Data Governance and Public Trust:

Exploring the Sources of Low Trust Levels in Public Data Controllers in Ghana

April 2022

CIPESA

Table of Contents

CIPESA acknowledges the contribution of Selassie Tay and Alhassan M. Kamil in the writing of this report.

The report was produced with support from the Hewlett Foundation in the context of promoting data openness among public and private actors, and advancing respect for data rights towards citizens' participation and informed policy decisions in rights-respecting data-for-development initiatives.

Abstract

In the past decade, digitisation and the adoption of digital technology requiring data systems has become widely spread in Africa. With this comes the complexities of how data is collected, processed, shared, and utilised, including issues of data privacy and protection. Countries have adopted several laws and policies designed to promote access, address privacy and personal data protection concerns as well as stimulate the uptake of data-based initiatives. Trust plays a significant role in building data systems that are accurate as people are more willing to share their personal data with data controllers.

Like other African countries, Ghana has enacted several laws and policies, including the Data Protection Act, 2012 (Act 843), The National Identification Register (Amended) Act, 2017 (Act 750), and The Cybersecurity Act, 2020 (Act 1030). Ghana has also embarked on several massive data collection programmes, including the mandatory SIM Card registration and the issuance of national IDs. However, the data collection programmes have been hit by high levels of apathy from the public, and this has been attributed to the low levels of trust in public institutions that collect and control data.

The objective of this research therefore is to investigate the sources and impact of this low level of trust among Ghanaian public. The research also explores the possible ways public trust can be bolstered by data governance systems. The study employed quantitative surveys and qualitative in-depth interviews for data collections.

The study found a prevalence of mistrust in public data controllers in Ghana. The main reason for the mistrust stemmed from the lack of public education and awareness among data subjects as well as personal experiences relating to data breaches by data controllers.

Introduction

In the past decade, digitisation and the adoption of digital technology became pervasive on the continent, introducing new complexities to how data is collected, processed, and utilised by governments and other data controllers. This necessitated the enactment of data protection laws to address issues such as privacy infringement, data security, and public trust. As a result, data governance – a framework of policies, laws, regulations, and processes that enable, guide, and sometimes limit the collection, use and sharing of data - became prominent for governments who wanted to leverage the benefits of the data revolution for development and for public service delivery.[1] For instance, the number of countries in Africa with data protection laws tripled from around eight in 2012 to 26 in 2019.[2] As of 2022, there were 33 countries with data protection laws or regulations.[3] Whereas this increase in data governance regulations is progressive and highlights the importance of data governance in Africa, a critical challenge that remains less well attended to is the issue of public trust in data governance processes and the institutions mandated for that purpose.

Though no specific study on public trust and data governance within the African context has been cited, surveys conducted by Afrobarometer reveal a low level of public trust in public institutions.[4] For instance, findings from the 2019 Afrobaromenter survey (Round 8) in Ghana show that trust of public institutions was a mixed bag across institutions. For example, only 15% said they trusted parliament compared to 30% who did not have any trust at all; other institutions include the Election Commission (21% trust vs 19% no trust at all); Courts of Law (16% trust vs 25% no trust at all); Ghana Revenue Authority (10% trust vs 27% no trust at all).[5]

Public trust and data governance has been studied elsewhere[6] and the results are instructive for the African context. For instance, a 2017 study by the UK Information Commissioner's Office found that only 49% of Britons trusted national government departments and organisations to store their personal data. Other surveys in Australia and in the US have identified similar levels of distrust.[7] This is particularly compelling considering the vast gap in the robustness of the data management systems between Africa and the advanced countries where these studies have been carried out.

1 *Craig Stedman and Jack Vaughan, 'What Is Data Governance and Why Does It Matter?', 2020.*

2 *Graham Greenleaf, 'Global Data Privacy Laws 2019: 132 National Laws and Many Bills', Privacy Laws & Business International Report, 157, 2019, 14–18.*

3 *Recent developments in African data protection laws – Outlook for 2022, https://www.engage.hoganlovells.com/knowledgeservices/news/recent-developments-in-african-data-protection-laws-outlook-for-2022_1_1*

4 *Afrobarometer, Corruption and Trust in Political Institutions in Sub-Saharan Africa (Accra, Ghana, 2008); Afrobarometer, 'Trust and Corruption in Public Institutions : Ghanaian Opinions' (Accra, Ghana: Afrobarometer, 2014) <https://afrobarometer.org/sites/default/files/media-briefing/ghana/gha_r6_presentation3_trust_corruption.pdf*

