

A Value Assessment of Personal Data: Towards Greater Privacy Consciousness in Africa

Efe Lawrence-Ogbeide¹, Chiemeka Felix Nwosu², Olumide Babalola³

¹Faculty of Law, University of Montreal, Montreal, Canada

²Data Protection and Intellectual Property, The University of Law, Leeds, United Kingdom

³Faculty of Business and Law, University of Portsmouth, Portsmouth, United Kingdom

Email address:

efe.lawrence-ogbeide@umontreal.ca (Efe Lawrence-Ogbeide), chiemekafnwosu@gmail.com (Chiemeka Felix Nwosu), olumide@oblp.org (Olumide Babalola)

To cite this article:

Efe Lawrence-Ogbeide, Chiemeka Felix Nwosu, Olumide Babalola. A Value Assessment of Personal Data: Towards Greater Privacy Consciousness in Africa. *International Journal of Law and Society*. Vol. 6, No. 3, 2023, pp. 229-240. doi: 10.11648/j.ijls.20230603.18

Received: July 11, 2023; **Accepted:** July 27, 2023; **Published:** August 5, 2023

Abstract: The world has become a global village, as the digital age has increased our interconnectedness. A crucial component in this digitalization era is personal information-based data or big data; literally, the string that connects many modern devices and web applications most people today cannot live without. Accordingly, a reinforced consciousness drive towards personal data protection is pivotal. This is the core of this article, and our focus is Africa. On the one hand, it can be argued that African legal regimes contribute to a situation where laws are either unnecessarily delayed or, if they exist, do not necessarily address the peculiar circumstances of the clime, but rather use a 'cut and paste' approach. On the other hand, there is the question of how much responsibility individuals impose on themselves, in terms of safeguarding their personal information when exploring the digital age, we live in. This article takes a comparative approach to consider both factors, emphasizing the critical need for improved privacy consciousness in African countries, as the number of its people using smart devices, the internet, and other data-based applications, grows. The work is particularly relevant, considering that primary data protection laws are evolving in the region.

Keywords: Africa, Data Protection, Personal Data, Privacy, Privacy Consciousness, Privacy Paradox

1. Introduction

Laws have long existed to guarantee privacy or private life, central of them the universal human right to privacy. However, with respect to its coverage of this relatively 'new' class of privacy – personal data, the realities of the digital age have subjected that right to questioning in some jurisdictions. Hence, some jurisdictions have beyond the traditional right to privacy, further created and adopted a new class of fundamental right – the right to data protection. The Charter of the fundamental rights of the European Union provides for this in Article 8. It has been argued that although the two rights are distinct, they heavily overlap [53].

There have been instances where even the jurisprudence in the EU is seen to oscillate between the interpretation of private life as including the protection of personal data sometimes and other times, not including [43]. Nevertheless,

with the provision of Article 8 of the CFREU, the rights stand demarcated and are to be treated so. As a result, the discussion over whether or not data protection could be regarded a fundamental right is rendered moot. Where there are no demarcations and no ambiguity, data protection can be effectively argued to fall under the right to privacy or not, depending on the facts of each instance. In Nigeria for instance, the court decisions have oscillated between both arguments and the position whether personal data breaches must be accommodated under the right to privacy enshrined in section 37 of the 1999 Constitution of the Federal Republic of Nigeria ("CFRN"), remains largely undefined. For example, on the one hand, in the case of Incorporated Trustees of Digital Rights Lawyers Initiative v. The National Identity Management Commission, LPELR – 55623 (CA, 2021) [24], the Nigerian Court of Appeal held that the right to privacy under Section 37 of the CFRN ought to be interpreted expansively to include protection of personal data

under the Nigerian Data Protection Regulation (“NDPR”). On the other hand, in the unreported case of Incorporated Trustees of Laws and Rights Awareness Initiative v. The National Identity Management Commission, Suit No. FHC/AB/CS/79/2020, the Federal High Court of Nigeria held that breach of a Data Subject’s right under the NDPR is not (necessarily) a breach of the right to privacy under the CFRN.

Whether as part of the right to private life or on its own as the right to data protection, data protection rights are today more popular than they were a little less than a decade ago. With the emergence of the GDPR, many jurisdictions across the globe have sought to define or modify their own data protection regimes. Given the pervasiveness of personal information today, as well as its immense worth, it is crucial that individuals understand not only the reality of the digital age in terms of their data but also their rights or remedies existing to safeguard undue exploitation of this data. Our main objective, therefore, is to give an assessment of the value of personal data, geared towards increased privacy and data protection consciousness in African countries, particularly. Our hypothesis is that there is an underestimation of the value of Personal Information (PI) by users in some cases, in other cases, no interest in knowing at all. Where however, there may be some estimation, we hypothesize that individuals do little or nothing to maximize the potential value of their personal data. We therefore call for further research for data protection legislation in African countries, nuanced by provisions enabling models for maximizing the value of PI, whether in a monetary sense or otherwise. Moreso, as many African countries are still in the stages of developing primary laws for the subject matter.

There are two parts to this article. Part one emphasizes the importance of personal data to individuals and then to tech giants. Part two will go on to discuss the potential threats and risks in today’s technologically driven world, to paint a picture of what people face when they (in)voluntarily give away their PI, sometimes in exchange for something they believe is reasonably valuable in comparison to what is given away. It will then analyse African countries’ efforts to solve these concerns through various legal frameworks. We conclude our thoughts by addressing the ‘privacy paradox,’ in which individuals have a behavioural pattern that contradicts their theoretical claim to privacy, and thus argue for greater individual responsibility.

2. The ‘Gold’ in Personal Data

Most of the new and trending technologies of the 21st century heavily rely on data to run. These technologies typically collect, store, or share personal information belonging to users. For example, the Internet of Things (IoT) which refers to a concept of connected objects and devices of all types over the Internet wired or wireless [71]. IoT relates to the ability of devices and objects to connect to the internet to essentially send and receive data in a more advanced manner than we have been accustomed to. These devices typically carry built in wireless internet connectivity for them

to communicate. Home automation systems, home appliances and even certain medical devices show how this technological phenomenon has been impactful [48]. With the number of connected smart devices projected to rise to a number between 20 and 50 billion from the year 2020 [45], the implication is that an increasingly high number of devices will have the capability of connecting to the internet, ranging from personal devices and gadgets such as refrigerators, doorbells and toys, to office computers and devices. In the past, Africa was said to have a slow rate of adopting IoT compared with other continents [57]. Only short of a decade after, the projections of an increase in IoT revenue which is invariably linked to adoption, is not a surprise, considering the population of some countries in the continent [39]. The stats by GlobalData show the rate of IoT growth in Africa, like its middle eastern counterpart. Similarly, the statistics by Statista show an upward trajectory for IoT revenue in Nigeria [36] and in South Africa [37], with their IoT market’s largest segments being smart home technologies. The implication is that the IoT phenomena is becoming increasingly popular in Africa, with the potential widespread use of IoT devices and these IoT gadgets generate a massive amount of data, belonging to users.

