



The role of privacy frameworks in building trust for digital identity services

Understanding end-user attitudes towards mobile services linked to their digital identity

End-User Research

Summary of findings, Conducted by Basis Research, 2019



The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences..

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: [@GSMA](https://twitter.com/GSMA)



The GSMA Digital Identity Programme is uniquely positioned to play a key role in advocating and raising awareness of the opportunity of mobile-enabled digital identity and life-enhancing services. Our programme works with mobile operators, governments and the development community to demonstrate the opportunities, address the barriers and highlight the value of mobile as an enabler of digital identification.

For more information, please visit the GSMA Digital Identity website at www.gsma.com/digitalidentity

Follow GSMA Mobile for Development on Twitter: [@GSMAM4d](https://twitter.com/GSMAM4d)

A four-market qualitative-led study, exploring two central GSMA hypotheses around privacy and trust

GSMA hypothesis

*That the presence of legal frameworks around privacy and data protection **increases***

1

Consumer trust in the digital ecosystem

(i.e. the belief that individuals' personal data will not be exploited by governments or private sector)

2

And, therefore: consumer willingness to access digital services linked to their identity or personal details

This study juxtaposed

- Two countries 'with' (comprehensive) privacy frameworks
- Two countries 'without' (comprehensive) privacy frameworks



Ghana



Zambia



Rwanda



Mozambique

WITH

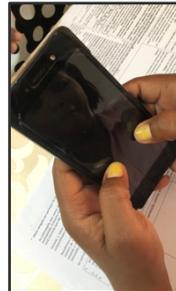
comprehensive legal frameworks around data protection

WITHOUT

comprehensive legal frameworks around data protection

to determine if these hypotheses were correct

Research incorporated face-to-face qualitative discussions, light-touch quantitative survey, expert engagement and desk research



Methodology (Ghana, Zambia, Mozambique, Rwanda)

- **Desk research;**
- **Four x 45-minute Key Informant Interviews (KIIs)**
 - With academics and legal experts with expertise in the field of data protection and privacy, freefound by Basis.
- **Face-to-face qualitative research**
 - Five x in-depth interviews and six x focus discussion groups per market;
 - Participants recruited in urban and rural locations;
 - Total sample size of 212 participants.
- **Light-touch quantitative research**
 - Completed by each participant prior to qualitative IDI or focus group.



Quantitative is based on small sample sizes (n=50 per market), and is not nationally representative; results should therefore be shared with caution

CONTENTS

- 6 Key findings
- 8 Context: legal background
- 10 Comparing countries 'with' and 'without' legal frameworks
- 14 Universal truths
- 25 Differences: 'with' and 'without'
- 31 Summary: similarities and differences
- 34 Conclusions
- 37 Role of data protection law
- 40 Implications for MNOs
- 43 Appendix

APPENDIX

- Full recruitment specification
- Market summaries
- Additional qualitative and quantitative data
- Individual end-user case studies

Key findings

A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. On the left, a man in a light-colored shawl carries a child on his back. In the center, a smaller child walks. On the right, another person is walking. The background shows a dense cluster of makeshift buildings with corrugated metal roofs. Numerous power lines crisscross the sky. The overall atmosphere is one of poverty and overcrowding.

Key findings

Mobile users' attitudes to trust, privacy and identity-linked services are often independent from the presence or absence of a comprehensive data protection/privacy law - although some slight differences do exist

1

Those in markets with legal frameworks may feel more informed, supported, or confident, in managing privacy

2

Willingness to access identity-linked services is universally high, if they offer a clear benefit and are provided by a sufficiently trusted entity

Market context



Looking at legal provision around data protection across markets

In 'with' countries

WITH

Ghana: Comprehensive data protection framework

- The Data Protection Act of 2012 provides a comprehensive legal framework for the management of user data and protection of individuals' privacy;
- It incorporates a new, independent regulatory body: the Data Protection Commission;
- Recognised as being in line with African Union Cyber Security and Data Protection Convention (2014) data protection guidelines.

Zambia: basics in place, but yet to meet international standards

- Communications are governed under the Electronic Communications and Transactions Act (2009) which provides numerous fundamental protections for consumers and citizens with regard to their data, including regulation;
- ...although no dedicated, comprehensive data protection law currently exists;
- A new Data Protection Bill has been proposed in June 2018 and agreed by the government, to protect against privacy intrusion;
- However this was rejected by the opposition and remains unratified.

In 'without' countries

WITHOUT

Mozambique: Rudimentary data protection framework

- Data protection forms only three articles of the Electronic Transactions Law (of 9 January, 2017);
- No independent regulator is described and there are no precise definitions around parties who handle data (e.g.: procesor de dados is used as the term for both data processor and controller);
- **From a KII legal insider:** *"[The law] is not very sophisticated in terms of what should be considered the right of the data subjects... It doesn't say what is compliant and what isn't."*

Rwanda: extensive legal framework, but criticised as 'open to abuse'

- The right to privacy is enshrined in the Rwandan constitution, and ICT Law no.24/2016 purports to create a robust regulatory framework protecting ICT users' personal data and privacy;
- However, the law has been criticised by international observers for the search and surveillance powers granted to authorities without the need for judicial review, and for allowing the government to intercept and penalise communications that are "detrimental to national sovereignty", "indecent" or cause "annoyance" or "anxiety";
- The regulator enforcing this law, the Rwandan Utilities Regulatory Authority (RURA) is not an independent body but is an organ of government, which critics suggested is increasing potential for conflicts of interest;
- **From a KII legal insider:** *"The laws are not enough to guarantee privacy; you can have all the laws you want, but if you do not enforce them, then they will not have an impact."*

In Ghana and Zambia: legal frameworks outline key DP principles (transparency, accuracy, etc); roles of data processor vs. controller; regulation. In Rwanda and Mozambique: laws are looser and/or subject to weaker oversight, and therefore open to abuse and difficult to enforce.



Comparing countries 'with' and
'without' legal frameworks

Our approach to comparing ‘with’ and ‘without’ markets – and what it revealed

The grounds for comparison

Five broad areas:

1. Awareness / perceptions of **laws and legal redress**;
2. Attitudes to **privacy**;
3. Openness to **data sharing** via / relating to mobile;
4. **Trust** (especially in MNOs); and
5. Openness to **identity-linked digital services**.

The rules of ‘difference’

- Any difference must be visible across both ‘with’ markets, versus both ‘without’ markets
 - Otherwise: it could be a market-specific anomaly on either side.
- Differences may emerge from qualitative or quantitative findings.

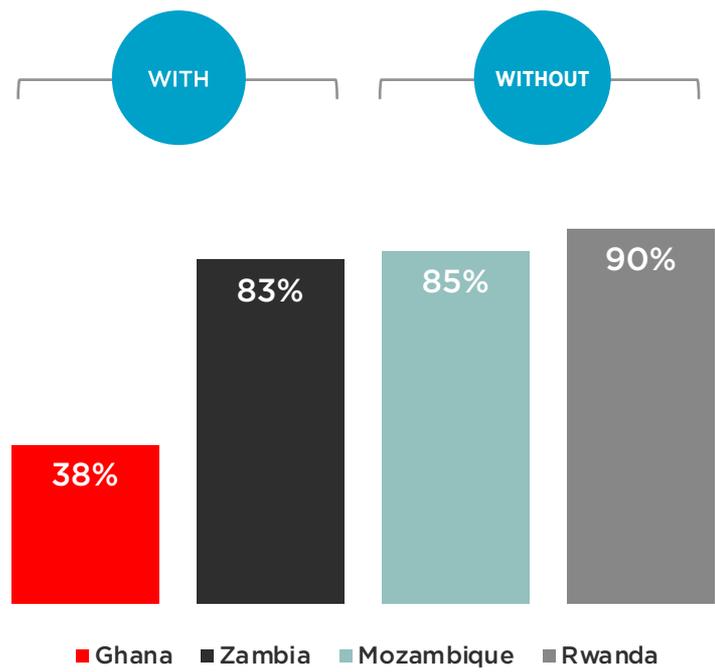
Based on these parameters

- Across these five areas, many similarities exist between countries ‘with’ and ‘without’ privacy law
 - We’ll refer to these as ‘universal truths’, and will highlight them first.
- There are clear differences between different populations within markets, and some marked differences between markets... but not **consistently** along ‘with’ vs. ‘without’ lines; yet
- Differences do exist between ‘with’ / ‘without’
 - These are nuances of comfort, willingness or perception – but together they do indicate a slightly different perspective.

The first thing to note: citizens are not necessarily aware of their country's legal status – particularly those in countries 'without' comprehensive privacy laws

Many end-users did not correctly identify whether data privacy laws existed in their country

Do you think these laws exist in your country?
I know / think they exist



How to explain this?
and what does it mean?



Q2. In other countries, laws such as the following exist. Do you think any of these exist in this country?
Base: all answering in each market (n=varies, min=49*). *Caution low base.

Digging into these beliefs, and their impact on this study

Why do end-users believe what they do?

- None had clear, concrete understanding of local data protection law
 - Those in Ghana were particularly doubtful of such laws existing, because they had not heard of them.
- Nonetheless: in ‘without’ markets, most believe that they are protected by this type of law
 - Both ‘without’ markets had recently-introduced (although limited) data protection laws;
 - These may have generated some news or PR coverage, especially in Rwanda, which has raised awareness around the laws that do exist;
 - End-users do not understand data/privacy issues or law in enough detail to recognise any shortcomings; and
 - Only a handful in Without markets felt that while laws exist, they are vague / never applied.
- Confusion too between data protection law and other laws which protect privacy / identity
 - E.g. around fraud (scamming, identity theft) or defamation (online slander, revenge porn);
 - These crimes use victims’ ‘personal data’, and known to be punished by law; and
 - This was often extrapolated to all abuses of personal data, including by organisations.