5 *https://afrobarometer.org/sites/default/files/publications/Summary%20of%20results/afrobarometer_sor_gha_r8_en_2020-02-09.pdf*

6 *Viral Chawda, 'Building Trust in Government's Use of Data', KPMG <https://home.kpmg/xx/en/home/insights/2018/06/building-trust-in-governments-use-of-data.html [accessed 7 April 2021].*

7 *Chawda.*

Data Governance in Ghana

Ghana has demonstrated a remarkable commitment to data governance and open access to data[8] by instituting several measures including the enactment of the Data Protection Act, 2012 (Act 843), which established the Data Protection Commission with the mandate to protect the privacy of individuals and to regulate access, processing and sharing of personal data.[9] The government also passed the Cybersecurity Act of 2020, to among others, prevent cybercrimes involving the unauthorised use of personal data. Several institutions have been established to ensure the responsible collection, processing, and use of individuals' personal data. Government institutions that collect, process, and use people's data for socio-economic development purposes include the Ghana Statistical Service, Ghana Revenue Authority, the Electoral Commission of Ghana, the Births and Death Registry, and the National Identification Authority (NIA). The NIA was set up in 2003 under the Office of the President with a mandate to establish and manage a national database and to collect, process, store, retrieve and disseminate personal data on the population by issuing national identity cards.

Despite all these efforts towards responsible data governance, there still exists a number of problems that hamper Ghana's responsible data governance ambition. Further, there is a noticeable indifference and mistrust in the public institutions mandated to collect and manage people's personal data as well as the various initiatives established for this purpose. Acoording to a 2019 survey by the Afrobarometer, a majority of Ghanaians expressed "little" or "no" trust at all in institutions such as the Ghana Revenue Authority (54%), the Police (69%), the Electoral Commission (41%), and Parliament (55%), among others.[10] Although the survey was not focused on data governance, it nevertheless unmasks the high levels of mistrust among the populace for state institutions including those that are directly involved in the data governance process.

Notably, the Electoral Commission (EC) and the National Identification Authority (NIA) are of interest due to the volume and importance of the personal data that they manage. For instance, in the period leading up to the 2020 elections, the Electoral Commission (EC) published the national voters' register containing the personal data of individual voters online.[11] The data released by the EC was so detailed and included the biodata of registered voters such as names, age, residential address, and images. It also displayed the barcodes that could be used to generate the biometric data of individuals such as the fingerprints. This action attracted public outcry, raising questions about the institution's casual approach in safeguarding the security and privacy of individuals' personal data. Essentially, for some voters the action of the EC amounted to a breach of privacy, further deepening the public mistrust for the institution.

Likewise, the NIA has also suffered visible public mistrust and apathy.[12] The authority only gained public patronage in 2020 when the acquisition of the National Identification Card was linked to the right to vote and the enjoyment of certain public services, thus overriding though not addressing the issue of public trust and apathy.

Moreover, other initiatives aimed at increasing data availability for policy purposes have suffered serious pushback which is reflected in public suspicion and mistrust of the government's motives. One such initiative was the COVID-19 Tracker App which was designed to help in tracing COVID-19 patients and their contacts.[13] In another action,, the Communications Ministry asked the Central Bank of Ghana to release data of mobile money subscribers to a private contractor for tax revenue assurance purposes.[14] Despite the tremendous effect public trust is likely to have on data governance, there has been limited research and public discourse on this issue in Ghana.

---

8 Government of Ghana, Data Protection Act of Ghana 2012 (Ghana: Act of Parliament, 2012) <http://www.dataprotection.org.gh/sites/default/files/Data Protection Act , 2012 (Act 843).pdf

9 Government of Ghana, Data Protection Act of Ghana 2012 (Ghana: Act of Parliament, 2012) <http://www.dataprotection.org.gh/sites/default/files/Data Protection Act , 2012 (Act 843).pdf >.

10 Afrobarometer, https://afrobarometer.org/sites/default/files/publications/Summary%20of%20results/afrobarometer_sor_gha_r8_en_2020-02-09.pdf

11 BBC, 'Voters List 2020: Ghana Electoral Commission Publish Final Voter Register Online for 7 December Election', BBC (Accra, Ghana, 30 November 2020) https://www.bbc.com/pidgin/tori-55138308

12 National Identification Authority, 'Our History', National Identification Authority, 2020 <https://www.nia.gov.gh> [accessed 7 April 2021].