Additionally, Africa as with most other parts of the world, is experiencing a mind-blowing increase in the number of internet users. As of April 2022, there were five billion internet users worldwide, amounting to sixty three percent of the global population. Out of this number, 4.65 billion or over 93 percent were social media users [38]. Bringing it home to Africa, Nigeria the most populated in the continent and one of the most populous in the world has a record of 84 million internet users with an internet penetration amounting to 38 percent of its population. Almost 81 million out of the 84, is said to be mobile internet usage. Its South African counterpart has about 80% of their population recorded as internet users. These numbers are not far-fetched. Today, there is a proliferation of applications that individuals are hooked on, whether for business, research, or pleasure. In this ‘addiction’ to the applications lie the gold, the applications themselves, the ‘mining’ field; technology firms the ‘miners.’ The big technology firms like – Google, Apple, Facebook, Amazon, Microsoft (GAFAM) arguably, the biggest participants.

A common business practice that prevails with GAFAM and even smaller tech firms, is advertising. An interesting New York Times piece refers to it as “the central villain” of the internet that needs to be restrained [50]. Indeed, the digital advertising business is the gold mine that transforms raw gold - latent attention, into fine gold – real or literal wealth, put in the coffers of the tech businesses. Digital advertising operates by targeted advertising which is a type of marketing strategy that involves tracking people’s online behaviour to show people, individually targeted advertisement. It involves monitoring people’s online behaviour and using the collected information. Information about millions of people is collected for this purpose. For instance, in 2015, Facebook said it had 1.55 billion monthly

active users, today in 2022, it is roughly 2.96 billion [75, 26]. Google as at 2013, said it had 90% of Internet users worldwide within its reach [52]. Targeted advertising has its good and its ugly sides. As consumers, people make satisfied purchases, faster and sometimes cheaper. On the flip side, it can be misused for example, for discriminatory practices, digital propaganda, etc. The scope of this article limits us from discussing all these, extensively.

The power for surveillance held by the internet and by extension actors in the business, is huge. Just as with private actors, for state actors too, the unimaginable extent of personal information out there should not be underemphasized. In the US case of *State of Arkansas v. James A. Bates*, Case No. 2016-370-2 (Ark. Cir), the defendant was charged with first-degree murder with the help of evidence collected by his Amazon Echo smart speaker. Although the prosecutors later dropped the charges against him, the case raises privacy issues such as ownership of personal data collected from personal devices in light of criminal allegations against the device owner. In that case, Amazon initially declined to share data from its servers noting that the company will not release customer information without a valid and binding legal demand properly served on them, although they eventually released the information after Bates consented to the release. While the case revealed that the records of the smart speaker are stored in Amazon servers, it also exposed the ambiguities in existing laws to define when control of personal data passes from the owner of an IoT device to appropriate authorities. Similarly, in an interesting trial popularly known as the “fitBit trial – *State of Connecticut v. Richard Dabate*, TTD-CR17-0110576-T (JD Tolland, 2022), a jury has now recently found Richard Dabate guilty of murdering his wife in 2015 at their home. Here also, a fitness wearable belonging to the victim provided specific details to the police in charging the victim’s husband who had a contradicting version of the events surrounding her death. State police, doubtful of Dabate’s story conducted a detailed investigation which included obtaining data from Connie Dabate’s (the victim) Fitbit, posts to social media and data from their home’s alarm system.

While the revelation in some of these cases have been invaluable in tacking criminal activity and pursuing civil claims, this article focuses on the consequential privacy issues raised in them. Many times, data collected for public and national security purposes constitute personal data, which raises a conflict between two key interests - security and data protection [27]. Again, we are limited by the scope of this article only to analyse the latter, as it relates to the value of personal data to private actors. The overarching point to note however, is that technologies and businesses today depend on the personal information of individuals to thrive, and with the widespread usage of the internet and IoT devices, personal data is almost inevitably disclosed, used, and collected. These data can be used to establish what we are interested in, where we go, our intentions, etc. While this can provide great opportunities for improved services, it must

be weighed against our desire for privacy.

3. The Value of PI from the User’s Perspective

The reality of the digital age necessitates a better understanding on the part of owners of PI, of the intricacies of their ownership. Ownership in this context is drawn from its very definition. Used interchangeably with the term personal data, PI has been defined similarly, across countries, to be “information relating to an identified or identifiable individual” [30]. The similarity in definition is found for example in transnational policy instruments such as the 1980 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; the 1981 OECD Guidelines for the protection of privacy and transborder flows of personal data, etc. The definition of personal data given by the gold standard GDPR is “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

3.1. Demystifying the Concept of PI

The challenge with the GDPR definition of personal data above, is that, as new technologies push the bounds of data protection, identifying a person has gotten more difficult. Debates over these complexities continue, resulting in varied provisions in various countries’ laws and even the literature. For example, the Dutch data protection authority considers face detection in relation to smart billboards to be personal data processing, whereas its Irish counterpart does not [63].

The meaning of identifiable under the GDPR (which is similar to the provisions of the data protection Directive 95/46/EC) [25], has been argued to be too broad, especially after the decision of the Court of Justice of the European Union (CJEU) in the 2016 *Patrick Breyer v. Bundesrepublik Deutschland* case, Case No. C-582/14 (Sec. Ch. 2016) [16], where the court took the position that a dynamic IP address in the hands of a website publisher is a piece of personal data, if the publisher has the legal means enabling it to identify the visitor [9]. The decision in the case suggests that data will continue to be personal even if legal means are required to make a person “identified.” This does suggest a very broad definition of “identifiable,” which contrasts with the narrowing approach on identification provided by the Article 29 Working Party (WP), an independent European working party that dealt with issues relating to the protection of privacy and personal data until May 25, 2018, when the GDPR went into effect.

With regards to information relating to a natural person that is “identified or identifiable”, the WP considers “a natural person as “identified” when, within a group of

persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix "-able")... [80]. The approach of the WP is to 'zoom in' to identify an individual beyond just a name, for instance. Regrettably, while the GDPR itself is binding, the opinion of the WP, though influential, are not necessarily binding, raising questions of how identification under the GDPR itself should be interpreted or understood [63]. Clearly in *Breyer*, the WP's interpretation of identification appeared to have been ignored.

Additionally, some commentators have argued against the uncertainty raised by certain data, proposing the need to modify the definition of PI in light of current trends and realities. Eloise Gratton refers to the uncertainty raised with IP addresses and the varying schools of thought as to whether IP addresses constitute personal data, citing oscillating court judgements in the same jurisdiction – France [30]. John Thompson argues that the borders between private (personal) and public are highly contested and contestable [42]. Others have argued against the notion of personally identifiable information. Purtova also argues that due to the dynamic approach to the definition of personal data (especially adopted in Europe), the lines between personal and non-personal data can get blurry, creating a difficulty to relate the data to an identifiable natural person [62]. Ziegeldorf et al argue that there are ambiguities in existing legislation regarding the notion of personally identifiable information (PII) [84]. These arguments largely spring from the nature of the cyberspace which indeed, is the most natural habitat for a fluid dissemination of personal information [14].

