

# THE PROLIFERATION OF LOCATION BASED SERVICES IN KENYA: AN ASSESSMENT OF PRIVACY AND AI CONSIDERATIONS

AUTHOR: JOSHUA KITILI  
EDITOR: NELLY C. ROTICH



**Strathmore University**

*Centre for Intellectual Property and  
Information Technology Law*

# TABLE OF CONTENTS

<b>1.0 Introduction</b>	<b>5</b>
<b>2.0 Research Objectives</b>	<b>7</b>
<b>3.0 Methodology</b>	<b>7</b>
<b>4.0 Overview of Location Based Services</b>	<b>8</b>
<b>5.0 Location Based Services in Kenya</b>	<b>11</b>
<hr/>	
<b>6.0 Laws and Regulations applicable to Location Based Services in Kenya</b>	<b>13</b>
6.1 The Constitution of Kenya 2010	13
6.2 The Data Protection Act, 2019	14
6.3 The Data Protection (General) Regulations 2021	15
<hr/>	
<b>7.0 Privacy and AI Considerations</b>	<b>16</b>
7.1 Privacy Considerations	16
7.2 AI Considerations	17
7.2.1 Safety and security	18
7.2.2 Fairness and non-discrimination	18
7.2.3 Right to privacy and data protection	18
7.2.4 Transparency	19
7.2.5 Responsibility and accountability	19
<hr/>	
<b>8.0 Privacy risks associated with LBS apps</b>	<b>20</b>
8.1 Information sharing by users	20
8.2 Misuse of personal data	21
8.3 Unauthorised access of personal data	21
8.4 Lack of consent	21
8.5 Third party sharing	22
<hr/>	
<b>9.0 Assessment of Privacy and AI measures by LBS Platforms in Kenya</b>	<b>23</b>
9.1 Delivery Services	23
9.2 Transportation Services	25
<hr/>	
<b>10.0 Overall performance of the platforms</b>	<b>28</b>
10.1 Jumia Food	28
10.2 Glovo	29
10.3 Uber	29
10.4 Bolt	30

---

<b>11.0 Recommendations</b>	<b>31</b>
11.1 General recommendations from the privacy policies assessment	31
11.2 Policy Recommendations	32
11.2.1 Location data legislations	32
11.2.2 Key Terminologies	33
11.2.3 Location Data Definitions	33
11.2.4 Location Data Rules and precise location requirement	34

---

<b>12.0 Conclusion</b>	<b>35</b>
------------------------	-----------

# ACKNOWLEDGEMENT

The preparation and publication of this report have been made possible through funding from **Hewlett Foundation**. I would like to thank the organisation for their continued support.

I am particularly grateful to our **Editorial Team** for their time and subject matter expertise. Special thanks to **Jacala Solutions Ltd** for the design outline of the report. The contributions of **Nelly Chepngetich Rotich**, Research Fellow at the Data Governance Centre, have greatly enhanced the overall quality of this report.

A heartfelt thanks to the management and administrative team for providing essential support, coordination and organisation, ensuring the successful completion of this report.



# EXECUTIVE SUMMARY

Technological advancements have significantly impacted how various services are accessed. Among these services are Location-Based Services (LBS), which have become popular among many Kenyans. Recognizing the proliferation of these services, this report analyses the privacy and Artificial Intelligence (AI) considerations that data controllers, data processors, mobile application developers, and users should factor in when engaging with them.

The report begins by defining LBS as mobile applications that provide location-dependent information and the requisite system components. It highlights the transformative impact of mobile phones on the lives of Kenyans, noting the widespread use of smartphones essential for accessing location-based services.

Significantly, the report assesses relevant laws and regulations applicable to LBS in Kenya, such as the Constitution of Kenya 2010, the Data Protection Act 2019, and the Data Protection (General) Regulations 2021, and offers suitable policy recommendations. It also extensively discusses privacy and AI considerations, focusing on safety and security, fairness and non-discrimination, the right to privacy and data protection, transparency, responsibility, and accountability.