13 Ministry of Communication, 'Launch of GH COVID-19 Tracker App', Ministry of Communication (Accra, Ghana, 2020) https://www.moc.gov.gh/launch-gh-covid-19-tracker-app

14 Citinewsroom, 'Communications Ministry Fights BoG over Mobile Money Data', Citinewsroom (Accra, Ghana, 14 November 2018).

Significance of Trust in Data Governance

Trust plays a significant role in building accurate data systems. The lack of trust is the main reason why many people do not provide personal information to data controllers.[15] Trust is also one of the primary reasons why people tend to use specific technology or systems. The object of trust can be the persons handling the data or the information technology systems it runs on.[16]

Trust can be fostered by instituting robust and dynamic procedures that ensure data privacy and protection. Data controllers understanding the legislative and regulatory requirements within their jurisdiction, and complying with them, is the best place to start. The effectiveness of data governance by data controllers can impact the trust of data subjects in the data systems. According to Mayer et al, trust implies beliefs that a person, technology, and by extension system has the attributes necessary to perform as expected in a situation. This empowers data subjects to be less hesitant in sharing data.[17]

Data governance refers to a system that defines the authority and control that a network of actors within an organisation have over data assets and how these may be used.[18] Data governance covers people, processes, and technologies essential for managing and protecting data assets. The goals of data governance are to remove data silos within organisations by harmonising the data systems through a collaborative process, with stakeholders from the various participating units, and to ensure that data is used properly, both to avoid introducing data errors into systems and to block potential misuse of personal and sensitive data of data subjects.[19]

Having a poor data governance system has implications for complying with primary legislation for data privacy, in the case of Ghana, the Data Protection Act, 2012, which is designed to improve data governance by regulating the activities of data controllers in accessing and processing individuals' data. The Ministry of Communications, through its Minister, is given power by an executive instrument to stipulate actions that constitute assessable processing if it is likely to cause substantial damage or substantial distress to a data subject, or otherwise significantly prejudice the privacy rights of a data subject.

Data controllers are organisations – public or private – that determine the purposes for which and how personal data is processed.[20] These institutions are enjoined to comply with the binding privacy provisions. It is mandatory for government departments and agencies to designate an officer to act as a data supervisor. Section 17 of the Data Protection Act requires persons or institutions that process data to consider the privacy of data subjects by applying the following principles: (a) accountability, (b) lawfulness of processing, (c) specification of purpose, (d) compatibility of further processing with purpose of collection, (e) quality of information, (f) openness, (g) data security safeguards, and (h) data subject participation.

15 *F. David Mayer, Roger C. Davis, James H. and Schoorman, 'An Integrative Model of Organizational Trust', The Academy of Management Review, 20.3 (1995), 709–734 https://doi.org/https://doi.org/10.2307/258792*

16 *Thomas P. Novak and Marcos Peralta Donna L. Hoffman, 'Building Consumer Trust Online', Communications of the ACM, 42.4 (1999), 80–85 https://doi.org/10.1145/299157.299175*

17 *Mayer, Roger C. Davis, James H. and Schoorman.*

18 *Vaughan.*

19 *Craig Stedman and Jack Vaughan, 'What Is Data Governance and Why Does It Matter?', 2020.*

20 *Sylvie Delacroix and Neil D Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance', International Data Privacy Law, 9.4 (2019), 236–52 https://doi.org/https://doi.org/10.1093/idpl/ipz014*

Methodology

A multi-method approach was used in collecting and analysing the data. Specifically, the researchers used surveys, in-depth interviews, and literature review. Considering the COVID-19 protocols, most of the data collection was done in a virtual form or by phone calls. An online tool was used for the surveys while the in-depth interviews were conducted by telephone or face-to-face while observing the COVID-19 protocols.

For the survey data, cross-sectional surveys were conducted to measure the perceptions and views of members of the public using simple random sampling. Simple random sampling was adopted as the method of sampling due to its advantage of ensuring equal participation and internal validity.[21] The researchers administered an online survey to respondents via social messaging platform WhatsApp, which is among the most popular social networking sites among Ghanaians. According to datareportal.com, as of February 2020, there were 14.76 million internet users, 39.97 million mobile connections, and six million active social media users in Ghana. In percentage terms, Ghana has 48% internet penetration, 130% mobile connections, and 20% social media penetration. The percentage of internet users using WhatsApp is 82%.[22] A total of 203 people completed the survey that was shared through numerous WhatsApp groups. Five key informants were interviewed, and these were drawn from the National Identification Authority (NIA), Electoral Commission (EC), National Communication Authority (NCA), Telecommunications Industry (Expresso), and the Financial Sector (Zenith Bank). These individuals were purposely chosen because of the mandates of their institutions with regard to data governance in Ghana.