3.2. *Estimating the Value of PI*

The implication of the foregoing discussion is that where however, an individual can be identified or identifiable through information relating to him/her, then that information may be classified as personal data. What identifies an individual could arguably be as simple as a name, a number or an IP address or a cookie identifier, etc., giving quite a wide spectrum. However, the focal point is that, with prevailing technological realities and modern practices, ownership of personal data becomes more complex to define and manage. Notwithstanding, from the viewpoint that PI can be ascertainable one way or the other (more so, by legal interpretation), regardless of its fluid nature, its ownership must then be duly recognized and respected, with lawful transfer complied with. However, the practises of today's big techs raise the critical problems of what constitutes legal and lawful transfer of PI, and to what extent is compliance with such rules observed? We now explore the topic of transfer as a basis for benefiting from the value of PI, having discussed the worth of PI extensively in part 1 of this essay, and with an attempt here to additionally highlight the foundation for ownership.

Data has been defined to be a digital representation of information and to have several classifications, including

personal data which forms the basis of the discussion in this article [64]. As data is defined by information, they are therefore considered closely linked. With respect to what forms information, we find the "functional" approach to defining information adopted by Purtova and Maanen, interesting. According to them, information is not defined by what it is, but by what it does [64]. Their analysis is used to define under what circumstances data can be considered as an economic good; for instance, whether as non-rivalrous, i.e., used infinitely; or excludable, i.e., where access to it may be blocked by technological means such as encryption; etc. They further reasonably argue that the realities of technological advancements nowadays, make allowance for a (data) pools settings, in which data can be managed, akin to walled gardens or clubs where access is granted to paying customers only for example, and all others excluded from the benefits of membership. This is not to say that excludability fully deals with the issue of free access to personal data, especially by GAFAM, but that at the least, individuals can have the option of barricading unauthorized and illegal access to their data, in the form of security measures and legal prohibitions, which then makes data excludable.

This analysis is relevant to our discussion to the extent that, it is agreeable that data may be excludable, and, on that basis, the owner of data can sufficiently regulate the transfer thereof, depending on their judgement of what they stand to benefit. Value is estimated by what the owners of PI are willing to receive in exchange for their PI. The value could also be determined by what owners of PI are willing to pay to protect their information. A survey [70] which gathered responses from 5,000 adults in six countries: Australia, Germany, Japan, New Zealand, the United Kingdom (UK) and the United States (US) revealed that 39% liked the idea of monetary compensation from a company for sharing their personal data. 20% claimed they most value product discounts. Although 91% of survey respondents worry about the potential abuse of their personal data, some are interested in financial compensation, others prefer greater convenience in using services and more responsive customer service and support in exchange for sharing their personal data with a company. Money interestingly tops the list.

Consequently, consent to transfer PI in exchange of benefits, whether monetary or otherwise becomes pivotal. Whether a person chooses to transfer their PI is then totally up to them and what they want; and consent becomes truly central [44]. The import of consent for instance, is that websites and embedded third parties obtain the requisite approval to collect, process, and share individuals' personal data [47]. However, despite the regulatory and compliance measures put in place by regulators and site owners respectively, compliance to consent requirements remain on shaky grounds [47]. Research in the past has shown that online services go as far as often deceiving users to obtaining their positive consent [51]. Consent is therefore crucial in the consideration of value of PI, to a consumer, as well as in the general discourse on privacy and data protection in Africa.

4. The Value of PI to Private Actors

In the digital ecosystem, personal data means different things to the players - tech companies, their intermediaries, and the consumers. For tech companies, the value of personal data to their business has been particularly emphasized by these peculiar business entities' meteoric rise and dominance in world politics and economy in the last decade. Tech companies (especially Big Tech) now control the services and products narrative as much as they dominate political economies [7]. The value derived by private actors from their routine accumulation and control of personal data will be discussed under two subheadings of monopolistic or anti-competitive interests and the 'assetization' of personal data for profits. Even though the latter is sometimes waved off as a negligible portion of the broader problems, it underscores the insufficiently unanalysed risks or detriment that legal or untoward harvesting of personal data poses to consumers [6].

4.1. *Assetization of Personal Data from a Business Perspective*

Within the context of the value propositions from the collection of personal information rather than a fixation on the property rights assertible by consumers, this section is concerned with the granular benefits that private actors (and their prospective investors) derive from their collection and access to consumers' personal data without necessarily laying claim to the ownership of the database as an asset itself [4, 31, 33, 41].

Access to consumers' online activities and their engagement on various platforms translate into quantifiable assets which tech companies and their investors utilize for varying business objectives [8]. Just like choses in action, personal data are viewed by tech companies as intangible assets [61]. The asset in personal data from business perspective appears in two transactional realities: first, it represents the product when used for varying business revenue-generating purposes and secondly, it is the lifeblood of corporations which economic activities depend on [45] hence, the expression - data is the new oil [40]. For companies with the business model of operating search engines or social media site, personal data gathered across these various platforms have become products which are sold to potential investors. From the business perspective, monetizing personal data amassed through technology, these companies have become 'the energy or new money of the digital world' [68].

4.2. *Transactions in Personal Data Markets*

The commodification of personal data is further accentuated by the 'establishment' of personal data markets. In these invisible markets, as a business model, companies or data brokers auction the personal data of millions of web users collected using various platforms [69]. A study conducted by Bolton Consulting Group speculated that personal data markets can generate 330 billion Euros in economic value to companies in Europe and this figure, by

extension includes that of Africans [76]. While these personal data markets are invisible and largely unstructured, data brokers play the role of intermediaries connecting parties and facilitating transmission for the exchange of users' personal data which may include their profiles and life stories shared on social media [3].

To maximize profits accruable from use and sale of personal data, companies invest in software that ease the harvest, appropriation, and storage of consumer data as the stock-in-trade for these businesses [67]. These invisible markets control digital economics, remain largely unstructured and in 2017, the estimated revenue per user was valued at 56 US dollars with the African valuation slightly lower [83]. The market itself is a network that facilitates the production of personal data by various systems predominantly driven by commercial forces with the sometimes unconscious participation of users [72].

4.3. *Secondary Layer-Value from Aggregation and Analytics*

4.3.1. *Aggregation for Anti-Competition Purposes*

The proliferation of social media platforms and online advertising facilitates the mass collection of online consumers' personal data and behavioural patterns. As a matter of business routines, (large) corporations gain access to their customers' personal data and online transaction trails which information are converted to different uses subject to their respective business models. The dynamics of all these are not lost on African markets as GAFAM are estimated to hold massive data of African residents as much as their European counterparts. A 2021 Report estimated 15% growth for the African data market between 2020-2028 with Egypt, South Africa, Kenya, Morocco and Ethiopia as entire participants [18].

In 2017, Apple's sale of millions of smartphones and Facebook's opening of over 30 million accounts gave the companies access to users' personal data which information was later used to monitor and analyse their consumers' online behaviours for the respective companies' market gains [13]. Within the context of benefits accruable to businesses from dealing with personal data, anti-competitive tendencies constitute the 'collection mining of personal data legally or otherwise for dominant advantage in any market' [78]. Data mining provides businesses with a graveyard or pool of personal data which gives them access to specific consumers' information not available to other market players which do not have the capacity or financial muscle to access such information. Data mining is now accepted as an industry-wide tool enhancing anti-competitive practices by using extracted to gain dominant market advantage customers' information [32].