“I do not know about such a law.”
male, Ghana

“I don’t know the exact law. But there must be something.”
female, Rwanda

What could this mean?

- Most (in this sample) living in countries without comprehensive legal frameworks believed that they were protected;
- And over a third of those in markets ‘with’ comprehensive laws did not know about them; so
- Consumers cannot reliably describe to us the impact of law on their own levels of trust; but
- We can compare attitudes and behaviours in ‘with’ and ‘without’ – to assess if presence of law, even when not acknowledged, has any impact.

A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. On the left, a man in a light-colored wrap walks towards the right. In the center, a child walks away from the camera. On the right, another person walks towards the camera. The background shows a dense cluster of makeshift buildings with corrugated metal roofs. Numerous power lines crisscross the sky. The overall atmosphere is one of poverty and urban overcrowding.

Universal truths

In all four countries: there was a spectrum of awareness of, and attitudes to, privacy with regard to organisations

This spectrum drives greater differences in attitudes to privacy, within each country, than 'with' vs. 'without' does

privacy-alert



privacy-uninformed

- Much **more aware of the risks of sharing data** with organisations (including via mobile);
- **Higher awareness of digital privacy issues** – e.g. sensitised to breaches; aware of passive data share by their handset; some knowledge of how data is captured by online and social media platforms, etc.;
- More likely to describe **“worrying”** about sharing data with organisations (although not necessarily avoiding doing it).

Who are they?

- More likely to live in urban environments;
- More typically, but not exclusively, male;
- Internet users were often privacy-alert;
- More frequently higher education: students, teachers; and
- Especially common in Ghana.

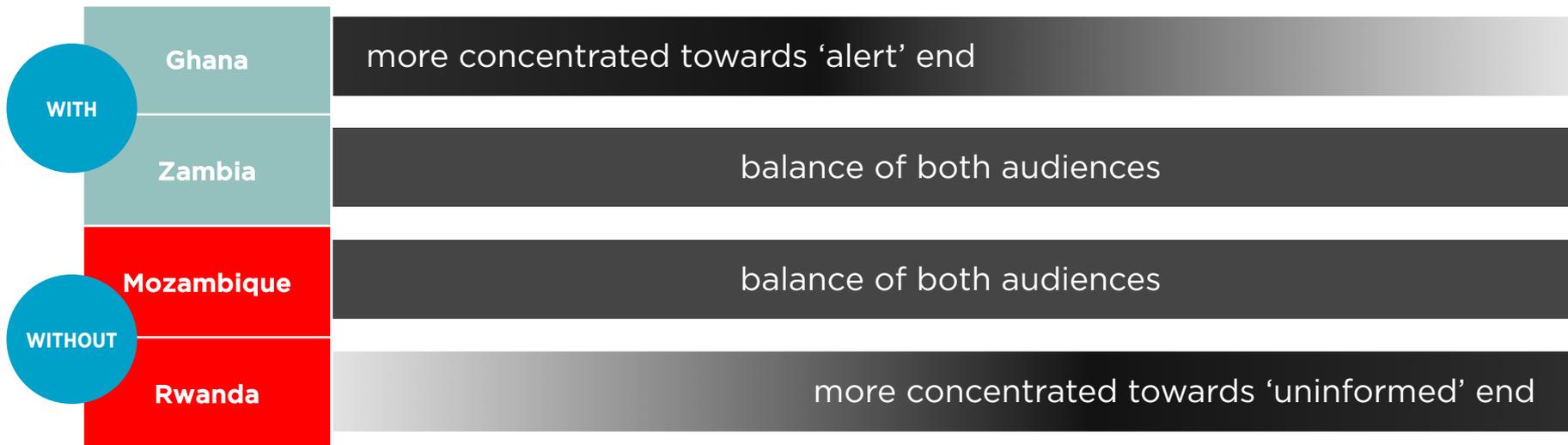
- Much **less aware of, or sensitive to, the risks of sharing data** with organisations (incl. via mobile);
- **Lower awareness of digital privacy issues**; may have had less exposure to ‘horror stories’ around data breaches; unaware of passive data sharing;
- Much less **concerned or worried** about sharing data with any organisation – what’s the risk?

Who are they?

- More likely to live in rural environments;
- More typically, but not exclusively, female;
- More likely to be basic handset / non-internet users;
- Often lower levels of education, or manual jobs; and
- Prevalent in Rwanda.

Based on qualitative: proportions of privacy alert vs. uninformed audiences may vary by market – but the spectrum exists across ‘with’ and ‘without’

privacy-alert  privacy-uninformed



HOWEVER, despite this general awareness of risk: openness to share or access data via, or relating to, mobile was high (in all markets)

If you have, or assuming you had, a smartphone (and cost / literacy were not barriers)

How willing are you, or would you be, to...

	WITH	WITHOUT
Use mobile money	98%	99%
Open a Facebook account	96%	97%
Send WhatsApp messages	96%	98%
Download a new app	97%	95%
Use your mobile for second-factor authentication	91%	97%

no significant differences here between With vs. Without: willingness is universally **high**

Results from: those who have already done this, or are very / slightly willing to

Q1. Let's imagine you own a smartphone, and it is free to do any of the activities below. If you weren't sure how to do any of them, someone could show you how. If so, how willing would you be to do each of the following.

Base: all answering in each market (n=varies, min=49*). Base too low to show scores for some codes in Ghana. *Caution low base.

This is because

Perceived risks and concerns rarely impacted on behaviour

Regardless of country, or presence of laws: the vast majority were content to share personal data if there was a good enough reason to do so.

This is assuming that the data recipient passes a (often sub-conscious, and low) trust threshold

Almost all well-known brands, organisations, even apps and websites achieve this by default.

Often it is enough for an app to simply look respectable / trustworthy.

The data value equation is consistent: if there's a strong benefit to sharing personal data, it consistently outweighs the risks

Disadvantages of sharing or accessing data via / relating to mobile



- **Risks (privacy-alert):** data will escape my control; might create problems for problems later?
- **Nagging discomfort (privacy-alert):** is this the right / sensible thing to do?

Advantages of sharing or accessing personal data via / relating to mobile

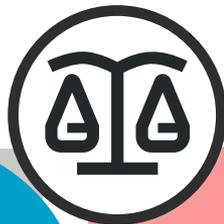
- **Benefit of service use:** I can enjoy services I want to use;
- **Need:** There is no alternative - if I do not give my data, I will not be able to use standard services (transfer money / own a mobile);
- **Convenience / recovery:** if I give correct data to an MNO, it will be easier to recover an account, SIM or device later; and
- **Security, e.g. if registering a SIM:** giving my data to MNO reduces criminals' ability to prosper.

Typically, set aside in favour of the **advantages**

Other enabling factors

- Other people (like me) do this, and have no problem;
- I will be careful with what I share, avoiding anything that I consider especially sensitive / risky.

Illustrating this digital data value equation



“The internet is porous. People can access things, information can land up in unauthorised hands.”

male, Zambia

(Some) awareness and fear of risks of digital data share (amongst privacy-alert)

But benefits of service use take over...

“I’m scared. But I’d rather stick my neck out; if something bad happens, it happens.”

male, Mozambique

“It asks you all these questions and you just want to register properly, to use the service. You don’t question it.”

male, Rwanda

“When you’re signing into WhatsApp, the information... where is it going? We don’t know... we just feel good that we’re opening WhatsApp.”

male, Zambia

“What am I supposed to do? ... if you aren’t on it, you’re missing out!”

female, Ghana

“If everyone else uses the app, nothing bad happens to them, why should it happen to me?”

female, Mozambique

SIM registration is considered in this light: the advantages (rational and emotional) outweigh the disadvantages

“If they say that in order to get a SIM card, we must give our IDs, that’s the way it is. That’s how it’s done throughout the country.”

male, Rwanda

High levels of comfort with KYC protocols on SIM registration

- Few in any country questioned this; it is the procedure in place and should be followed;
- Having a SIM registered in your name evokes security
 - Rationally: if lost, it is much easier to retrieve your phone number or resolve issues;
 - Reduced risk and easier restitution in case of fraud, mobile money theft, improper use of your SIM / number.
- Emotionally too, a sense of properness, ownership and legitimacy – even national pride
 - A sense of doing things “right”: helping in the fight against crime and threats to national security;
 - Several – especially in rural locations – talk about pride at presenting their official ID to register;
 - This can be conflated with showing you’re a citizen of the country, and worthy of services.
- Some expect MNOs to keep their data on file, for easier sign-up to future products, e.g. mobile money.

For those with SIMs registered in others’ names – **none** in our sample cited privacy concerns as their reason for non-registration

Reasons for having a SIM registered in another’s name:

1. **Age limitations:** getting the SIM before they reached the eligible age or registering a SIM in their own name for their children to use’;
2. **Convenience of access:** close friends or family register a SIM in someone else’s name, if it’s easier for them to do so;
3. **Timeliness of access:** to make the most of a time-limited promotion on behalf of someone else (who can’t access a store in time);
4. **Gifting:** if top-up credit and a SIM are a gift to someone else.