Regarding data analysis, the data gathered from the surveys was analysed using graphs and descriptive statistics in the form of percentages, means and standard deviations to give a broader picture about public trust, perception, and awareness relative to the government institutions with the mandate for data governance. Data gathered from the interviews and documentary reviews was analysed using narratives and thematic analysis. This was used to complement and triangulate the survey analysis to provide an in-depth understanding of the issues. Each interview was transcribed and the transcribed data was coded to break it down into meaningful and manageable chunks for purposes of analysis. Coding helped to prevent the interviewer from over-emphasising the importance of any one aspect early in the study and helped ensure a thorough analysis of the entire interview (Charmaz, 2006; Stake, 2010).

21 *(Fox et al., 2007)*

22 *'Datareportal Ghana 2021, https://datareportal.com/reports/digital-2021-ghana*

Results

Prevalence of Mistrust

Public trust in data controllers is essential to building a credible data system. Unfortunately, trust cannot be achieved by a body of law, but it can be nurtured through sets of behaviours, norms, and relationships between data controllers and data subjects. Findings show that there is a high prevalence of mistrust of public data controllers among the population. For instance, only 30% of the respondents said they had trust in data controllers while 29% said they did not have trust while 41% said they somehow trusted data controllers.

Figure 1: *Trust for data controllers*

Justification for Mistrust

Respondents cited several reasons for the low levels of trust in data controllers, including concerns for data insecurity; little or no information provided on use of data; and perceived unauthorised access to data. Other reasons cited include lack of knowledge of a legislation that guarantees rights of data subjects; belief that data could be used against them; and bad experience encountered in previous engagement with data controllers.

According to the key informant from the Electoral Commission, the prevalence of mistrust has a historical nature to it.

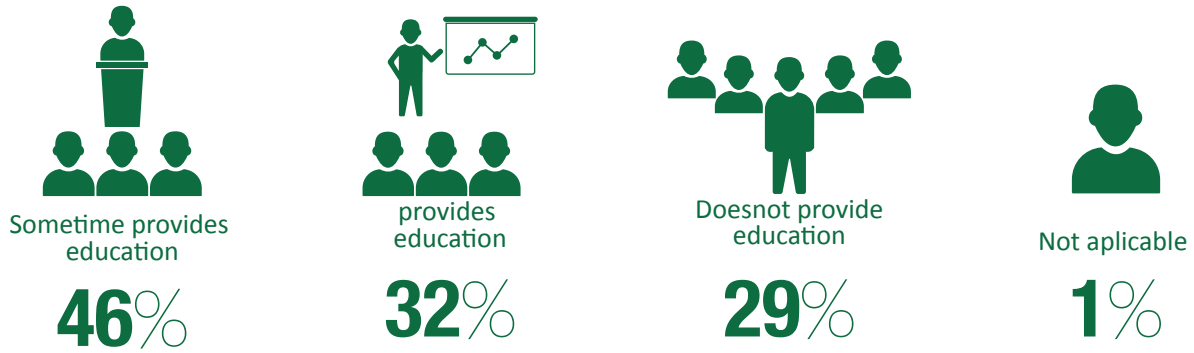
> *"Historically if you look at our evolution as a nation with colonisation, you'd observe that the colonialists started collecting data even then. But the way they went about the whole process, the people were not given sufficient education and awareness. So, it was like you collect my data, and you're going to use it for something negative, so people would shy away. Even with the poll tax many people were not ready, they were not willing to pay because they just saw it as a way of the white man getting information from them. So, we had gone as a country like that, after independence it continued, the government wanted to collect data, I think for Governance. But the way in which it was done people always adduced negativity. So that has been the [background]; somebody wants to know your name, your age, where you come from, your parents, and it is like the next minute the police will come and arrest you."*

Behavioural Effect of Mistrust

The possible behavioural manifestation of the mistrust that data subjects held towards data controllers was highlighted when respondents were asked if they shared their data if they had the choice. Half of the respondents (51%) said no. Among the reasons for not wanting to share were inadequate awareness creation by data controllers (55%); lack of knowledge of any data protection laws in Ghana (35%); lack of trust in the government (33%); and non-appreciation of the benefits of data sharing (25%).