Organizations have profited from using consumers' information mined to, at the expense of their competitors, detect credit card fraud, analyse consumers purchasing power and behaviours, predict consumer personal preferences to improve services and products [54]. For instance, in a case before the US Federal Trade Commission, between Google

and Double Click Inc it was revealed that Google reportedly denied their competitors access to their own share of consumers information - Meta data - used for global online advertisement to the detriment of their rivals [11]. Anti-competitive control over consumers' personal data is usually exercised in two broad ways. First is the acquisition of personal data through exclusive agreements executed by advertising partners barring them from using competitors' services. Again, Google has been accused of these sharp practices when they executed intermediation agreements mandating publishers and their visitors to exclusively use their search engines while preventing access to other search engines on Google's platform. This exclusively enables Google direct traffic to its search engine and consequently harvest massive consumer data to the exclusion of other search engines [28]. Secondly, anti-competition issues also arise where service providers refuse to honour consumers' right of data portability by transferring the accumulated personal data to rival service providers [77].

4.3.2. Acquisition for Target Marketing and Advertising Revenues

In maximizing profits from purchased consumers' data, investors engage in direct marketing by targeting consumers whose personal data meet their specific criteria [12]. The value proposition here is measured in terms of revenues generated from such target advertising and eventual market sales [82]. Companies use accumulated personal data to track their customers' online behavioural patterns and then tailor their advertising campaigns towards the perceived needs of their customers. On the flip side, maintaining a robust pool of consumers' data improve the companies' marketing choices by enabling them to target their customers' specific needs, hence reducing the companies' budgets for advertisement expenses [23].

When companies analyse and aggregate consumer data internally collected or bought from data brokers, they predict specific industry trends along the line of market demands and consumer preferences. This information enables the companies to make projections towards minimizing losses and maximizing returns on their investments. All these are quantified in terms of profits for such companies, hence boosting their revenue drives [2].

5. Threats and Risks to Privacy in an Interconnected World

As noted in earlier paragraphs, in the privacy debate, two problematic concepts are the differentiation between 'privacy' and 'data protection'. Some critics consider privacy and data protection to be identical [20] while others hold divergent views [15]. Attempts have even been made to distinguish the sphere of privacy from that of data protection utilising case law from the European Commission and Court of Human Rights (ECtHR) interpreting the right to privacy entrenched in Human Rights Treaties. Whatever be the case, one thing that is clear is that both concepts are interrelated, and the

importance of privacy cannot be overstated. Legal scholars, philosophers, and social scientists all agree that having the freedom to live one's own life and not having unauthorised access to one's personal information are fundamental components of what it is to be a human [55].

This is also compatible with public law jurisprudence, which is why the European Convention on Human Right has been repeatedly interpreted to wit, that "the idea of personal autonomy is a fundamental premise underpinning the interpretation of the Convention's guarantees" and grants individuals "the capacity to conduct one's life in a way of one's own choice" [56]. Thus, every intrusion into a functional adult's personal information space therefore undermines one part of his or her autonomy, such as the freedom to be as publicly accessible or inaccessible as he or she wishes. And in areas of our life where we have realistic expectations of privacy - like the control and processing of sensitive identifiable personal information by data controllers - a premium is placed on its accessibility through an extended data protection framework and enforcement mechanism to ensure added protection.

A consequence of increased global connectivity using the internet and social media is a tantamount increase in the risk to the privacy of the personal information of active digital users whose number currently stands at about 5 billion globally [35]. Data subjects are frequently required to provide their personal information before they are allowed full access to the operating platforms who would then have control of their information. As a result, there may be increased privacy hazards that people and organizations need to be aware of and the media is awash with accounts of prominent technology companies and brands losing control, selling consumer's personal information on their own initiative, or suffering data breaches that left millions of personal records vulnerable to misuse by mischievous others. Although, the African continent is considered to be the least connected in the world [79], it is not left out as 2022 witnessed a handful of these privacy threats:

In Angola, the Data Protection Agency (ODA) in April 2022 fined a Savings and Credit Bank for publicly disclosing the personal data of 278 of their employees on their social media platforms without authorization [10]. Also, on December 21, 2022, the Kenyan Data Protection Commissioner (ODPC) issued its first penalty notice of Five Million Kenyan Shillings (KES 5,000,000) against the Kenyan arm of the multinational technology company 'Oppo', following an enforcement notice against the company for using a complainant's photo on their social media platforms without consent. In Tunisia, Mali and Senegal the respective Data Protection authorities also issued administrative sanctions in 2022 for various violations of data protection law threatening the privacy of individuals, especially by multinational giants [66]. In Nigeria, three law suits filed early in 2022 are still pending before the court alleging; the use of tracking technologies by government agencies which are embedded with shrouded trackers that are capable of monitoring the online activities of anyone that

uses their software, unauthorized disclosure of law enforcement database containing private information and, non-compliance with the Data Protection Regulations in whitelisting countries on an international data transfer allow-list without proper checks [34].

Individuals and organisations must be aware of these many challenges and risks to their privacy in our increasingly interconnected society which can be surmised to include data breaches and cyber-attacks, unsanctioned surveillance and tracking activities, increased identity theft and fraud, heightened cases of loss of control of personal data by the Tech Giants as was made popular in 2021 following the UK Supreme Court's landmark judgement concerning Google's loss of control of the sensitive personal data of 4 million iPhone users through an unsolicited sanction of a tracking technology [46], which could result in tantamount cases of loss of privacy and autonomy [55]. These developments have generated widespread concerns around how to improve security frameworks over the personal data we provide because as internet usage continues to rise, and the volume of data being produced and stored continues to rise, data protection through robust legal and regulatory framework becomes more and more crucial.

6. A Synopsis of the Legal Regimes for Privacy in Africa

The data protection frameworks of African Union (AU) nations are fundamentally backed by universal privacy rules incorporated in their national constitutional texts. Similar to the ECHR, Africa has the Convention on Human and People's Rights at the continental level, although it is noteworthy that in stark contrast it does not explicitly make provisions for the right to privacy [81]. Interestingly, the right to privacy is subsequently acknowledged in Article 10 of the African Charter on the Rights and Welfare of the Child, although being in a specialised convention [73] and more recently in 2019, the Declaration of Principles on Freedom of Expression and Access to Information in Articles 39 to 42, developed primarily by the Special Rapporteur of the African Commission on Human and Peoples' Rights (ACHPR) on Freedom of Expression and Access to Information, elaborately addresses the right to privacy in the digital context and essentially fills the void in the recognition of the right to privacy in the African Convention [22].

As a result of the need for stronger and more comprehensive laws concerned specifically with data protection growing from increased risks to privacy, the AU adopted the Convention on Cyber Security and Personal Data Protection ("the Malabo Convention/the Convention") in June 2014. Ideally this would have been Africa's version of the GDPR (or the relevant African Directive), but it has not lived up to expectations as the 15-member-state ratification threshold needed to bring it to full effect has not been reached at the this present time, with the most recent number put at 13 states [58]. Additionally, an issue with the

Convention's consistency with international standards is that, it fails to define key terms that underpin the principles of adequacy [49]. Clarity is critical, and these omissions could lead to misunderstandings, particularly in instances requiring cross-border enforcement [5]. However, it must be acknowledged that the Convention has some merits. Much of the task was given to the states, who were required to design security standards and a solid legislative framework for creating a trustworthy digital environment for electronic transactions, protecting personal data, and avoiding cybercrime. The Convention also defines necessary requirements for processing personal data and emphasises guidelines that are considerably more stringent when dealing with sensitive data [60].