Trust varies by scenario, but it is more willingly granted to some entities and people than others

End-user willingness to trust someone with their data is affected by various factors:

what information I am giving

how carefully protected or 'risky' is my information?
If it is money-related, some may be more careful

who I am giving it to

Do I know the company? If to an employee: how 'verifiable'?

the individual's attitudes to privacy

The **privacy-alert** are inclined to be more wary: particularly in urban areas, where breaches of trust are more common

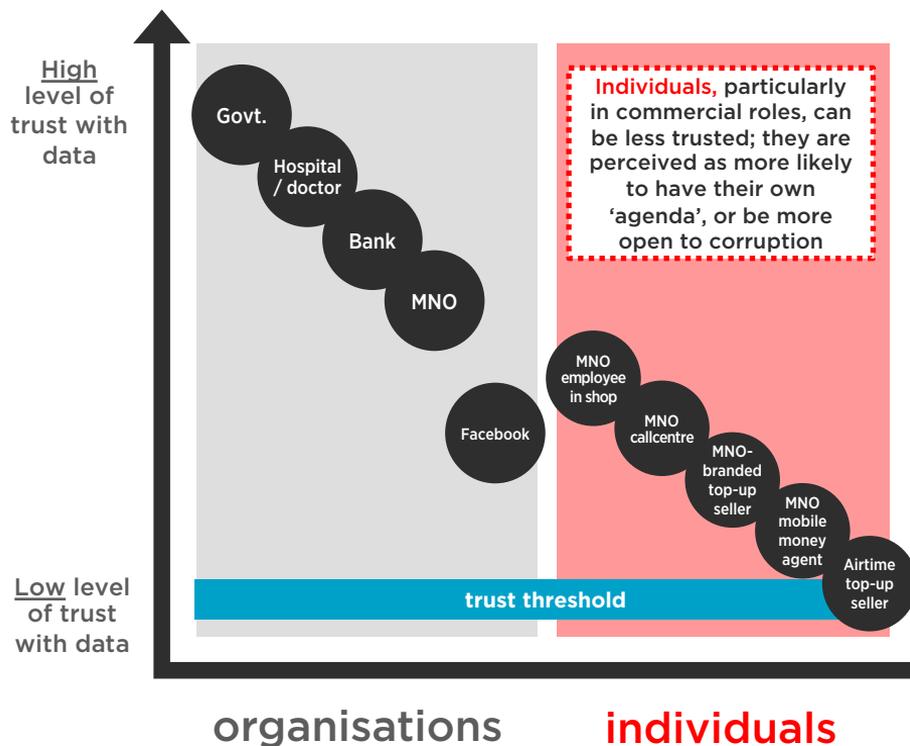
The **privacy-uninformed** are split: some are fearful of what they do not understand, and reticent to trust; others are more naïvely trusting



'Who I will trust' is also based on a number of elements:

- Trust is formed over time – but it can be boosted by:
 - **Past history**: all are more inclined to trust organisations and individuals who have caused no previous (known) breaches, or disappointments;
 - **Transparency**: if consumer data is required, knowing what it will be used for can be reassuring to consumers – e.g. to prevent crime; and
 - **Respectability**: sizeable organisations, which others trust, are seen to be reliable.
- It is reduced by:
 - **Previous bad experience**, especially financial loss;
 - **Negative stories from others, or PR** – although these rarely have fatal impact; and
 - **Conspicuously improper/unofficial third party** – if they do not “look” respectable.
- Again, however: the trust threshold to share data is regularly low;
- End-users are often willing to trust organisations with their data – without necessarily trusting their wider corporate agenda.

Organisations are typically trusted more than individuals – although both are trusted enough to supply data to



As 'official' bodies, government and hospitals are highly trusted with personal data

- They exist to support, and do good for, citizens;
- They're anticipated to have relatively robust training and protocols;
- There's perceived to be limited benefit that employees could derive from deliberate misuse of data in their care; and
- Low awareness of previous data breaches.

Banks are mostly felt to be very secure

- Only a tiny minority who've experienced problems are uncertain.

At organisational level: MNOs are relatively well trusted

- On the whole, at a broader level: MNOs are felt to provide a reliable service to most customers, most of the time;
- And typically, customers trust them to hold their data – especially as they have no choice, if they want to use a phone.

Facebook is lower down the trust scale

- For most, Facebook is a risky place to be (as a user)... but not necessarily because they doubt Facebook's credibility or trustworthiness – just that it is a place inhabited by bad actors, where much data is freely available;
- However, the more privacy-Alert had some reservations – it can feel like more of an unknown, intangible quantity than local companies with physical presence.

Willingness to use identity-linked digital services (including from MNOs) was high – providing there's a benefit to doing so

Now

Huge majority are willing to use digital services which link their identity and mobile number (where available):

- Use mobile money, download a new app, open Facebook account, and send WhatsApp message: greater than **90% are willing** to do this in all markets.

And many are already using identity-linked services:

- Receiving government SMSs about health campaigns, cholera outbreaks (Zambia);
- Linking a mobile number to a government profile, for digital access (Zambia; Rwanda); and
- Linking a mobile number to bank account, for bank updates via SMS (Mozambique).

In future

Almost all would be happy to use more services linking mobile and identity (from MNOs or otherwise), providing there is a clear benefit:

E.g. an MNO-provided 'financial ID profile'* was universally positive

What if MNOs could use mobile money / top-up history, with permission, to offer tailored finance deals?

- In all locations: at least **two-thirds of participants** were immediately willing for their MNO to access this data – and **this increased after more detailed discussion of the benefits**;
- Key benefit: helping me manage my finances better, succeed commercially;
- None expressed concerns** around privacy or the role of MNOs in this capacity: this is data that they'd have anyway, I can see why they need it, and it's in my interests that they use it;
- Some wished that this service could **integrate more data & services**:
 - That this becomes a bigger tool – not just an opportunity to receive a sales offer, but would also help remind of / track repayments later;
 - That 'headlines' of analysis (of their data) are shared with customers – could be interesting and useful to understand one's own behaviours.

* see Appendix for full concept description

A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. On the left, a man in a light-colored wrap walks towards the right. In the center, a child walks away from the camera. On the right, another person walks towards the camera. The background shows a dense cluster of makeshift buildings with corrugated metal roofs. Numerous power lines crisscross the sky. The overall atmosphere is one of poverty and urban overcrowding.

Differences: 'with' and 'without'

There are, however, several differences between ‘with’ and ‘without’ markets

Across the five key areas of exploration, differences are apparent in **four: legal redress, privacy, data sharing, and trust**

These are mostly nuances of comfort, perception or knowledge



WITHOUT

	In countries ‘without’ robust data protection laws
1. Awareness / perceptions of laws and legal redress	<ul style="list-style-type: none"> Less likely to mention telecoms regulators than those in With markets (especially: in urban)
2. Attitudes to privacy	<ul style="list-style-type: none"> Higher belief that conversations may be monitored by the ‘authorities’
3. Openness to data share via / relating to mobile	<ul style="list-style-type: none"> Greater openness to sharing personal data with an MNO (if the MNO offered a service they wanted to use) But: more caution around smaller-scale private organisations that they share personal data with
4. Trust (especially in MNOs)	<ul style="list-style-type: none"> For MNO-enabled ID sign-up: more likely to demand visibly robust, store-based processes (due to trust and security concerns around individual agents)
5. Openness to identity-linked digital services	No visible differences here – high openness in all countries

On legal redress: those in ‘with’ countries more spontaneously described the presence of, and support from, telecoms regulatory bodies

WITH

In Ghana and Zambia

- Especially in urban areas: spontaneous references (albeit from minority) to national telecoms regulators;
- In Ghana: National Communications Authority was mentioned;
- In Zambia: national campaigns around SIM registration recalled from national telecoms regulator, ZICTA*; whom
- Consumers can contact directly with telecoms-related issues; some envisaged reporting MNO data breaches here.

“We were in school in rural areas and they were telling us about ZICTA.”

male, Zambia

“I think I heard something from the National Communications Authority – they had changed the law about something.”

female, Ghana

WITHOUT

In Rwanda and Mozambique

- Many assumed that the government, or departments within it, would be in charge of this space – or (more vaguely) that the police would handle problems;
- But little sense of dedicated focus, or support; or
- The ability for consumers to take telecoms-related personal data problems to them – which would be welcome.

“If that happens, I can accuse someone of a crime, refer to the service provider to find the person who has done the crime.”

male, Rwanda

“There should be an institution or an office we can go to to resolve [data breaches]. These are problems we face on a daily basis.”

male, Mozambique

On openness to sharing personal data: Paradoxically, those in countries ‘without’ comprehensive privacy laws were more willing to share certain personal data...

How willing would you be **to share the following data with an MNO?**

(assuming that you need to do so, to access a service which they’re offering and which you want to use)

	WITH	WITHOUT
Your name	99%	97%
Your photo	78%	88%
Your address	78%	94%
Your children’s names (if you have children)	57%	79%*
Your email address (if you use email)	68%	82%
Your bank account number (if you have one)	34%	80%
Access to your mobile money transaction history (if used)	64%	80%*
Access to your health records	65%	75%

This suggests

Those in ‘without’ countries are less cautious with their data – they’re more willing to supply any personal information requested by an MNO

Results from: those who are very / slightly willing to

Q3. How willing would you be to give your mobile phone network each of the following pieces of information about yourself?

Base: all answering in each market (n=varies, min=46*). *Caution low base.

 = statistically significant difference between both With and both Without markets

 = statistically significant difference by With / Without – BUT heavily driven by Rwanda

However: in ‘without’ countries, more spontaneous mention of needing to check ‘credentials’ before sharing data with smaller companies / individuals

WITH

In Ghana and Zambia

End-users want, and expect, to know who they’re sharing data with

But occasions where this was a problem seemed isolated

WITHOUT

In Rwanda and Mozambique

- Determining that a company or individual is bona fide, and substantial, felt very necessary to many, before sharing information – and could be hard to do;
- Particularly, in relation to smaller entities (i.e. not: government or major corporate brands);
- Heightened awareness of potential for acts of wrongdoing by employees; and
- More references here to instability: individuals and businesses disappearing quickly.