When respondents were asked whether data controllers provided any form of education when collecting data, 32% answered yes while 21% answered no. Majority of the respondents, representing 45%, answered "sometimes". The data is presented below in figure 2.

Figure 2: *Data Controllers Educating Data Subjects*

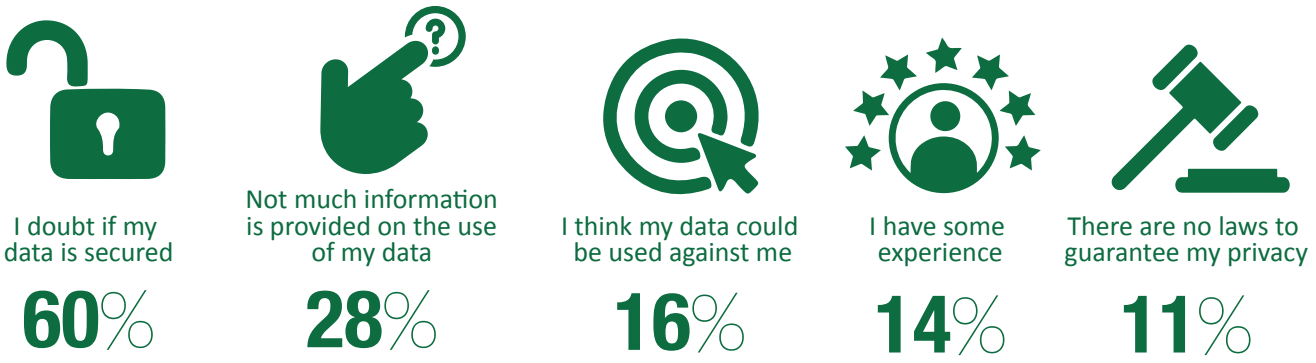


The data further reveals the need for data controllers to educate data subjects on their rights, laws protecting these rights, operational measures instituted to ensure data privacy and protection, the data cycle, purpose of data collection, benefits to be derived from data collection and processing, services that are being offered, and the recourse mechanism in place to address any grievances. This education can take the form of one-on-one briefing at the point of data collection or media campaigns via traditional and new media channels. Further, clear communication, transparent processes, user-centric engagement, and credible, visible systems for recourse could be helpful in bolstering public trust.

Sources of the Low Level of Trust

The levels of trust data subjects have towards data controllers is influenced by a combination of factors including concern for the safety of their data, and previous personal experiences of data breaches. In addition, the lack of sensitisation and clear information on the purposes of data collection breeds mistrust of what the data controller may be hiding from the data subject.

Figure 3: *Sources of low level of trust*



From the above figure, it can be noted that some respondents were not talking from a position of knowledge of the Data Protection Act, the legislation that provides guidelines on how data controllers are to collect and manage data. From the data, 54% of respondents were not aware of any law that regulates how personal information should be collected, processed, and used by data controllers – private and public. The remaining 46% had knowledge of the Data Protection Act.

On the issue of breach of privacy, regulatory interference and data subject complicity, a key informant from Zenith Bank, admitted the possibility of a customer's data leaking but was quick to note that some of the data transfers are consented to by data subjects.

> *"Some of these microfinance institutions can get information from public service workers and send them text messages advertising their products which I highly doubt they get that information from financial institutions. These people tend to wonder where they get their numbers from and that is where these suspicions come from but then, the truth of the matter is these people who are hungry to get your information use various dubious means to obtain the information from multiple sources and not necessarily the financial institutions. They can go to the telecommunication companies and try to convince them into letting them have access to the information they need."*