There is also the laudable AU Data Privacy Framework that was endorsed by the AU Executive Council in February 2022 [21, 74]. This is likely the most recent important project pertaining to data governance undertaken by the AU in reaching its 2030 Digital Strategy and advancing the data governance agenda at the continental level. One of the main goals of the AU's Digital Strategy has been to guarantee that the Malabo Convention enters into force, albeit by 2020. With this goal yet unmet, the AU Executive Council's recent acknowledgment of the Data Policy Framework might be the best new attempt to make this a reality.

The adoption of legislation ensuring the protection of personal data has progressed more slowly in the African region than the adoption of rules governing a general right to privacy, which are found in the constitutions of almost all countries. Before the GDPR was implemented in 2016, only 16 of the 55 countries had adopted explicit data protection laws. However, that number has swiftly increased to 35 countries at the time of this publication of which 26 have working data protection authorities [66]. The architecture and methods for implementation of data protection laws vary greatly among the nations that have them. Legal, political, economic, and cultural distinctions among the various countries have an impact on the laws that are different in those countries.

A number of West African countries have adopted data protection measures, with laws adopted almost evenly before and after the GDPR's adoption in 2016. Apart from Uganda, Kenya and Rwanda, several nations in Central and East Africa (such as Sudan, South Sudan, Somalia, Ethiopia, Eritrea, Comoros, Burundi) have not enacted major data protection rules and particularly there is an uneven patchwork of rules in Southern Africa. Several countries have adopted data protection laws that are not currently in force, with data protection authorities that only exist on paper (such as Botswana, Seychelles, Equatorial Guinea and Madagascar); however, on the flipside, Tanzania and Eswatini are the latest in 2022 to have joined the long list of African nations that have enacted robust data-protection legislation with a recognized regulatory authority in the same spirit as the GDPR [66].

An important improvement with these recently enacted laws post-GDP is the increased regulatory provision of

stronger protections for sensitive personal data, and data minimization in processing in line with renewed GDPR focus. Case studies have demonstrated that the breadth of legal intricacies and depth of Africa's data protection laws varies in content when the timeframes of adoption are considered, i.e., evaluating legislation before GDPR (for example, Tunisia (2004) and Morocco (2009) and after GDPR (for example Kenya (2018) and Tanzania (2022) [16]. A major reason for this shift is attributed to the adequacy provision contained in the GDPR which strongarms African countries to ensure their laws meet the threshold for qualification of free flow of data to and from their European counterparts [49].

Although 'exigent priorities' of successive conflicts and pressing economic hardship have been identified as a crucial influence in Africa's current last-pace condition of data privacy jurisprudence [81], recent developments record that the respective states are making sustained progress in matching up its legal and regulatory framework to facilitate compliance with global best practices. Countries like Morocco and Nigeria are making sweeping amendments to their existing legal framework to bring it closer to the global standard, it has also been noted that countries like Botswana and Rwanda would be releasing new data protection laws before the close of 2023 [66].

7. Beyond Laws: Reforming the Paradoxical Pursuit of Privacy

In theory, consumers claim they are concerned about their privacy. However, their behaviour shows the opposite of that concern. Consumers readily share their personal data for the benefits attached to doing so, even when they do not fully understand how the data will be used. The Genesys survey referred to in earlier parts of this article showed that 91% of survey respondents worry about the potential abuse of their personal data [70]. In that survey, about 70% claim it's improper for businesses to share their information with third parties, without authorization. Also, between 2013 and 2014, increase of online privacy concerns, including in Africa and elsewhere across the globe was recorded [29]. So, although, privacy and data protection conversations are increasingly prevalent nowadays, especially with regards to the unauthorized accumulation and use of personal data, individuals are not taking commensurate and proactive steps to stop or significantly reduce the trend of unauthorized use of personal data.

This phenomenon known as the privacy paradox has been in existence for a relatively long time now. Simply, it describes the irreconcilable difference of information privacy attitude and actual information privacy behaviour. For example, in the Genesys survey, only about half (53%) of those surveyed said they take steps to deter the tracking of their personal data, such as opting out or disabling cookies collection software. While web services providers are legally bound to comply with these data protection provisions, it is imperative that users consciously maximize the protection

mechanisms available to them. The 2019 decision of the CJEU in the case of *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH*, Case No. C-673/17 (the *Planet49*) [16], is instructive. The court ruled that a pre-selected checkbox which the user must deselect to refuse his or her consent does not constitute valid consent. The reasoning of the court was to the effect that, for consent to be valid, active behaviour on the part of the user is necessary. This implies action on the part of the user and ultimately, a responsibility to decide what action to (or not to) take.

Typically, a bunch of us users will and, in fact do not pay attention to these measures of safeguards available to us. Another example is with privacy policies. Again, in the Genesys survey, 91% claim to read privacy statements provided by companies, which are meant to tell consumers how their data will be used. However, only 20% of survey respondents say they actually review the privacy statements all the time. Whereas the original intention behind the notice and choice privacy framework was to give individuals a great level of control of the use, collection and disclosure of their personal data. Although, there are valid conversations bordering on the transparency on privacy policies, language used to draft them, etc., which fall outside of the scope of this article, the overarching point here, is that consumers need to safeguard their personal data more consciously and proactively.

In another empirical research on the privacy paradox [59], 543 individuals were surveyed to assess the extent to which individuals ignored privacy policies and terms of service when joining social networking platforms. The results revealed 74% skipped privacy statements, selecting the 'quick join' clickwrap. What is striking in the survey, is the revelation of the average adult reading speed (which is 250-280 words per minute) versus the reading time presented by participants. 250-280 words per minute suggested the given privacy policy should have taken 29-32 minutes and the terms of service, 15-17 minutes to read. However, participants who did not select the click wrap, gave an average reading time of only 73 seconds for the privacy policy. All participants were presented the terms of service and had an average reading time of only 51 seconds. Most of the participants agreed to the privacy policy and the terms of service; 97% to the latter and 93% to the former. The survey also included two 'gotcha clauses' to further assess the extent to which users ignore privacy policies [59]. The first had to do with the sharing of users' data with the US' National Security Agency (NSA) and other security agencies; the second and more outrageous clause had to do with users immediately assigning their first-born child as part of their payment obligations to access the social networking service. Interestingly, only 9 (1.7% of those surveyed) mentioned the child assignment clause and 11 (2%) mentioned concerns with data sharing; albeit only one of the 11 mentioned the NSA.

An additional example of unguarded behaviour on the part

of consumers, is granting permission to smart devices to access their location data. The Genesys survey also showed that 81% of respondents allow smartphone apps to access their location data. Some automatically grant access to such requests on their devices. Others do so after a little scrutiny. While it is reasonably justifiable to use modern technologies for the purpose of convenience, again, it is also reasonably expected that consumers pay a high level of attention to what is subscribed to, and ultimately permitted.