“There are certain organisations I’m very reluctant about. I don’t feel secure. I can’t validate their official status.”

female, Mozambique

“Companies open every day and they close every day.”

female, Mozambique

“Better in the hands of a company. A company will keep it secret, but an individual can publish it.”

Male, Rwanda

In terms of trust: those in ‘without’ countries were more likely to seek extra reassurance, to build on new MNO identity initiatives

Potential MNO-enabled national ID Sign-up was well-received in all four countries

What if MNOs could use their infrastructure to help people sign up for national ID?

- The benefits here are obvious, particularly convenience and accessibility for those in rural areas;
- This would reduce wait and travel times to enroll;
- Calls across countries for clear stamp of government accreditation, and overt government publicity: to show training has been conducted, and that this is an official mandate; however
- Mixed attitudes by ‘with’ / ‘without’, in terms of which MNO touchpoints would be trusted in this capacity.

“There would need to be a partnership, like between the MNOs and the government.”

female, Mozambique

WITHOUT

In Rwanda and Mozambique

- Greater comfort in store-based processes: this feels more robust, with ‘computers’, and a greater likelihood of training / screening being conducted and adhered to;

“They need to be trustworthy and keep the information they receive secure and safe.”

male, Rwanda

“The information would be very vulnerable ...Whereas now it’s just in [the district office], instead it would be in 100 places.”

female, Mozambique

A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. On the left, a man in a light-colored shirt and shorts is walking towards the right. In the middle, a child is walking towards the left. On the right, a woman in a light-colored dress is walking towards the left. The background shows a dense cluster of small, makeshift buildings with corrugated metal roofs. Power lines are visible across the sky. The overall atmosphere is one of poverty and urban overcrowding.

Summary: similarities and differences

Similarities and differences in countries ‘with’ vs. ‘without’ comprehensive privacy laws

	Universal truths	Markets ‘with’ comprehensive data & privacy law	Markets ‘without’ comprehensive data & privacy law
Understanding of relevant legal frameworks	<p>Citizens are unclear about privacy/data protection law – it is conflated with other laws, or assumed to exist when it does not.</p> <p>Especially confusing when laws are in place, but are inadequate, e.g because they are poorly worded or leave loopholes for authorities to exploit.</p>	<p>Marginally higher knowledge, including some awareness of regulators.</p>	<p>Very low knowledge, minimal awareness of regulators’ identity or roles.</p> <p>7 out of 8 believe that they are protected, despite the lack of comprehensive legal frameworks.</p>
Attitudes to personal privacy	<p>Maintaining privacy from ‘other people’ is important to all.</p> <p>Only the more Privacy-alert are sensitive to privacy risks of sharing data with organisations.</p>	<p>Generally believe their communications are private.</p> <p>More conscious of potential risks/disadvantages to sharing personal information publicly on social media platforms (strangers or scammers accessing this).</p>	<p>Likely to believe that authorities monitor their communications, and may take steps to avoid this (e.g. using Whatsapp, which they believe to be more secure).</p> <p>Less informed about the potential risks of social media sharing.</p>
Willingness to share personal data with MNOs	<p>The digital data value equation: if a service is desirable, (and a basic trust threshold is met), concerns more likely to be outweighed by willingness to share personal data to access the desirable service</p>	<p>Slightly less willing to give their personal data to MNOs, especially financial data.</p>	<p>Slightly more willing to give their personal data to MNOs.</p> <p>But more cautious sharing with smaller organisations.</p>
Trust in organisations and individuals	<p>Organisations are generally trusted - government and hospitals are trusted most, but banks and MNOs also rank highly.</p> <p>More doubts around individual representatives of an organisation, who may be prone to corruption/criminality.</p>	<p>Slightly more comfortable providing identity data to mobile agents, who they believe to be endorsed by MNOs.</p>	<p>Slightly less comfortable providing identity data to mobile agents.</p> <p>But still willing to do so in order to access a service.</p>
Openness to identity-linked digital services	<p>Widespread openness to use identity-linked solutions from MNOs.</p> <p>Providing these present obvious customer benefit, most are very happy to provide or allow MNOs to use their data.</p>	<p>Privacy issues never a major factor in this decision – all generally willing to sign up to identity-linked online/digital services.</p>	

How can we summarise those in countries ‘with’ vs. ‘without’ comprehensive privacy laws?



WITH

Those in ‘with’ countries

May be more likely to keep certain elements of data more private.

May have a higher level of trust that regulators will help and support them.

Those in ‘without’ countries

Are more ready to share much of their data with big organisations like MNOs

but: may have more suspicions over smaller bodies

Perceive less support from regulators.

Have a firmer belief that ‘authorities’ are intercepting their communications.



WITHOUT

Conclusions:



From this study: many consumers often do not know, with accuracy, whether data protection laws in their country are comprehensive or not

So we cannot state that laws increase trust in their own right; any impact, if present, is indirect rather than consciously perceived

Furthermore

- X In all markets, citizens have greater or lesser degrees of trust depending on their position on the privacy alert-uninformed spectrum;
- X No difference in willingness to use personal data-linked mobile services between countries 'with' or 'without';
- X End-users in 'without' markets were more likely to share data with MNOs; those in 'with' markets were more cautious;
- X No visible difference in trust in key corporate bodies, across 'with' and 'without'
 - In 'without' countries, slightly lower levels of trust in relation to smaller entities - with regard to foundational ID delivery.

How can we reframe this? in countries where stricter legal frameworks are present

- ✓ There's less apparent fear about 'who I'm sharing my data with';
- ✓ There's higher awareness of regulatory presence in the telecoms space – and a greater sense of closeness to them.

Those in markets with legal frameworks may feel more informed, supported, or confident, in managing privacy

On the basis of this study: the presence of laws does not affect enthusiasm for identity-linked digital services

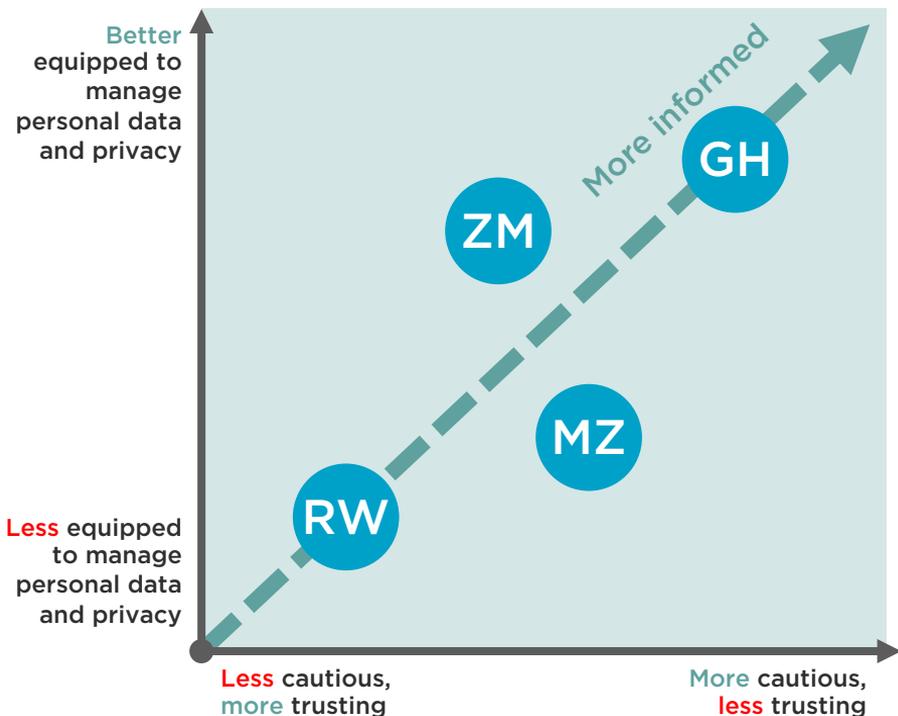
- Openness to use identity-linked mobile services did not differ significantly across countries;
- If tangible benefit is outlined, openness to use is consistently high
 - Providing the reason for sharing data is clear, and it is going to be for personal / the greater good.
- The link between trust and behaviour (with regard to service registration and adoption) is a subtle one
 - End-users were willing to engage with almost all organisations, particularly major local or global brands, as they are trusted 'enough'.
- This is true in all four countries, for major organisations and brands – including MNOs
 - Only slightly more sensitivity around data which MNOs have less 'right' to, or purpose for (e.g. bank accounts, or children's information).

Willingness to access identity-linked services is high, if they propose a clear benefit and are provided by a (sufficiently) trusted entity

A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. The person on the left is carrying a bag. The person in the middle is walking away from the camera. The person on the right is walking towards the camera. The background shows several small, makeshift buildings with corrugated metal roofs. There are many power lines crisscrossing the sky. The overall atmosphere is one of poverty and urban overcrowding.

Trust and the role of data protection law

A 'paradoxical' relationship between levels of knowledge and levels of trust



Many who are less informed about privacy are largely unaware of the risks or issues that it presents

As people become more informed about these issues, they become better able to manage their own privacy and data, but they also become more aware of the risks

- and therefore less naively trusting of organisations and platforms when it comes to their data.

We have seen that those in markets with more comprehensive legal frameworks are likely to be slightly better informed about these issues

- although other factors (digital literacy, education, affluence) are much more influential factors.

This means that, counterintuitively, those in the least protected markets are often the least concerned about these issues - and that putting better legal protections in place and educating the population about safe data behaviours is likely to make end-users less trusting and more cautious.