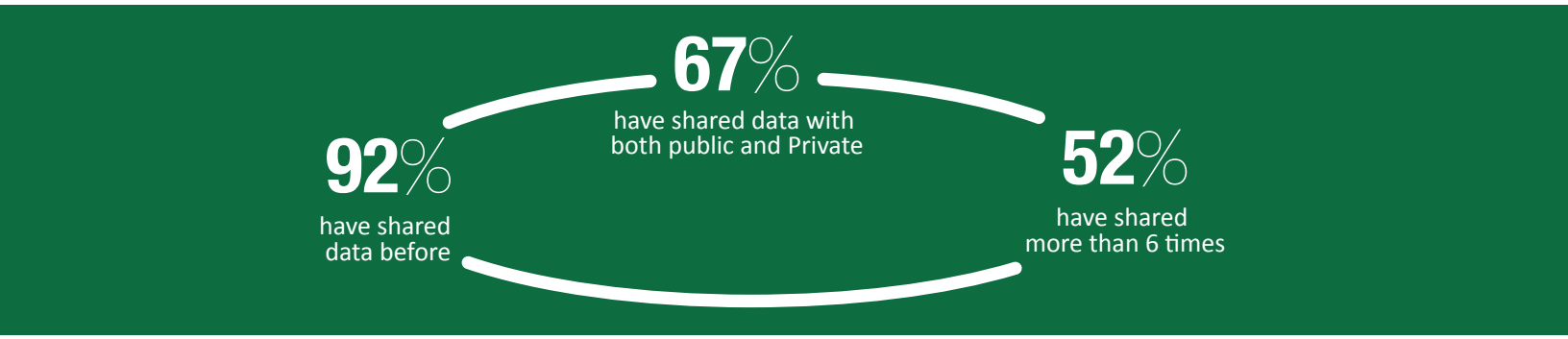
Respondents also pointed to the use or misuse of regulatory authority or executive powers to access people's personal data from especially private data controllers by the regulator. A clear example as cited is the campaign messages that citizens received during the 2020 elections from the government without their consent. Such instances of unsolicited messages erode the trust that the public has in data controllers. This act amounted to unauthorised release of individuals' data to both government and private entities in contravention of section 35 of the Data Protection Act. This section provides a comprehensive set of requirements that should be met before a data controller transfers the data of an individual to another person or entity to process. Among these requirements is the informed consent of the data subject.

Data controllers are required to inform data subjects of the processing of their personal data by the data controller or by another person or entity on behalf of the data controller. They are also required to give to the data subject, a description of the personal data to be collected, the purpose for which the data is being or is to be processed; and the recipients to whom the data may be disclosed. Additionally, the data controller must communicate to data subjects what constitutes personal data, what would be available to the data controller as to the source of the data, and the rationale behind the decision that would be made based on the processing of the data.

Experience With Giving Out Personal Data

Responses gathered from the survey show that the majority of the respondents have interacted with one or more data controllers in the process of accessing various services. The data controllers are both public and private institutions, including government agencies such as the Electoral Commission, National Identification Authority, Ghana Revenue Authority, Drivers and Vehicle Licensing Authority, and the Passport Office. The private ones are mainly financial institutions, telecommunication companies, schools, and hospitals. From the data, it emerged that 92.1% of respondents have shared their data with both public and private institutions. More than half (52%) have shared their data more than six times. Those who had shared their data 1-3 times were 24.7%, while (16.2%) had shared 3-6 times. From this, it can be inferred that the majority of Ghanaians are sharing data with public and private institutions.

Figure 4: *Institutions that respondents have shared their data with*



Lack of Knowledge on the Use of Data

Section 20 of the Data Protection Act, 2012 requires data controllers to seek consent of data subjects, provide them with information on why their data is being collected, and what value it brings them. However, the findings from the study shows that 50% of the survey respondents either do not know or are not sure of what their data is being used for, with only 47% of the respondents asserting that they know what their personal information is being used for. When asked why they do not know, 35% noted that they had no opportunity of knowing or asking; 27% said they usually do not ask; 8% do ask but never get satisfactory answers; 8% are in a hurry to complete their process; while 4% do not see the need for asking.

Part of the focus of good data governance practice should be to provide data subjects with the power to enforce their rights against data controllers in a cost-effective manner. Knowing their rights and responsibilities under the relevant laws as well as the value exchange for sharing their personal data is one of the surest ways of building trust with data subjects. A study conducted by the Centre on Global Brand Leadership in partnership with the Aimia Institute in 2015 found that data subjects are more willing to exchange sensitive data for a product or service they value.[23]

However, according to the key informant from the National Communications Authority, most of the time, the public is not willing to take time to study and understand the things they are signing up for or the kind of personal data they are sharing, especially the terms of services for digital products.