8. Conclusion

The article gives an evaluation of PI for the purpose of contributing to greater privacy consciousness in African consumers. In part one, we highlighted how PI is compiled into Big Data, which is then used by GAFAM-types for business operations, consumer transactions, and digital applications (IoT), quite often leading to unintentional personal information disclosure, identity theft, and discrimination in specific automatic selection contexts. Every time consumers engage in digital lifestyles or other aspects of the digital economy, such as when they use a payment card to shop, apply for a job, conduct online research, or post on social media, they inadvertently contribute to Big Data. While it is still true that the average consumer and internet user is unaware of the extent to which their online activities generate data that is being gathered, analysed, and used for various governmental and commercial purposes, it is equally crucial that people are aware of their moral obligation to respect their own privacy.

Consequently, in part two, we discussed the privacy paradox which indicates that when asked, individuals appear to value privacy, but when investigated further, their behaviours would be in the opposite direction, placing privacy at the very bottom of the priority spectrum. African consumers must begin to prioritize their privacy as a step towards changing this narrative. It is one thing for laws to exist, it is another thing for one to be aware of the existence and import of the law and knowing how to avail oneself of the benefits of the law. To the extent that laws exist to deter the unauthorized exploitation of personal data, individuals, understanding the value of their data, should begin to take on the duty of safeguarding it or otherwise, maximizing the potential value in it. Consumers must understand the value of their personal information and take deliberate steps to protect it. This often-overlooked ethical responsibility would entail careful use of credit cards, social media, and passwords in addition to encryption and security software to restrict access to devices, an understanding of data rights to know how to manage data that has already been disclosed and seek redress in situations of unfair exploitation.

The moral obligation also extends to participation in legislative reforms and consumer activism at the governmental level. In the African sphere, there is much of which to be constructively critical of. We have demonstrated how the issue(s) largely lie with the lacklustre governance and enforcement of initiatives at the continental level. The

AU is operating well below par in comparison to its regional counterparts. As such, putting in place a system to coordinate regional and transnational collaboration is one aspect where the AU and its agencies would benefit strongly. The AU commission would also do well to leverage on the individual countries strides in legislative enactments and policing, to take their peddle off new law/policy roll-outs and instead considerably help the countries by enabling practical collaborations on data protection issues between them and relevant international and regional organisations, much like the EU has done with its overarching directives. This would be focal, especially now with the swing of the African Continental Free Trade Area Agreement (AfCFTA) which requires regional harmonization between member states in pursuance of the Protocol on Trade Services, not to mention its consistency with one of the core concepts of the Digital Transformation Strategy, which emphasises the need of fostering unity and collaboration with international organisations and Regional Economic Communities (RECs).

References

- [1] '08182022DabateSentencing'. n.d. CT.Gov - Connecticut's Official State Website. Accessed 13 December 2022. <https://portal.ct.gov/DCJ/Press-Room/Press-Releases/08182022DabateSentencing>.
- [2] Acquisti, Alessandro. 2010. 'The Economics of Personal Data and the Economics of Privacy', January.
- [3] Agogo, David. 2021. 'Invisible Market for Online Personal Data: An Examination'. *Electronic Markets* 31 (4): 989–1010.
- [4] Al-Khouri, Ali. 2012. 'Data Ownership: Who Owns "My Data"?' *International Journal of Management & Information Technology* 2 (November): 1–8. <https://doi.org/10.24297/ijmit.v2i1.1406>.
- [5] Babalola, Olumide. 2022. 'Data Protection Legal Regime and Data Governance in Africa: An Overview'. Africa Portal. African Economic Research Consortium (AERC). 18 February 2022. <https://www.africaportal.org/publications/data-protection-legal-regime-and-data-governance-africa-overview/>.
- [6] Beauvisage, Thomas, and Kevin Mellet. 2019. *Datasets: Assetizing and Marketizing Personal Data*.
- [7] Birch, Kean, and Kelly Bronson. 2022. 'Big Tech'. *Science as Culture* 31 (1): 1–14. <https://doi.org/10.1080/09505431.2022.2036118>.
- [8] Birch, Kean, DT Cochrane, and Callum Ward. 2021. 'Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech'. *Big Data & Society* 8 (1): 20539517211017308. <https://doi.org/10.1177/20539517211017308>.
- [9] Borgesius, Frederik Zuiderveen. 2017. 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition Case Notes'. *European Data Protection Law Review (EDPL)* 3 (1): 130–37.
- [10] 'BPC is ordered to pay more than \$500, in fine for violation of the Data Protection Act – IT Portal'. 2022. 30 April 2022. <https://pti.ao/bpc-e-condenado-a-pagar-mais-de-500-mil-dolares-em-multa-por-violacao-da-lei-de-protecao-de-dados/>.