Whilst the presence of data protection law may not be perceived by end-users – its importance was accentuated by all audiences

Consumers in all countries saw the value of laws protecting treatment of their data

- Laws of this nature may operate ‘behind the scenes’: they are not top of mind; but
- They are important – providing support and protection if needed; and
- Though those in markets with comprehensive data protection frameworks may not necessarily feel much more protected, arguably they should be much more protected, and also better able to manage their own data & privacy.

KII interviewees accentuated this

- Clear frameworks protect end-users, who may not understand them;
- They support local commerce – since business owners know exactly what to do in order to behave appropriately;
- GDPR-grade privacy law opens up opportunities for trade with EU; and
- One KII called for the major African MNOs to take the lead, ahead of individual governments - in defining a consistent, regional baseline agreement on data privacy in the telecoms space.

“If law exists... I’m protected. I’m like a child who has been bitten; I can run to my father and say, I have been bitten. The child is protected.”

male, Zambia

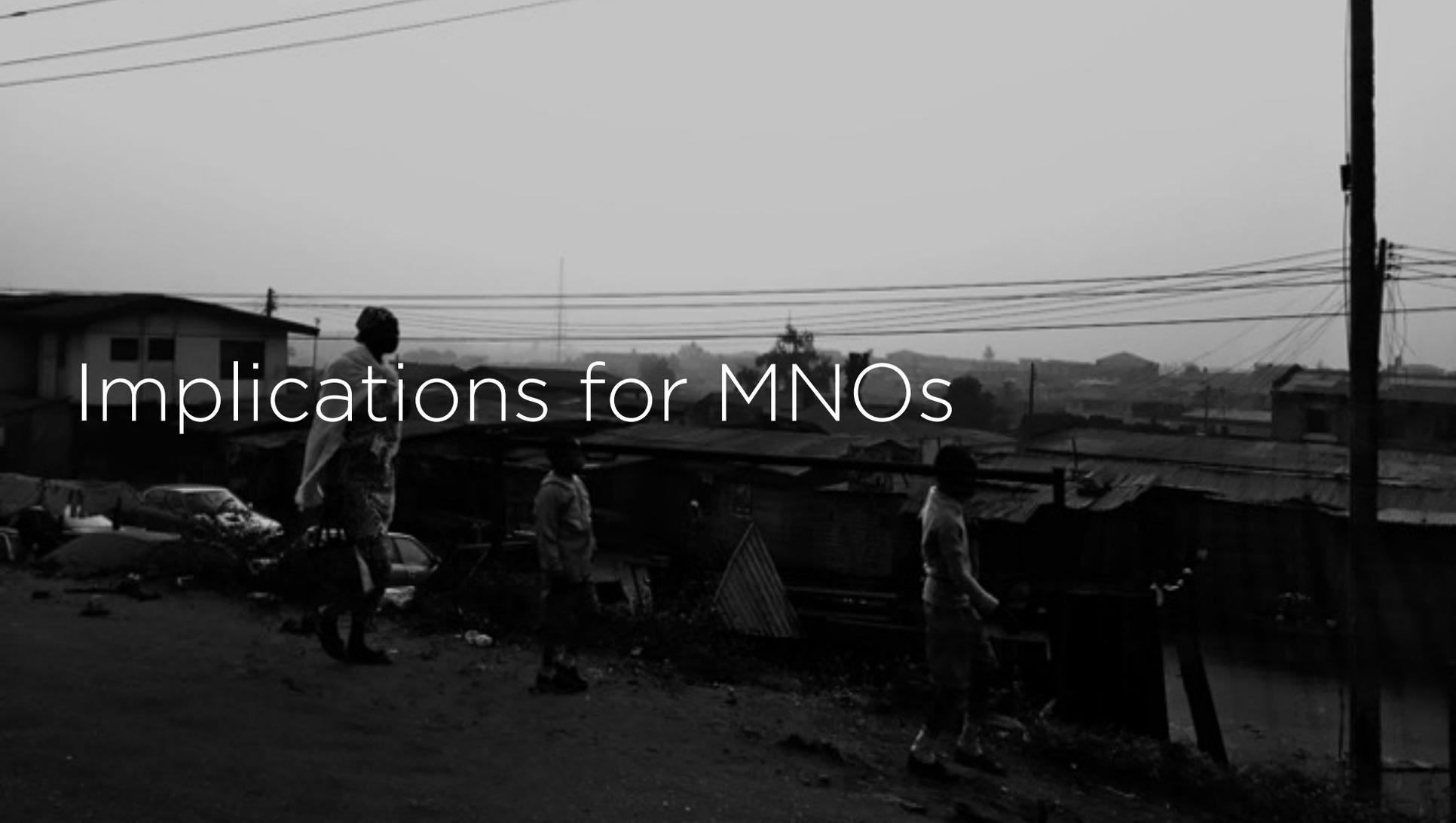
“The average person on the street wouldn’t know about these laws... Good data protection regulation matters.”

legal insider

“[Ideally,] level everyone on the same game... Europe [can] approach African countries and say, you need to have similar data protection laws to continue to have business together.”

legal insider

There is agreement that data protection law is desirable and supports all citizens: commercially, and in the case of breaches

A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. On the left, a man in a light-colored shirt and dark pants is walking towards the right. In the center, a child is walking towards the left. On the right, a woman in a light-colored dress is walking towards the right. The background shows a dense cluster of small, makeshift buildings with corrugated metal roofs. Power lines are visible overhead. The overall scene is one of poverty and informal housing.

Implications for MNOs

Five recommendations for MNOs emerging from this study

In communicating existing / new identity-linked products and services

1. Customers know MNOs hold a great deal of their data already, are comfortable with this, and willing for it to be used in their favour
 - But it is important to **accentuate how it will benefit them tangibly and clearly**
 - e.g. explain that this service will give them commercial advantages, or save them time re-registering for other products.

In designing identity-linked products and services

2. Services which take a **long-term view of consumer needs, and make transparent how their data has been used**, are more appealing than simply identifying personalised opportunities
 - So focus on delivering products which address these requirements - e.g. in the content of a financial profile, include spend illustration and analysis.

In building, and retaining, trust

3. Agents can be (for the more privacy-alert, and in urban areas) a weaker link in the MNO trust chain; **stores** are felt to be more reliable, so would ideally form the hub of MNO-enabled ID sign-up in future;
4. Where MNO-enabled ID sign-up is or becomes a possibility, **government accreditation** would be extremely valuable in reinforcing trust and legitimacy – particularly in markets without data protection law, where customers may feel less supported by telecoms regulation;
5. **Overt evidence of training, and computer technology**, also reinforce consumer trust: MNOs should make these apparent where they have a role to play in supporting foundational identity ecosystems

An aerial photograph of a densely populated urban area, possibly a hillside neighborhood, with numerous houses and buildings. The entire image is overlaid with a semi-transparent red color. The text is centered over the image.

The role of privacy frameworks in building trust for digital identity services

Understanding end-user attitudes towards mobile services linked to their digital identity



APPENDIX

Methodology



Detailed sample and recruitment criteria

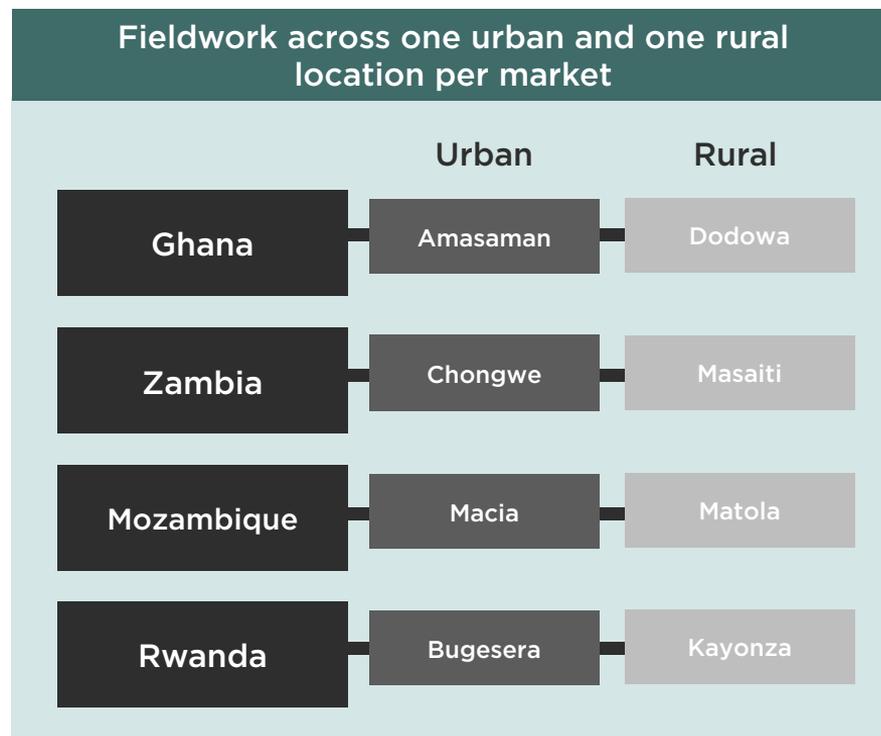
Rationale for these four countries:

These countries were selected from a longlist of 10 potential Sub-Saharan African countries – based on:

- Presence vs. absence of data protection law (as determined by GSMA desk research), for comparative purposes;
- Avoidance of current political instability, or recent high profile data breaches, which could skew focus in research; and
- Markets with at least 30% national identity cover: to avoid research needing to address only a tiny minority of more ‘engaged’ individuals in any country.

Rationale for these locations in-country:

- Representation of an urban and rural spread – with rural areas to be in a different province and / or geographically separate to the urban destination; and
- Participant job roles to be reflective of urban and rural diversity – e.g. in rural, higher proportion of those working in agriculture, fishing, etc.