> *"In most instances, the public is so lazy that they feel reluctant in reading certain texts or terms of agreement before agreeing to it simply because they are in a hurry. Along the way, these users receive messages or information and won't understand why those messages keep on coming, foregoing the fact that they had subscribed earlier on to these prompts without reading the terms. Complaints are later made at the various network offices saying they don't understand why they keep receiving messages."*

[23] *Aline Blankertz & Louisa Specht, What Regulation for Data Trusts Should Look Like (Berlin, 2021) https://www.stiftung-nv.de/sites/default/files/regulation_for_data_trusts_0.pdf*

Condition Under Which Trust Can be Fostered

As shown in figure 5, respondents provided suggestions in fostering public trust in institutions charged with collecting and processing data. These include installing systems that ensure data is not leaked, breached, or abused; adequate education on the handling and usage data; and the enactment of stricter laws to protect data and uphold the rights of data subjects. Respondents also want to have the opportunity to delete or alter their data any time they want. Most respondents were happy to provide data so long as it goes to improve service delivery. This ties in with the conclusion reached by Centre on Global Brand Leadership (2015) that data subjects are willing to share their data when they know data controllers can help them understand and control how their data is used. From the data, it appears respondents are more comfortable sharing their data with private data controllers than with public ones. Majority, representing 41%, trust private data controllers more than public data controllers (24%), while 35% trust neither of them. Measures must be put in place to address the mistrust of public data controllers as this has implications for elections, revenue mobilisation and government service delivery.

Figure 5: *Conditions on which data subjects will trust data controllers*

Conclusion and Recommendations

The findings show that Ghanaian citizens have a low level of trust in data controllers based on how they collect, store, process, share, and discard data. Inadequate public education, lack of awareness on legislation, doubt in safety of the data governance systems, occurrence of data breaches and regulatory interference, non-enforcement of existing data privacy and protection legislation, have been identified as major sources of the low level of trust. In turn, this low level of trust is affecting both public institutions such as the Electoral Commission, National Identification Authority, Ghana Revenue Authority, Drivers and Vehicle Licensing Authority, and private ones like financial institutions, telecommunication companies, schools, and hospitals. Nonetheless, there is a high level of sharing information with these institutions.

While Ghana has in the past years enacted legislation to support the effective, efficient, and responsible data governance, a key missing link is the enforcement and effective implementation of the existing legislation on data governance.

Consequently, our recommendations are aimed at addressing the key causes of the low trust in data controllers so as to improve data governance in Ghana.

Government:

- Government must ensure that data controllers adhere to the Data Protection Act, especially the provisions on security measures, right to informed consent, right to object to processing of one's personal data and the right to participate in the process.
- The government should put in place an accountability mechanism where the Data Protection Commission receives direct feedback from data subjects on specific themes after contact with a data controller. This will enable the government to hold data controllers accountable and to appropriately enforce the necessary laws and regulations.
- Government should conduct public education and awareness raising activities as these are very crucial and remain some of the key drivers of the low participation and trust among data subjects.

Data controllers – public and private:

- Data controllers, who have the right or are assigned the responsibility of collecting, processing, storing, and transferring data, have a duty to ensure that the data governance system is safe, reliable, and responsive.
- Data controllers need to adhere to the existing laws and regulatory frameworks within the data governance system while placing above all other considerations the safety, security, and privacy of their data subjects.
- Data controllers should mainstream public education and ensure professional handling of the data they collect and hold.

Civil Society Organizations (CSOs):

- CSOs should conduct research and policy advocacy and engage government and other key stakeholders with the objective of promoting compliance with laws and respect for the privacy and security of the individual data subject .
- CSOs should independently and/or in partnership with public institutions sensitise and raise awareness on data rights and data governance.
- CSOs should also broker partnerships with government and data controllers to hold fora, seminars and outreach programs aimed at deepening understanding and building trust among citizens.
- The media should partner with both public and civil society organisations to educate the masses on data rights and data governance.
- Media should also investigate and report on all reported cases of data breaches by both public and private data controllers.

References

Afrobarometer, *Corruption and Trust in Political Institutions in Sub-Saharan Africa (Accra, Ghana, 2008)*

Ansah, Marian, *'Communications Ministry Fights BoG over Mobile Money Data', Citinewsroom.Com (Accra, Ghana, 14 November 2018)*

BBC, *'Voters List 2020: Ghana Electoral Commission Publish Final Voter Register Online for 7 December Election', BBC (Accra, Ghana, 30 November 2020) <https://www.bbc.com/pidgin/tori-55138308>*

Center on Global Brand Leadership, 'What Is the Future of Data Sharing?', *Columbia University, 2021 <https://www8.gsb.columbia.edu/globalbrands/research/future-of-data-sharing> [accessed 20 November 2021]*