- [11] Brockhoff, Julia, Bertrand Jehanno, Vera Pozzato, Carl-Christian Buhr, Peter Eberl, and Penelope Papandropoulos. 2008. 'Google/DoubleClick: The First Test for the Commission's Non- Horizontal Merger Guidelines', no. 2.
- [12] Christiansen, Linda. 2011. 'Personal Privacy and Internet Marketing: An Impossible Conflict or a Marriage Made in Heaven?' *Business Horizons* 54 (6): 509–14. <https://doi.org/10.1016/j.bushor.2011.06.002>.
- [13] Christl, Wolfie. 2017. 'How Companies Use Personal Data Against People'.
- [14] Crépeau, Laurent. 2022. 'Responding to Deficiencies in the Architecture of Privacy: Co-Regulation as the Path Forward for Data Protection on Social Networking Sites'. *Canadian Journal of Law and Technology*, no. 19.
- [15] Cuijpers, Colette. 2008. 'A Private Law Approach to Privacy; Mandatory Law Obligated?' SSRN Scholarly Paper. Rochester, NY. <https://papers.ssrn.com/abstract=1090837>.
- [16] 'CURIA - List of Results'. n.d. Accessed 25 January 2023a. <https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-582/14>.
- [17] 'CURIA - List of Results'. n.d. Accessed 26 January 2023b. <https://curia.europa.eu/juris/liste.jsf?num=C-673/17>.
- [18] 'Data Center Market in Africa - Industry Outlook and Forecast 2021-2026'. n.d. Accessed 7 February 2023. <https://www.reportlinker.com/p05822887/Data-Center-Market-in-Africa-Industry-Outlook-and-Forecast.html>.
- [19] 'Data Protection Laws in Africa: A Pan-African Survey and Noted Trends | United States International Trade Commission'. n.d. Accessed 10 February 2023. https://usitc.gov/staff_publications/jice/data_protection_laws_africa_pan_african_survey_and.
- [20] De Hert, P., and S. Gutwirth. 2009. 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action'. In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poulet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, 3–44. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-1-4020-9498-9_1.
- [21] 'Decisions of the Fortieth Ordinary Session of the Executive Council | African Union'. n.d. Accessed 10 February 2023. <https://au.int/en/decisions/decisions-fortieth-ordinary-session-executive-council>.
- [22] 'Declaration of Principles on Freedom of Expression 2019'. n.d. African Commission on Human and Peoples' Rights. Accessed 10 February 2023. <https://achpr.au.int/en/special-mechanisms-reports/declaration-principles-freedom-expression-2019>.
- [23] Deighton, Robert C. Blattberg and John. 1991. 'Interactive Marketing: Exploiting the Age of Addressability'. MIT Sloan Management Review. 15 October 1991. <https://sloanreview.mit.edu/article/interactive-marketing-exploiting-the-age-of-addressability/>.
- [24] 'Digital Rights Lawyers Initiative & Ors v. NIMC'. 2021. 20 October 2021. <https://lawpavilion.com/blog/whether-the-meaning-of-the-term-privacy-of-citizens-is-restricted-to-specific-aspects-of-life-of-a-citizen/>.
- [25] 'EUR-Lex - 31995L0046 - EN'. n.d. Text/html; charset=UTF-8. Official Journal L 281, 23/11/1995 P. 0031 - 0050; OPOCE. Accessed 25 January 2023. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3Aen%3Ahtml>.
- [26] 'Facebook MAU Worldwide 2022'. n.d. Statista. Accessed 13 December 2022. <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>.
- [27] Garstka, Krzysztof. 2018. *Between Security and Data Protection: Searching for a Model of a Legal Big Data Surveillance Scheme within the European Union Data Protection Framework (2018) HRBDT Occasional Paper Series*.
- [28] Geradin, Damien, and Monika Kuschewsky. 2013. 'Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue'. SSRN Scholarly Paper. Rochester, NY. <https://doi.org/10.2139/ssrn.2216088>.
- [29] Gerber, Nina, Paul Gerber, and Melanie Volkamer. 2018. 'Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior'. *Computers & Security* 77 (August): 226–61. <https://doi.org/10.1016/j.cose.2018.04.002>.
- [30] Gratton, Eloise. 2013. 'If Personal Information Is Privacy's Gatekeeper, Then Risk of Harm Is the Key: A Proposed Method for Determining What Counts as Personal Information'. SSRN Scholarly Paper ID 2334938. Rochester, NY: Social Science Research Network. <https://doi.org/10.2139/ssrn.2334938>.
- [31] Hicks, Jacqueline. 2022. 'The Future of Data Ownership: An Uncommon Research Agenda'. *The Sociological Review*, May, 00380261221088120. <https://doi.org/10.1177/00380261221088120>.
- [32] Hormozi, Amir M., and Stacy Giles. 2004. 'Data Mining: A Competitive Weapon for Banking and Retail Industries'. *Information Systems Management* 21 (2): 62–71. <https://doi.org/10.1201/1078/44118.21.2.20040301/80423.9>.
- [33] Hummel, Patrik, Matthias Braun, and Peter Dabrock. 2021. 'Own Data? Ethical Reflections on Data Ownership'. *Philosophy & Technology* 34 (3): 545–72. <https://doi.org/10.1007/s13347-020-00404-9>.
- [34] 'Ikigai Innovation Initiative Challenges the Federal Government and Its Agencies for Violations of Digital Rights'. 2022. *Ikigai.Org* (blog). 14 September 2022. <https://ikigaiinnovation.org/ikigai-innovation-initiative-challenges-the-federal-government-and-its-agencies-for-violations-of-digital-rights/>.
- [35] 'Internet and Social Media Users in the World 2023'. n.d. Statista. Accessed 10 February 2023. <https://www.statista.com/statistics/617136/digital-population-worldwide/>.
- [36] 'Internet of Things - Nigeria | Statista Market Forecast'. n.d. Statista. Accessed 13 December 2022. <https://www.statista.com/outlook/tmo/internet-of-things/nigeria>.
- [37] 'Internet of Things - South Africa | Market Forecast'. n.d. Statista. Accessed 13 December 2022. <https://www.statista.com/outlook/tmo/internet-of-things/south-africa>.
- [38] 'Internet Users in the World 2022'. n.d. Statista. Accessed 29 July 2022. <https://www.statista.com/statistics/617136/digital-population-worldwide/>.

- [39] 'IoT Revenue to More than Double in Middle East and Africa by 2023, Says GlobalData'. 2020. *GlobalData* (blog). 7 January 2020. <https://www.globaldata.com/media/technology/iot-revenue-to-more-than-double-in-middle-east-and-africa-by-2023-says-globaldata/>.
- [40] Irawan, Dasapta, Yuniarti Ulfa, Astyka Pamumpuni, Indra Dinata, Thomas Putranto, and Hari Siswoyo. 2021. 'Reusable Data Is the New Oil'. *E3S Web of Conferences* 317 (January): 05023. <https://doi.org/10.1051/e3sconf/202131705023>.
- [41] Janeček, Václav. 2017. 'Ownership of Personal Data in the Internet of Things'. SSRN Scholarly Paper. Rochester, NY. <https://doi.org/10.2139/ssrn.3111047>.
- [42] John B. Thompson. 2011. 'Shifting Boundaries of Public and Private Life'. *Theory, Culture & Society* 28 (4): 49–70. <https://doi.org/10.1177/0263276411408446>.
- [43] Kokott, Juliane, and Christoph Sobotta. 2013. 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR'. *International Data Privacy Law* 3 (4): 222–28. <https://doi.org/10.1093/idpl/ipt017>.
- [44] Lawrence-Ogbeide, Efe. 2022. 'Delineating the Legal Framework for Data Protection: A Fundamental Rights Approach or Data Propertization?' *Canadian Journal of Law and Technology* 20 (August): 23.
- [45] Lieshout, Marc van. 2015. 'The Value of Personal Data'. In *Privacy and Identity Management for the Future Internet in the Age of Globalisation*, edited by Jan Camenisch, Simone Fischer-Hübner, and Marit Hansen, 457: 26–38. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-18621-4_3.
- [46] 'Lloyd v Google LLC [2021] UKSC 50 (10 November 2021)'. n.d. Accessed 10 February 2023. [https://www.bailii.org/cgi-bin/format.cgi?doc=/uk/cases/UKSC/2021/50.html&query=\(Lloyd\)+AND+\(v.\)+AND+\(Google\)+AND+\(\(2021\)\)+AND+\(UKSC\)+AND+\(50.\)](https://www.bailii.org/cgi-bin/format.cgi?doc=/uk/cases/UKSC/2021/50.html&query=(Lloyd)+AND+(v.)+AND+(Google)+AND+((2021))+AND+(UKSC)+AND+(50.)).
- [47] Liu, Zengrui, Umar Iqbal, and Nitesh Saxena. 2022. 'Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy?' *ArXiv: 2202.00885 [Cs]*, February. <http://arxiv.org/abs/2202.00885>.
- [48] Ly, Branden. 2017. 'Never Home Alone: Data Privacy Regulations for the Internet of Things'. *University of Illinois Journal of Law, Technology & Policy* 2017 (2): 539–58.
- [49] Makulilo, Alex Boniface. 2013. 'Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?' *International Data Privacy Law* 3 (1): 42–50. <https://doi.org/10.1093/idpl/ips031>.
- [50] Manjoo, Farhad. 2018. 'Tackling the Internet's Central Villain: The Advertising Business (Published 2018)'. *The New York Times*, 31 January 2018, sec. Technology. <https://www.nytimes.com/2018/01/31/technology/internet-advertising-business.html>.
- [51] Matte C., Bielova N., Santos C., and SP 41st IEEE Symposium on Security and Privacy. 2020. 'Do Cookie Banners Respect My Choice?: Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework'. *Proceedings - IEEE Symposium on Security and Privacy* 2020-May: 791–809. <https://doi.org/10.1109/SP40000.2020.00076>.
- [52] 'Meet the Google Display Network'. n.d. Think with Google. Accessed 13 December 2022. <https://www.thinkwithgoogle.com/intl/en-145/future-of-marketing/digital-transformation/google-display-network/>.
- [53] Miguel Asensio, Pedro A. de. 2020. 'Data Protection in the Internet: A European Union Perspective'. In *Data Protection in the Internet*, edited by Dário Moura Vicente and Sofia de Vasconcelos Casimiro, 457–77. Ius Comparatum - Global Studies in Comparative Law. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-28049-9_18.
- [54] Mitchell, Tom M. n.d. 'Machine Learning and Data Mining'.
- [55] Moreham, N. A. 2005. 'Privacy in the Common Law: A Doctrinal and Theoretical Analysis'. SSRN Scholarly Paper. Rochester, NY. <https://papers.ssrn.com/abstract=2383498>.
- [56] Moreham, 2018. 'Unpacking the Reasonable Expectation of Privacy Test'. *Law Quarterly Review* 134 (Oct 2018): 651–574. <https://doi.org/10.3316/agispt.20190213006682>.
- [57] Ndubuaku, Maryleen, and David Okerefor. 2015. 'State of Internet of Things Deployment in Africa and Its Future: The Nigerian Scenario'. *The African Journal of Information and Communication (AJIC)*, no. 15 (December). <https://doi.org/10.23962/10539/20335>.
- [58] 'OAU/AU Treaties, Conventions, Protocols & Charters | African Union'. n.d. Accessed 10 February 2023. <https://au.int/en/treaties/african-union-convention-cybersecurity-and-personal-data-protection>.
- [59] Obar, Jonathan A., and Anne Oeldorf-Hirsch. 2020. 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services'. *Information, Communication & Society* 23 (1): 128–47. <https://doi.org/10.1080/1369118X.2018.1486870>.
- [60] Orji, Uchenna Jerome. 2018. 'The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?' *Masaryk University Journal of Law and Technology* 12 (2): 91–129.
- [61] Prainsack, Barbara. 2019. 'Logged out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons'. *Big Data & Society* 6 (1): 205395171982977. <https://doi.org/10.1177/2053951719829773>.
- [62] Purtova, Nadezhda. 2017. 'Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency'. SSRN Scholarly Paper 3070228. Rochester, NY: Social Science Research Network. <https://papers.ssrn.com/abstract=3070228>.
- [63] Purtova 2022. 'From Knowing by Name to Targeting: The Meaning of Identification under the GDPR'. *International Data Privacy Law* 12 (3): 163–83. <https://doi.org/10.1093/idpl/ipac013>.
- [64] Purtova, Nadezhda, and Gijs van Maanen. 2022. 'Thinking of Data as an Economic Good: What It Can (Not) Teach Us about Data Governance'. arXiv. <https://doi.org/10.48550/arXiv.2212.10244>.
- [65] Rameem Zahra, Syed, and Mohammad Ahsan Chishti. 2021. *Security and Privacy in the Internet of Things*. First edition. 1 online resource vols. Boca Raton, FL: CRC Press. <https://www.taylorfrancis.com/books/9781003016304>.