Recruitment criteria

General Criteria

Gender: mix of male and female

Age: all 18-50

- FGD: mix of youth (18-24), younger (25-35) and older (36-50);
- IDI: mix of younger (18-30), mid (25-35) and older (31-50);
- Lifestage;
- FGDs: Youth to fall out naturally, younger/older – aim for all to have children (mix of younger/older, male/female);
- IDIs: Younger to fall out naturally, older/mid – aim for all to have children (mix of younger/older, male/female).

Social grade: C1C2DE

Literacy: all to be able to read to some degree

Segment/profession: Aim for mix of respondents participating in the formal and informal economy

Specific Criteria

Handset ownership and status: natural fall-out of basic, feature and smartphones

- Aim for 10 respondents participating in the formal and informal economy.

Mobile use and spend

- All to make use of paid for mobile service twice a month or more;
- Half in each FGD and half of all IDIs per market to use or have used internet / internet-enabled services on their mobile.

SIM registration

- Across groups and IDIs four-11 individuals per market to have a SIM registered in someone else's name.

Mobile money

- At least two per group to have their own mobile money account;
- Three IDIs to have their own mobile money account.

Qualitative/Quantitative end-user recruitment breakdown Ghana and Zambia

Ghana

	FGDs - 6 x 90 min		
Urban	G1 MALE - 25-35	G2 FEMALE - 36-50	G3 FEMALE - 18-24 SMARTPHONE USERS
Rural	G4 MALE - 18-24	G5 MALE - 36-50 SMARTPHONE USERS	G6 FEMALE - 25-35

	IDIs - 5 x 60 min		
Urban	IDI1 MALE - 18-30 SMARTPHONE USER	IDI2 FEMALE - 31-50	IDI3 MALE - 25-35
Rural	IDI4 MALE - 31-50	IDI5 FEMALE - 18-30 SMARTPHONE USER	

Zambia

	FGDs - 6 x 90 min		
Urban	G1 MALE - 25-35 SMARTPHONE USERS	G2 MALE - 36-50	G3 FEMALE - 18-24
Rural	G4 MALE - 18-24	G5 FEMALE - 36-50 SMARTPHONE USERS	G6 FEMALE - 25-35

	IDIs - 5 x 60 min		
Urban	IDI1 MALE - 18-30 SMARTPHONE USER	IDI2 FEMALE - 31-50	
Rural	IDI4 MALE - 31-50 DIFFERENT SIM	IDI5 FEMALE - 18-30 SMARTPHONE USER	IDI3 MALE - 25-35

Qualitative/Quantitative end-user recruitment breakdown Mozambique and Rwanda

Mozambique

	FGDs - 6 x 90 min		
Urban	G1 MALE - 25-35	G2 FEMALE - 36-50	G3 FEMALE - 18-24 SMARTPHONE USERS
Rural	G4 MALE - 18-24	G5 MALE - 36-50 SMARTPHONE USERS	G6 FEMALE - 25-35

	IDIs - 5 x 60 min		
Urban	IDI1 MALE - 18-30 SMARTPHONE USER	IDI2 FEMALE - 31-50	
Rural	IDI4 MALE - 31-50	IDI5 FEMALE - 18-30 SMARTPHONE USER	IDI3 MALE - 25-35

Rwanda

	FGDs - 6 x 90 min		
Urban	G1 MALE - 25-35 SMARTPHONE USERS	G2 MALE - 36-50	G3 FEMALE - 18-24
Rural	G4 MALE - 18-24	G5 FEMALE - 36-50 SMARTPHONE USERS	G6 FEMALE - 25-35

	IDIs - 5 x 60 min		
Urban	IDI1 MALE - 18-30 SMARTPHONE USER	IDI2 FEMALE - 31-50	IDI3 MALE - 25-35
Rural	IDI4 MALE - 31-50	IDI5 FEMALE - 18-30 SMARTPHONE USER	

Key Informant Interviews

Four x 45-minute telephone interviews were undertaken

Policymaker

Former Rwandan minister for Information and Communications Technology

Academic

Lecturer in Company Law, specialising in Africa

Legal expert

International Corporate Lawyer and Privacy Thought-Leader

Academic

Lecturer at the Open University of Tanzania and Co-Director of African Law and Technology Institute (AFRILTI)

Two MNO-enabled concepts described to end-users in this study: financial ID profile, and NID sign-up via MNO networks

MNO-provided financial ID Profile

- There's a new service being introduced soon for farmers in another country;
- A mobile network will request permission to check their mobile money transactions and airtime top-up history;
- If they accept: the network would be able to create an economic 'profile' of each customer, based on their transaction history and cashflow;
- This will be used to identify customised services, such as loans or microinsurance, which they may find useful – and then invite them to access these;
- This will give farmers better access to products which could help their business; and
- This could apply to and benefit anyone, in any capacity – work or personal.

MNO-enabled NID Sign-up

- In some locations, particularly in rural areas, there may be no easily accessible government offices through which people can sign up for national identity – although MNO stores or agents may be present;
- So what if: you could go to any mobile phone store, or agent, and they could register you for NID in the same way that they register customers' SIMs - by taking your details, biometrics, photo, and proof from other ID?
- This would be uploaded to the national database;
- You would receive your card in the same timeframe as if you had applied via a government office; and
- Your personal information would be protected in the same way as it is now, when you register for a SIM - with strict data protection and privacy protocols in place.

Market context



Ghana: overview of use of mobile, identity, and key data share concerns

Mobile usage

- Widespread use of two mobiles and multiple SIMs – often one for data and one main SIM for voice;
- Widespread use of mobile internet – Facebook, WhatsApp, Google, YouTube; and
- Mobile money very commonplace, used for transfers but also for savings.

Identity context

- The great majority are registered with the official national Voter Card, which remains the primary system of identity;
- A new National ID Card is being piloted, but distribution is extremely limited (only certain neighbourhoods in Accra are in the pilot); and
- In 2017 SIM registration became mandatory for new and pre-existing SIMs, as part of a drive to counter mobile money fraud.

Digital data sharing: risks and concerns

- Some concerns with online shopping – financial information particularly sensitive;
- A growing consciousness of privacy issues around social media – some adjusting privacy settings, inputting less information, or signing up with false details to limit the amount of information about them available online; and
- Few concerns about sharing data with organisations – easily outweighed in value exchange & reassured by social proof.

Zambia: overview of use of mobile, identity, and key data share concerns

Mobile usage

- Many have more than one SIM for increased coverage, a minority have multiple handsets;
- Used for basic communication – huge life change in rural, saves time travelling to communicate with friends/family/colleagues;
- Internet use more prevalent around younger demographic;
- Mobile money used widely; and
- SMS updates from government are common – for health advice, outbreaks etc.

Identity context

- A national citizen registry has been in place since 1964, and enrolments rates for the National registration Card (NRC) are high, at 88% for men and 83% for women; and
- An NRC number is required to register a new SIM, and the majority of SIMs are registered correctly.

Digital data sharing: risks and concerns

- Some concerns around how much personal data is made public e.g. not putting too much up on social media for everyone to see;
- A high awareness of the risk of crime or misuse of data if it falls into the wrong hands e.g. someone using their details for SIM registration or accessing your mobile money account; however
- Fears centred around individual bad actors, scammers and hackers – with little concern around how organisations store or handle data.

Rwanda: overview of use of mobile, identity, and key data share concerns

Mobile usage

- Two SIMs in one handset very widespread;
- Majority use just for basic communication – calls and messages, and mobile money transactions (buying electricity) – with lower rates of internet usage; and
- SMS services relatively common, e.g. from banks to alert for fraud (for those who have bank accounts), or results from hospitals/clinics.

Identity context

- Enrolment rates for National Identity Card (NID) extremely high; and
- Majority also have their SIM registered to their own name.

Digital data share: risks and concerns

- Very few concerns sharing data with organisations, certainly nothing that would stop them using a service; and
- A widespread assumption that the government has access to everything you communicate electronically and can catch you if you say anything “bad” i.e. anti-government.

Mozambique: overview of use of mobile, identity, and key data share concerns

Mobile usage

- At 41%, Mozambique has the highest smartphone penetration of tested markets;
- Participants reflected this: a high proportion (particularly in Matola, but also younger respondents in rural Macia) owned one;
- Amongst this audience, social media access (Facebook, sometimes Twitter and Instagram) was common;
- For several, this was the mainstay of their internet usage – although more advanced / affluent mobile users reference online banking;
- Multiple SIMs were common, to benefit from different deals and coverage; and
- These were often in dual SIM handsets (with only older males typically owning more than one handset).

Identity context

- Penetration of the Bilhete de Identidade, the foundational ID card, is at 61%;
- The government has introduced legislation requiring SIM card registration; and
- Alternative forms of identification (apart from the Bilhete de Identidade) are acceptable for this process.

Digital data sharing: risks and concerns

- Concerns relating to identity theft, or personal data breaches, were more prevalent in urban Matola, where crime was described as a common occurrence;
- Corruption and bribery were believed to be particularly rife, with frequent mentions of information (of all types) being passed by company employees to individuals for a fee;
- Along similar lines, a number mentioned past experiences or known local stories of people being mugged or robbed based on social media postings; information from medical tests being shared by staff; and
- In Macia, this was more infrequent.

A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. On the left, a man in a light-colored shirt and shorts is walking towards the right. In the middle, a child is walking towards the left. On the right, another person is walking towards the left. The background shows several small, makeshift buildings with corrugated metal roofs. Power lines are visible across the sky. The overall scene is one of poverty and informal housing.