Chawda, Viral, *'Building Trust in Government's Use of Data', KPMG <https://home.kpmg/xx/en/home/insights/2018/06/building-trust-in-governments-use-of-data.html> [accessed 7 April 2021]*

Citinewsroom, *'Communications Ministry Fights BoG over Mobile Money Data', Citinewsroom (Accra, Ghana, 14 November 2018)*

Colebatch, *H.K., 'Making Sense of Governance, Policy and Society', 33.4 (2014), 307–16 <https://doi.org/10.1016/j.polsoc.2014.10.001>*

CTVET, 'Ghana Targets a 40 Percent Increase in Enrolment in Tertiary Education by 2030', 2021 *<https://ctvet.gov.gh/ghana-targets-a-40-percent-increase-in-enrollment-in-tertiary-education-by-2030/> [accessed 21 November 2021]*

Donna L. Hoffman, Thomas P. Novak and Marcos Peralta, *'Building Consumer Trust Online', Communications of the ACM, 42.4 (1999), 80–85 <https://doi.org/10.1145/299157.299175>*

Government of Ghana, *Data Protection Act of Ghana 2012 (Ghana: Act of Parliament, 2012) <http://www.dataprotection.org.gh/sites/default/files/Data Protection Act , 2012 (Act 843).pdf>*

Greenleaf, Graham, *'Global Data Privacy Laws 2019: 132 National Laws and Many Bills', Privacy Laws & Business International Report, 157, 2019, 14–18*

'Household Survey on ICT in Ghana' *<https://statsghana.gov.gh/gssmain/fileUpload/pressrelease/Household Survey on ICT in Ghana (Abridged) new (1).pdf>*

Kooiman, J, 'Problems and Opportunities (First-Order Governance). *In Governing as Governance', SAGE Publications Ltd, 2003 <https://doi.org/https://www.doi.org/10.4135/9781446215012.n9>*

Lawrence, Sylvie Delacroix and Neil D, *'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance', International Data Privacy Law, 9.4 (2019), 236–52 <https://doi.org/https://doi.org/10.1093/idpl/ipz014>*

Mayer, Roger C. Davis, James H. and Schoorman, F. David, *'An Integrative Model of Organizational Trust', The Academy of Management Review, 20.3 (1995), 709–734 <https://doi.org/https://doi.org/10.2307/258792>*

Ministry of Communication, *'Launch of GH COVID-19 Tracker App', Ministry of Communication (Accra, Ghana, 2020) <https://www.moc.gov.gh/launch-gh-covid-19-tracker-app>*

National Identification Authority, *'Our History', National Identification Authority, 2020 <https://www.nia.gov.gh> [accessed 7 April 2021]*

Nick Fox, *Nigel Mathers, and and Hunn Amanda, Surveys and Questionnaires, Surveys and Questionnaires (East Midland, 2007) <https://doi.org/10.4324/9780203154281-35>*

Nookala, Raghav, *'Data Governance Models: Which Model Best Suits Your Organisation', 2016 <https://nttdata-solutions.com/us/local-blog/grc-and-security-local-blog/data-governance-models-| four-models-and-how-to-choose-which-is-best-for-your-organization/> [accessed 12 October 2021]*

O'Neil, C, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (Crown Publishing Group, USA, 2017)*

Public Sector Network, *'Public Sector Data Governance: Five Reasons Why Information Management Frameworks Are Crucial', Public Sector Network, 2020 <https://publicsectornetwork.co/insight/five-reasons-for-public-sector-data-governance/> [accessed 19 November 2021]*

Specht, *Aline Blankertz & Louisa, What Regulation for Data Trusts Should Look Like (Berlin, 2021) <https://www.stiftung-nv.de/sites/default/files/regulation_for_data_trusts_0.pdf>*

Vaughan, *Craig Stedman and Jack, 'What Is Data Governance and Why Does It Matter?', 2020*

Williams, *B. A., Brooks, C. F., & Shmargad, Y, 'How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications', Journal of Information Policy, 8 (2018), 78–115*

'Women Rights Online' *<https://webfoundation.org/research/womens-rights-online-2020/>*

World Bank, *'School Enrollment, Tertiary (% Gross) - Ghana', World Development Indicators | DataBank, 2021 <https://data.worldbank.org/indicator/SE.TER.ENRR?locations=GH> [accessed 20 November 2021]*

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
+256 414 289 502
programmes@cipesa.org
@cipesaug facebook.com/cipesaug Linkedin/cipesa
www.cipesa.org