children of God can speak into how technology is built and used: with justice, dignity, and love.
- Stand up for privacy, digital rights, and truth.

In Short:

- Be intentional. Be prayerful. Be a witness even in the digital world.
- Jesus didn't have Instagram, but if He walked the earth today, He would probably use tech to reach hearts, not followers.

Harnessing AI Beyond Chatting and Prompts?

By Lilian Agaba Nabwebale, Information Scientist

When people hear "Artificial Intelligence," they often think of chatbots. But in Uganda, AI is doing much more from detecting crop diseases to protecting wildlife and improving healthcare. It's transforming lives in unexpected ways.

1. Healthcare Heroes: Using AI to Track Outbreaks

In Uganda, the Ministry of Health has tapped into AI to make disease surveillance smarter and faster. With tools like mTrac, a mobile-based health reporting system, data from local clinics is analysed in real-time. AI algorithms help spot unusual trends, like a sudden spike in malaria cases in a specific district and trigger alerts so health teams can respond quickly. It's not just about data collection; it's about turning that data into lifesaving action.

2. Smart Farming with Your Smartphone

Enter EzyAgric, a Ugandan agri-tech solution bringing AI to the hands of farmers. Using a simple smartphone app, farmers can snap pictures of their crops. AI analyses the images and detects diseases, pests, or nutrient deficiencies, then recommends treatments or best practices. What used to take weeks and a visit from an expert now takes seconds. It's like having an agronomist in your pocket.

3. Saving Wildlife with Smart Collars

Poaching and human-wildlife conflict threaten Uganda's precious wildlife. But AI is helping protect it. In parks like Queen Elizabeth National Park, smart GPS collars fitted on elephants and

lions track their movements. AI algorithms monitor patterns, detect stress signals or unusual movement, and alert rangers to potential poaching risks or danger to nearby communities. It's a high-tech guardian angel for the wild.

4. Credit Without Collateral: AI in FinTech

In a country where traditional banking often excludes the informal sector, AI is opening financial doors. Companies like Numida and Ensibuuko use AI to assess loan eligibility by analysing alternative data, such as mobile money usage and SMS patterns, rather than relying on formal credit histories. The result? More Ugandans, especially youth and women, can access capital to grow their businesses. Some platforms even use AI-powered chatbots in local languages to improve financial literacy and guide borrowers.

5. Language Translation

Not everyone in Uganda uses English fluently and AI researchers know this. At Makerere University, language technology projects are training AI to understand and respond in Luganda. This means voice-based digital tools could soon help more Ugandans access services, search the web, or even interact with government systems, all in their native tongue. It's a step towards digital inclusion for all.

AI in Uganda isn't sci-fi. It is rooted, wild, and transforming society. It is not just chatbots; it is solving real problems. How will you harness AI? The possibilities are endless. Stop chatting. Start building.

SHOWCASING DIGITAL TECH INNOVATORS



DopaNite

A social media space where the only limit is your imagination.

sign up on
Dopanite.com

What Makes DopaNite Unique

- wallet
- Earn from posts
- Earn from affiliates
- Polls
- Elite community
- Chat
- 12 languages
- Record Posts
- Public Posting



chatshop

Do your shopping within WhatsApp

Start a chat with
+256-707-765683

Are you a vendor? Sign up
@ chatshopapp.com

What would you like to buy now

- Fashion and Clothing
- Books and Education
- Food and Beverages
- Jewelry and Watches
- Toys, Games, and Hobbies
- Sports and Outdoor Gear

Continue

FOR MORE FROM THE DIGITAL AGENDA FORUM

FOLLOW US ON X



Visit our YouTube Channel
at
<https://www.youtube.com/@DigitalAgendaT>

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

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

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

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

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

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

Follow us on

 **TikTok**

@digitalagendat

Visit our Website at
www.thedigitalagenda.org


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