Further qualitative quotes /
illustration

Key differences: gender

A handful of differences by males and females within this sample:

- In some cases, females were less digitally literate than males (in the same location)
 - Some women referred to knowing little themselves about handset functionality, or male family members helping them to use their mobile;
 - This could correlate with being more privacy-uninformed; however
 - This was not universally the case; for example, a number of rural males also displayed similarly low digital literacy and lack of alertness to digital privacy.
- Also, indications that women are more often subject to harassment, related to sharing identity details
 - Some women told stories of MNO employees calling female customers after receiving their phone number;
 - Others spoke of the risks of their photos being digitally edited or shared inappropriately online, by other internet users intent on fraud or damaging their reputation;
 - This links to slightly greater caution with their own image; males were more likely overall than women to be willing to share their photo with an MNO
 - **90% of males** in this sample were willing to do so, vs. **77% of females**.
- Women were often less convinced that redress for data breaches was possible, or likely to be successful
 - Some acceptance that “this is what happens” – whereas males were slightly more likely to declare a plan to involve police if needed.
- **HOWEVER:** on many parameters (including trust in various entities, willingness to access mobile services, willingness to share most personal data with MNOs, and openness to identity-linked services): no tangible differences between genders here
 - Also, no gender-led barriers to SIM registration were present within this sample; reasons women had unregistered SIMs were similar to those of males.

Key differences: urban vs. rural audiences

Those in rural areas were less privacy-alert, and less aware of the risks of personal data breaches

- In villages, many were accustomed to dealing with the same, known individuals within organisations
 - They were therefore more likely to trust them.
- This included mobile agents – who were, again, less likely to be assumed to be untrustworthy by ruralites
 - For some in rural areas, agents are familiar faces in the area and play a role in helping users to operate their handset; so trusted more;
 - That said: those in ‘without’ countries were still unwilling to accord them the responsibility of MNO-enabled NID sign-up – even if they are not actively dishonest, this seemed to several to lie outside their realm, and be more suited to those in stores.
- However, those in rural areas were slightly less willing to share their mobile money transaction history with an MNO
 - Only 63% of ruralites were open to doing this, compared to 81% of urbanites – potentially indicating greater caution with info around their spend; however
 - Once the MNO-provided Financial Profile was discussed in more detail, willingness was equally high in urban and rural locations; and
 - On all other measures, openness to sharing data and service usage was not significantly different across locations in any respect.
- Whilst in urban areas: awareness of identity-related crime, and sensitivity to risks of breaches, was higher in this sample
 - Stories of corruption and / or fraud were more frequent, so end-users more aware of the possibility of this happening to them.
- Additionally, communication around regulation had often percolated through to a higher degree in urban zones.

Worries around children's data are present, for some - but typically do not prevent parents from sharing

Participants' mental 'rules' for sharing data concerning their children were typically similar to their attitudes to their own

...only with slightly higher levels of caution, in some cases

- Some parents worry about children's information ending up in the wrong hands;
- In the worst case scenario, this could result in kidnapping, killing or forced criminal activity;
- This is known to be unlikely, but nonetheless, children are often seen as more vulnerable; some had restricted social media posts identifying their children's faces, due to perceived risks; and
- Isolated individuals described the possibilities of children being targeted by false NGOs or fraudulent sponsorship efforts, via bank or mobile money account donations to parents.

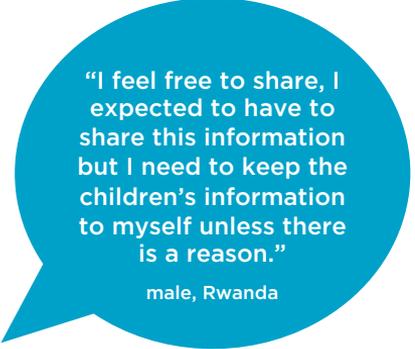
Data is shared, when needed and with known parties

- Benefit **outweighs concern**; there are few circumstances where data is withheld if it results in not being granted access or the ability to sign up to something;
- Organisations that feel **'official'** are more highly trusted e.g. health, education and government sectors; it is **part of procedure**; and
- Knowing **why the data is needed, and exactly which organisation it is going to**, is comforting and enables parents to give the required information without worrying.



"Hospital and school, anything to do with development for them I would give. But you might think that one company wants to help you but they might just want a share of your children's life!"

male, Zambia



"I feel free to share, I expected to have to share this information but I need to keep the children's information to myself unless there is a reason."

male, Rwanda

Terms and conditions are seldom read in full – due to length, and desire to access service benefit immediately

- Mixed understanding of what these are and how to interact with them
 - Those who are less tech literate and less educated are least likely to know what they are.
- Very few read full terms and conditions from start to finish when signing up for services
 - Some consider reading the summary bullet points enough.
- Felt to be too long and overwhelming; the expectation that they will be read in full is unrealistic
 - Most will simply click through and accept without reading so that they can get the service;
 - Exceptions to this: bank loans or other financial products, which a number comb in more detail.
- General acceptance that if others have signed up already then it will “probably be fine”.

“The reason I think people don’t care is that when it is their first time accessing that technology, website, or service, they are curious about it and they just accept them without reading them.”

male, Rwanda

“If you wanted us to read it, make it easier – it’s so small and so long.”

female, Ghana

“The first day I joined Facebook – you have to ‘agree’ in order to join; I didn’t care about it, I just wanted to get Facebook.”

female, Zambia

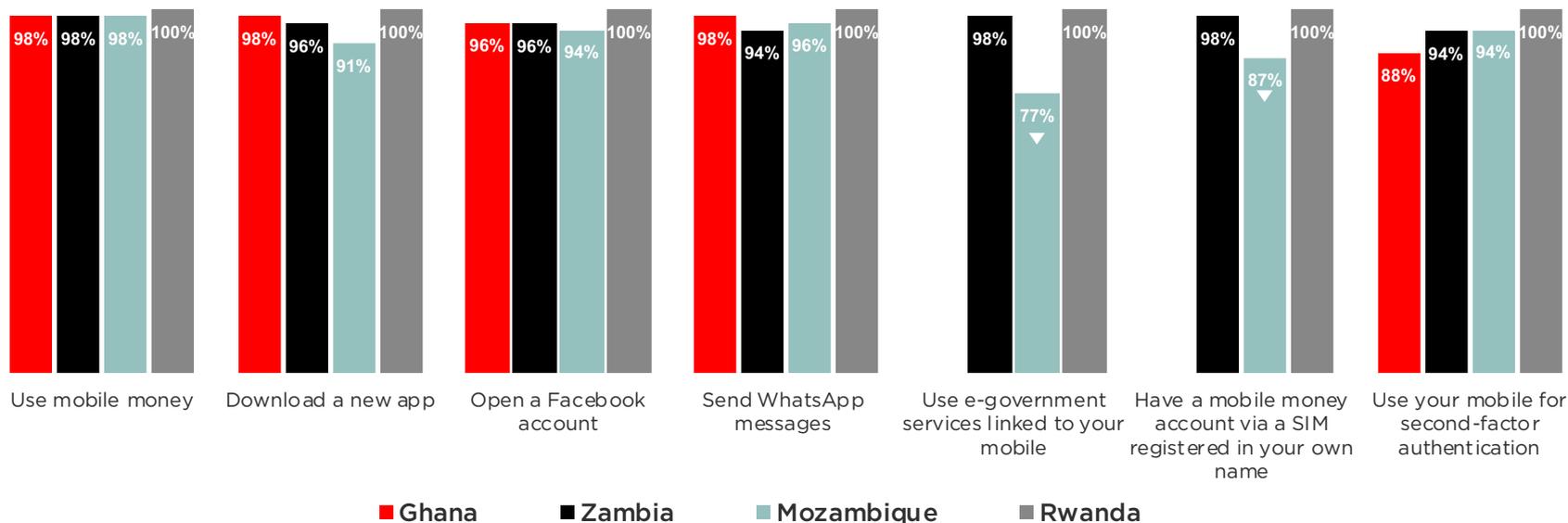
A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. On the left, a man in a light-colored wrap walks towards the right. In the center, a child walks towards the left. On the right, another person walks towards the right. The background shows a dense area of makeshift buildings with corrugated metal roofs. Numerous power lines crisscross the sky. The overall atmosphere is one of poverty and urban overcrowding.

Further quantitative data

Openness to share or access data via mobile was universally high, although those in Mozambique were less willing to link their mobile to e-gov services

If you have, or assuming you had, a smartphone (and cost / literacy were not barriers). **How willing are you, or would you be, to...**

Sig higher/ lower vs. all other markets 
Have already done this/ very/ slightly willing



Q1. Let's imagine you own a smartphone, and it is free to do any of the activities below. If you weren't sure how to do any of them, someone could show you how. If so, how willing would you be to do each of the following.