Notably, the report evaluates potential privacy and AI threats associated with LBS, including user information sharing, misuse of personal data, unauthorized access to personal data, lack of consent, and third-party data sharing. It also analyses the performance of popular LBS platforms in Kenya, such as Jumia Food, Glovo, Uber, and Bolt, and makes specific recommendations based on the assessment of their privacy policies.

This report aims to guide stakeholders in understanding the impact of LBS in Kenya and the need to implement necessary measures to address privacy and AI issues in location-based services. It will also be helpful for users who interact with these platforms regularly and for policymakers in creating robust laws and policies to protect data subjects.

# 1.0 Introduction



Location Based Services (LBS) have been defined as mobile applications that provide information depending on a user's location.<sup>1</sup> It also denotes 'applications integrating geographic location with the general notion of services.'<sup>2</sup> The system components required for an LBS to work include mobile devices, positioning, communication networks, service and content provider.<sup>3</sup> LBS integrates data from various resources which include 'Global Positioning Systems (GPS) satellites, cellular tower pings and short-range positioning beacons to provide services based on the user's geographical location.'<sup>4</sup>

The increased use of mobile phones has transformed the lives of many Kenyans in a positive way. Many people both in the urban and rural areas have a mobile phone which may either be a basic feature phone or a smartphone that enables them to access various services. Some of these services are location-based services which rely on consumers' smartphones for targeted advertisements or to provide interactive opportunities.<sup>5</sup> LBS has been used by online taxi services such as Uber and Bolt to take users to their preferred destination and google maps have also utilised LBS to direct a person to a specific destination or alert a driver about a traffic snarl-up.

Some common LBS apps include travel and tourism apps like Tripadvisor app<sup>6</sup> that

<sup>1</sup> Haosheng Huang and Song Gao, Location-Based Services <[https://www.researchgate.net/publication/324748144\\_Location-Based\\_Services](https://www.researchgate.net/publication/324748144_Location-Based_Services)> accessed 5 May 2023

<sup>2</sup> Jochen Schiller and Agnes Voisard, Location-Based Services (Elsevier 2004)

<sup>3</sup> Huang (n 1)

<sup>4</sup> Andrew Froehlich, Location-Based Services <[https://www.techtarget.com/searchnetworking/definition/location-based-service-LBS#:~:text=A%20location%2Dbased%20service%20\(LBS\)%20is%20a%20software%20service,or%20more%20location%20tracking%20technologies.](https://www.techtarget.com/searchnetworking/definition/location-based-service-LBS#:~:text=A%20location%2Dbased%20service%20(LBS)%20is%20a%20software%20service,or%20more%20location%20tracking%20technologies.)> accessed 5 May 2023

<sup>5</sup> Max Freedman, Location-Based Services: Definition and Examples (9 March 2023) <[businessnewsdaily.com/5386-location-based-services.html](https://businessnewsdaily.com/5386-location-based-services.html)> accessed 5 May 2023

<sup>6</sup> Tripadvisor, Meet your everyday travel app <<https://www.tripadvisor.com/app>> accessed 6 May 2024

offer users optimal routes and also interesting places to visit nearby.<sup>7</sup> Fitness apps like Google Fit<sup>8</sup> enable users to monitor their workout activities and also routes while some restaurants may use food delivery apps to deliver takeaway meals to customers.<sup>9</sup> An example of this in Kenya is the glovo app which enables users to order anything and track it in real time.<sup>10</sup> Other LBS include services like geo-social Networks (GSNs) whereby users share information about their current whereabouts for instance Foursquare.<sup>11</sup>

Although LBS is beneficial to a large extent, it is fundamental to assess the use of LBS apps in Kenya and also the privacy and Artificial Intelligence (AI) elements that should be addressed. For instance, geolocation tracking that is associated with LBS has raised some concerns that include organisation transparency of geolocation data, corporate espionage, stalking and even surveillance.<sup>12</sup> Digital surveillance intensified following the mushrooming of contact tracing apps as a result of the Covid-19 pandemic. Roger Clarke argues that humanity has entered the period of living in a “digital surveillance economy” where ‘acquisition and exploitation of large volumes of personal data through digital devices are used not only by governments for security purposes but also by corporations to target advertisements, manipulate consumer behaviour and maximise revenues from goods and services.’<sup>13</sup>