- [66] 'Roundup_on_data_protection_in_Africa_2022_1672742602 | PDF | Privacy | Information Privacy'. n.d. Scribd. Accessed 10 February 2023. <https://www.scribd.com/document/623358223/Roundup-on-data-protection-in-Africa-2022-1672742602>.
- [67] Schwartz, Paul M. 2004. 'Property, Privacy, and Personal Data'. *Harvard Law Review* 117 (7): 2056–2128. <https://doi.org/10.2307/4093335>.
- [68] Shen, Yuncheng, Bing Guo, Yan Shen, Xuliang Duan, Xiangqian Dong, and Hong Zhang. 2016. 'A Pricing Model for Big Personal Data'. *Tsinghua Science and Technology* 21 (5): 482–90. <https://doi.org/10.1109/TST.2016.7590317>.
- [69] Spiekermann, Sarah, Rainer Böhme, Alessandro Acquisti, and Kai-Lung Hui. 2015. 'Personal Data Markets'. *Electronic Markets* 25 (June): 91–93. <https://doi.org/10.1007/s12525-015-0190-1>.
- [70] 'Survey Shows Consumers Very Willing To Trade Personal Data for Financial Benefits'. n.d. Genesys. Accessed 25 January 2023. <https://www.genesys.com/press?release=122826>.
- [71] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. 2020. 'IoT Privacy and Security: Challenges and Solutions'. *Applied Sciences* 10 (12): 4102. <https://doi.org/10.3390/app10124102>.
- [72] Taylor, Linnet, Hellen Mukiri-Smith, Tjaša Petročnik, Laura Savolainen, and Aaron Martin. 2022. '(Re)Making Data Markets: An Exploration of the Regulatory Challenges'. *Law, Innovation and Technology* 14 (2): 355–94. <https://doi.org/10.1080/17579961.2022.2113671>.
- [73] 'The African Charter on the Rights and Welfare of the Child (ACRWC) | African Union'. n.d. Accessed 10 February 2023. <https://au.int/en/documents-45>.
- [74] 'The Digital Transformation Strategy for Africa (2020-2030) | African Union'. n.d. Accessed 10 February 2023. <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>.
- [75] Tweedie, Steven. n.d. 'More than 1 Billion People a Day Used Facebook in September'. Business Insider. Accessed 13 December 2022. <https://www.businessinsider.com/more-than-1-billion-people-a-day-used-facebook-in-september-2015-11>.
- [76] 'Unlocking the Value of Personal Data: From Collection to Usage'. n.d. Accessed 7 February 2023. <https://www.bcg.com/publications/2013/digital-economy-technology-unlocking-value-personal-data-collection-usage>.
- [77] Vezzoso, Simonetta. 2021. 'Competition Policy in Transition: Exploring Data Portability's Roles'. *Journal of European Competition Law & Practice* 12 (5): 357–69. <https://doi.org/10.1093/jeclap/lpaa096>.
- [78] Walters, Robert, Bruno Zeller, and Leon Trakman. 2018. 'Personal Data Law and Competition Law – Where Is It Heading?' SSRN Scholarly Paper. Rochester, NY. <https://doi.org/10.2139/ssrn.3275832>.
- [79] 'World Internet Users Statistics and 2023 World Population Stats'. n.d. Accessed 10 February 2023. <https://www.internetworldstats.com/stats.htm>.
- [80] 'Wp136_en.Pdf'. n.d. Accessed 25 January 2023. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
- [81] Yilma, Kinfe. 2022. 'African Union's Data Policy Framework and Data Protection in Africa'. SSRN Scholarly Paper. Rochester, NY. <https://doi.org/10.2139/ssrn.4253828>.
- [82] Zeithaml, Valarie A. 1988. 'Consumer Perceptions of Price, Quality, and Value: A Means-End Model and Synthesis of Evidence'. *Journal of Marketing* 52 (3): 2–22. <https://doi.org/10.2307/1251446>.
- [83] Zelianin, Aleksei. 2022. 'Personal Data as a Market Commodity in the GDPR Era: A Systematic Review of Social and Economic Aspects'. *Acta Informatica Pragensia* 2022 (1): 123–40.
- [84] Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. 2014. 'Privacy in the Internet of Things: Threats and Challenges'. *Security and Communication Networks* 7 (12): 2728–42. <https://doi.org/10.1002/sec.795>.