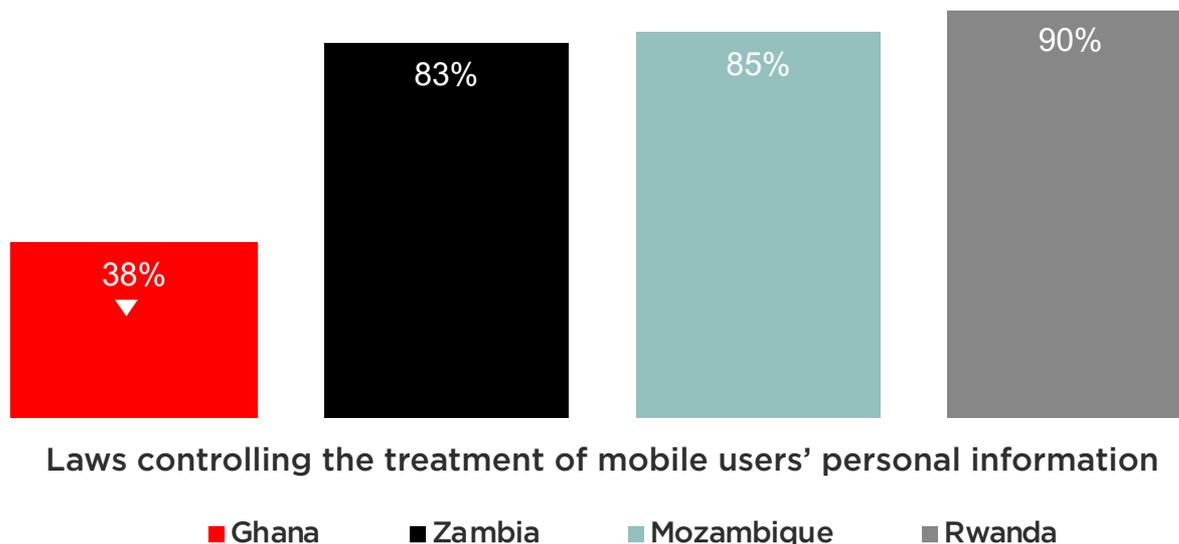
Base: all answering in each market (n=varies, min=49*). Base too low to show scores for some codes in Ghana. *Caution low base.

Respondents from Ghana were least likely to think that data protection laws existed in their country

Do you think these laws exist in your country?

I think they exist/ they do exist

Sig higher/ lower vs. all other markets 

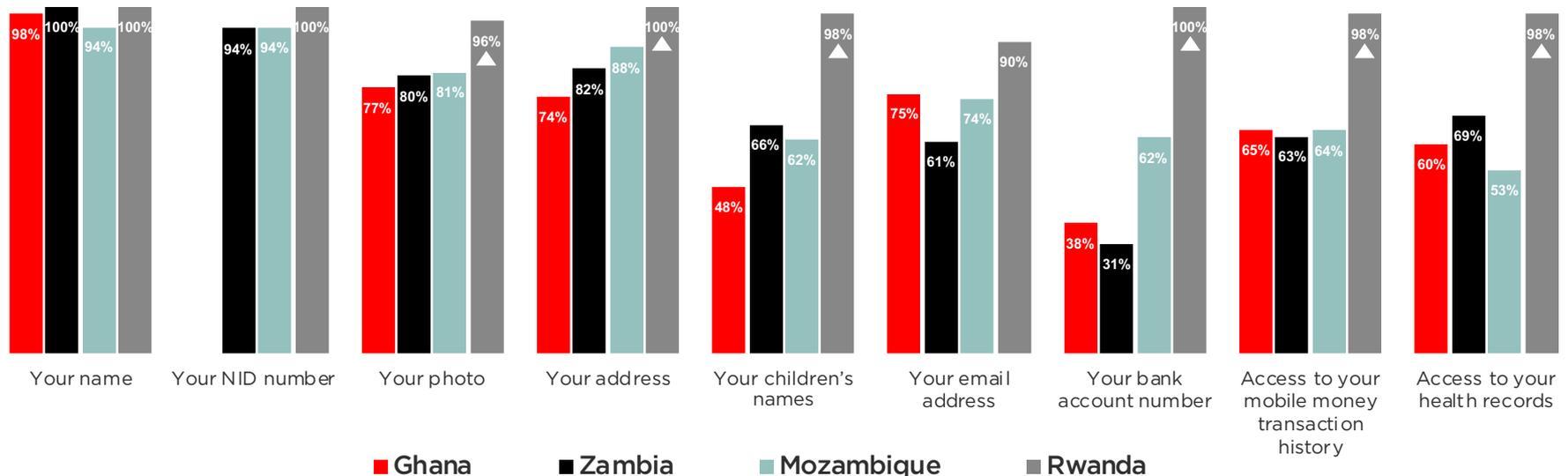


Rwandans are more willing to share personal information with an MNO than any other market

How willing would you be **to share this information with an MNO?**

(assuming that you need to do so, to access a service which they're offering and which you want to use)

Sig higher/ lower vs. all other markets 
Very/ slightly willing



Q3. How willing would you be to give your mobile phone network each of the following pieces of information about yourself?
 Base: all answering in each market (n=varies, min=46*). NID number data for Ghana suppressed. *Caution low base.

End-user case studies

A black and white photograph of a slum. In the foreground, three people are walking on a dirt path. On the left, a man in a light-colored shawl carries a child on his back. In the center, a young child walks. On the right, a woman in a light-colored dress walks. The background shows a dense cluster of small, makeshift buildings with corrugated metal roofs. Numerous power lines crisscross the sky. The overall atmosphere is one of poverty and daily life in a low-income urban area.

Case study: meet Jemima, Ghana



Jemima

Aged 29; mother of 2
lives in Amasaman
Seamstress

Jemima and mobile

- Jemima has two phones: one smartphone, one feature phone;
- She mainly uses her smartphone and mobile internet for work-related uses including mobile money, WhatsApp (to advertise and take orders) and YouTube (to research new styles);
- She also chats with friends through WhatsApp, and uses Instagram and Facebook – but her husband set up her accounts;
- She has two SIMs, one for each phone: Vodafone (feature phone) and MTN (smartphone); and
- She bought and registered her SIM with a mobile money agent in an MTN shop.

Privacy and trust

- Jemima is willing to share most forms of data with most organisations, as long as she understands why they need it;
- Registering her SIM reassures her that she can easily retrieve it if anything goes wrong;
- She is cautious about sharing information via Facebook; she does not really post anything, just goes there to see what her friends are doing – she prefers WhatsApp, which she believes to be more secure; and
- She is wary about MNO agents, and feels she can not fully trust them – however this does not stop her using them.

“I am careful about giving out this information.

I think, ‘why do you need this’, and they can explain – we will use it for this...

If it’s important, I will give them the information.”

“Everything you do there is on the world – everybody is seeing it. Sometimes I don’t want people to see what I do. WhatsApp is like this – anything you do, nobody will see it – but Facebook it is everywhere.”

“[Mobile Agents] know your information, and they can do things behind your back that you don’t want.”

Case study: meet Minerva, Zambia



Minerva

Aged 32; mother of 1
living in Chongwe

Minerva and mobile

- Minerva has two handsets and four SIM cards (two Airtel, one Zamtel and one MTN);
- She uses her phone for calling, texting and social media;
- WhatsApp, Facebook and Opera mini (web browser) are her most used apps – used for keeping up with her friends and the latest news; and
- Minerva rarely hesitates when submitting her details to mobile apps or websites, she has ‘no concerns’.

Privacy and trust

- Very few concerns around giving her personal details to organisations during sign up;
- Worries around privacy are around sharing her personal information on social media where anyone can see it and use it;
- She feels comfortable sharing with organisations as they are likely to have measures in place to ensure her data is not leaked or shared with others; and
- Minerva is more likely to question trusting an individual as there is always a risk that a person may do something bad of their own accord.

“It’s fine with me, I don’t mind giving my details, the companies are trying to know you better for a reason e.g. to block underage users.”

“I do care when my privacy is involved, but I know that with an organisation my privacy would be safe.”

“There are people who are good and people who are bad. As long as the individual is trustworthy, I’d give them my trust”

Case study: meet Emerita, Rwanda



Emerita

Aged 23, 2 small children
living in Kayonza
businesswoman

Emerita and mobile

- Emerita has a dual SIM handset with SIMs for Tigo and MTN; she switches between them so she can communicate with her friends on different networks;
- She uses the internet on her phone for banking and apps;
- Her SIM is registered in her name so that when she uses her mobile money account, the money she deposits is more secure; and
- The ability for her phone to be tracked is good because if it is stolen they will be able to find the person who stole it and return it to her.

Privacy and trust

- Emerita feels comfortable with organisations having her data as she knows she has willingly given the info herself and knows why they need it;
- She will share information about herself when required, but sometimes feels uneasy if she doesn't know what might happen next: "who is going to use it and how?"; and
- Password protection on bank accounts and mobile money are comforting; if something goes wrong she can only blame the mobile network as they are the only one's with access to this information.

"I opened a bank account and they asked for my phone number so they could send notifications about my account- I felt good giving this to them"

"I can give my children's information as freely as I give mine because you can't ask for a service from them without giving this information"

"I cannot give my identification to an institution if I don't know how they work"

Case study: meet Alberto, Mozambique



Alberto

Aged 31; father of 4
living in Macia
fisherman

Alberto and mobile

- Alberto has one Vodacom SIM and one handset;
- He uses his phone for calls, SMSs, and m-pesa (which is particularly useful to him for transactions in his job);
- He does not use internet, as he says he does not “have time” to configure his phone;
- He shares personal data via SMS, including fishing job applications; and
- He proudly showed his National ID card when he registered for his SIM - he was happy to follow the right process.

Privacy and trust

- Alberto is relaxed about organisations holding his personal data - although he would check who he is sharing information with initially;
- He feels that as he does not have a great deal of money, he is uncertain where any risks of sharing his data with bodies / people he knows could be;
- He trusts the government, MNOs, and civil servants because “they come with a badge”; and
- He believes MNOs keep users’ SMSs on file, but does not see this as a problem - he does not do anything bad.

“If I was driving, the police would ask me for my driving licence. [My Identity card] is something I have to provide for the official to know that I’m part of the country.”

“I am a normal person, a Mozambican, who is struggling in his life. If someone tried to do something bad [with my data], I’ve got nothing.”

if there’s a problem [with an MNO], I can go to them in person, so I trust them.”



GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600

Copyright © 2019 GSM Association