Location data has the potential of infringing on the right to privacy provided in the Constitution of Kenya.<sup>14</sup> This is because not only can the data collected be misused but it can also lead to cybercrimes and in extreme cases physical crimes like stalking or theft.<sup>15</sup> This study investigates the use of location data by LBS apps in Kenya, the privacy and AI considerations, the unforeseen risks associated with their use and any loopholes that can be addressed.

7 ibid

8 Google Fit, Coaching you to a healthier and more active life <<https://www.google.com/fit/>> accessed 6 May 2024

9 Freedman (n 5)

10 Glovo, Food delivery and more <[https://glovoapp.com/ke/en/?utm\\_source=google&utm\\_medium=cpc&utm\\_campaign=google\\_search\\_brandprotection\\_newusers\\_KE\\_City\\_Exact\\_digitalbudget\\_english&utm\\_campaignid=19146550719&utm\\_adgroupid=144546106535&utm\\_term=glovo%20kenya&utm\\_matchtype=e&utm\\_device=c&gclid=Cj0KCQjwk7ugBhDIARIsAGuvpPZsXqjz12H\\_PbjpZK1pphnwwMzan3o5rYizgLOBiMybZcYz3M6n5LcaAuX6EALw\\_wcB](https://glovoapp.com/ke/en/?utm_source=google&utm_medium=cpc&utm_campaign=google_search_brandprotection_newusers_KE_City_Exact_digitalbudget_english&utm_campaignid=19146550719&utm_adgroupid=144546106535&utm_term=glovo%20kenya&utm_matchtype=e&utm_device=c&gclid=Cj0KCQjwk7ugBhDIARIsAGuvpPZsXqjz12H_PbjpZK1pphnwwMzan3o5rYizgLOBiMybZcYz3M6n5LcaAuX6EALw_wcB)> accessed 5 May 2023

11 Michael Herrmann and others, ‘Privacy in Location-Based Services: An Interdisciplinary Approach’ (2016) 13 (2) SCRIPTed 145-170

12 Albert Remy, Geolocation data tracking: What are the privacy risks (4 February 2020) <<https://www.tmcnet.com/topics/articles/2020/02/04/444375-geolocation-data-tracking-what-the-privacy-risks.htm#:~:text=Another%20privacy%20issue%20linked%20to,fol-low%20them%20on%20social%20media.>>> accessed 5 May 2023

13 Mika Westerlund, Diane A. Isabelle and Seppo Leminen, The Acceptance of Digital Surveillance in an Age of Big Data <<https://timreview.ca/article/1427>> accessed 5 May 2023

14 Article 31 (c) and (d) of the Constitution of Kenya 2010 provides that, ‘Every person has the right to privacy which includes the right not to have- (c) information relating to their family or private affairs unnecessarily required or revealed or (d) the privacy of their communications infringed.’

15 GAO, Mobile Device Location Data <<https://www.gao.gov/assets/gao-12-903.pdf>> accessed 6 May 2024



## 2.0 Research Objectives

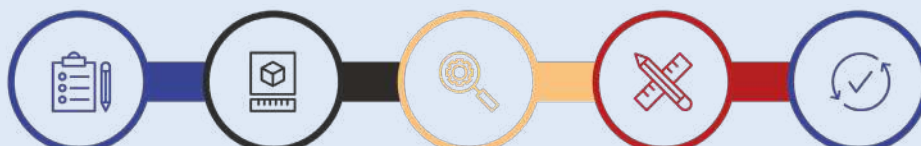
The objectives of the study were as follows:

1. To analyse and understand what LBS entails.
2. To assess the use of LBS by applications in Kenya.
3. To identify privacy and AI considerations arising from the use of LBS
4. To identify privacy risks associated with LBS apps.
5. To understand and analyse the current practices adopted by Kenyan LBS applications that assist with mitigating privacy and AI risks.
6. To identify any existing loopholes in the use of LBS apps and make appropriate privacy and AI recommendations.



## 3.0 Methodology

The study utilised desktop research to collect relevant data containing information that discusses LBS including privacy and AI considerations. The privacy initiatives of identified LBS platforms were also assessed to determine the measures taken to secure location data. This involved analysing the privacy policies or notices to assess whether privacy and AI parameters of the identified LBS platforms are robust to protect users. Doctrinal research was also utilised to identify applicable legislation that can regulate LBS, while comparative research of the regulatory landscape of other external jurisdictions was employed in making policy recommendations.





## 4.0 Overview of Location Based Services



Location Based Services can be divided into two broad categories, namely, user-requested and triggered.<sup>16</sup> The user-requested LBS category entails retrieving the position of a device once and thereafter using it on subsequent requests for location-dependent information.<sup>17</sup> In this case, the user determines whether and when to retrieve the location of their device and utilise it within the service.<sup>18</sup> It may encompass locating the user's current position (personal location) or locating nearby amenities like restaurants or banks (services location).<sup>19</sup> An example of this type of LBS is navigation that involves a map.<sup>20</sup> A triggered LBS on the other hand relies on a condition that has already been set up and its fulfilment retrieves the position of the device for example in emergency services where a call to an emergency centre activates an automatic location request from the mobile network.<sup>21</sup>

LBS determine a user's location through various ways namely:

- i. **Cell Tower-Based Identification** - This enables cell phones to determine their own location based on cell-relay towers that are nearby. <sup>22</sup>
- ii. **Global Positioning System (GPS)** - This enables users of GPS enabled devices to receive signals from a network of satellites<sup>23</sup> to determine the precise location

<sup>16</sup> TD' Roza and G Bilchev, An Overview of Location-Based Services <<https://link.springer.com/article/10.1023/A:1022491825047>> accessed 8 August 2023

<sup>17</sup> ibid

<sup>18</sup> Amit Kushwaha and Vineet Kushwaha, Location Based Services Using Android Mobile Operating System <<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c64cec41a5947b3709dc4423922d5889a580a700>> accessed 6 May 2024

<sup>19</sup> ibid

<sup>20</sup> ibid

<sup>21</sup> ibid

<sup>22</sup> ACLU, Location-Based Services: Time for a Privacy Check-In <[https://www.aclunc.org/sites/default/files/asset\\_upload\\_file183\\_9627.pdf](https://www.aclunc.org/sites/default/files/asset_upload_file183_9627.pdf)> accessed 14 August 2023

<sup>23</sup> ibid

on earth. The process is known as trilateration.<sup>24</sup>

- iii. **Wi-Fi Triangulation** - This is a technique that is used to determine the location of a device by analysing signals from nearby Wi-Fi access points.<sup>25</sup>
- iv. **Internet Protocol (IP) Address Approximation** - an IP address is a unique numerical identifier allocated to a device or network that connects to the internet.<sup>26</sup> Through it, any website or internet-based service can approximate a device's location.<sup>27</sup>
- v. **User-Provided Information** - Location Based Services can request a user to manually provide their current location.<sup>28</sup> However, the precision and accuracy lies with the service and user.<sup>29</sup>

A plethora of sectors utilise LBS to deliver services to users. Some of these services include:

- **Navigation and Travel** - Applications designated for this purpose enable a user to perform a search based on a specific location for instance to find the nearest restaurant or bus stop.<sup>30</sup>
- **Tracking and Geosocial Networking** - These apps enable users to share their location through online social networks<sup>31</sup>. Examples of these apps include Foursquare, Family Locator, Facebook Places, Twitter and Yelp.<sup>32</sup>
- **Gaming and Entertainment** - These apps have the ability to locate players by using location-based technology that facilitates specific interactions for instance Pokeman Go is regarded as leading the location game revolution.<sup>33</sup> The game uses both mapping technology and location tracking to create a virtual world for players.<sup>34</sup>
- **Retail and Real Estate** - These apps enable users to locate the nearest store and even shop from their phones while real estate apps show houses for sale or rent in a given area.<sup>35</sup>
- **Advertising** - These apps enable users to receive advertisements that are suitable to their current location or based on the patterns of frequently visited locations.<sup>36</sup>

<sup>24</sup> National Geographic, Triangulation <<https://education.nationalgeographic.org/resource/triangulation-sized/>> accessed 14 August 2023

<sup>25</sup> ACLU (n 22)

<sup>26</sup> Kinza Yasar, IP address(Internet Protocol address)< [https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address#:~:text=What%20is%20an%20IP%20address%20\(Internet%20Protocol%20address\)%3F,for%20communicating%20across%20the%20inter-net.](https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address#:~:text=What%20is%20an%20IP%20address%20(Internet%20Protocol%20address)%3F,for%20communicating%20across%20the%20inter-net.)> accessed 14 August 2023

<sup>27</sup> ACLU (n 22)

<sup>28</sup> ibid

<sup>29</sup> ibid

<sup>30</sup> FCC, Location-Based Services <<https://docs.fcc.gov/public/attachments/DOC-314283A1.pdf>> accessed 14 August 2023

<sup>31</sup> ibid

<sup>32</sup> ibid

<sup>33</sup> PlotProjects, Location- Based Games: How Geofencing can Optimise Your App <<https://www.plotprojects.com/blog/location-based-games-geofencing-optimize-app/>> accessed 14 August 2023

<sup>34</sup> ibid

<sup>35</sup> FCC (n 30)

<sup>36</sup> ibid

- **News and Weather** - These apps are designed to provide weather and news ideal for a user's specific location.<sup>37</sup>
- **Device Management** - These apps enable users to track their devices like phones using other devices like laptops. For instance, in cases where a user has lost a phone, these apps can enable the user to lock or erase data in that phone remotely.<sup>38</sup>
- **Public Safety** - In some areas, LBS apps are used for security purposes. For instance, Google's Amber Alert that is available in a few regions provides information on abducted children so that the public can assist in the search.<sup>39</sup>

The use of smartphones across the globe has had a significant impact on the increased use of various location based services.<sup>40</sup> Although earlier mobile phones (feature phones) also had LBS, they were limited to simple location tracking services while smartphones have transformed LBS because of their powerful operating systems and also various applications.<sup>41</sup> As of 31<sup>st</sup> December 2023, the Communications Authority of Kenya reported that the number of mobile devices in Kenya stood at 65.45 million, which translates to a penetration rate of 129.4 per cent.<sup>42</sup> Smartphone penetration rate stood at 66.4 percent while feature phone penetration rate stood at 62.9 per cent.<sup>43</sup> LBS are also frequently used in Kenya according to a study that was conducted by the United States International University (USIU) in 2020 at Lang'ata sub-county in Nairobi, which indicated that the majority of the respondents used LBS mobile apps more than three times a week, and 75.4% allowed mobile apps to use their GPS geolocation.<sup>44</sup>

The location information used in LBS may be used for a single purpose or stored then later used by combining with other information to target a consumer for instance in advertising.<sup>45</sup>

---

37 ibid

38 ibid

39 ibid

40 Haejung Yun, Dongho Han and Choong C. Lee, 'Understanding the Use of Location-Based Service Applications: Do Privacy Concerns Matter?' (2013) 14 (3) Journal of Electronic Commerce Research 215-230

41 ibid

42 Communications Authority of Kenya, Second quarter sector statistics report financial year 2023/2024 <<https://repository.ca.go.ke/bitstream/handle/123456789/1369/Sector%20Statistics%20Report%20Q2%202023-2024.pdf?sequence=1&isAllowed=y>> accessed 10 June 2024

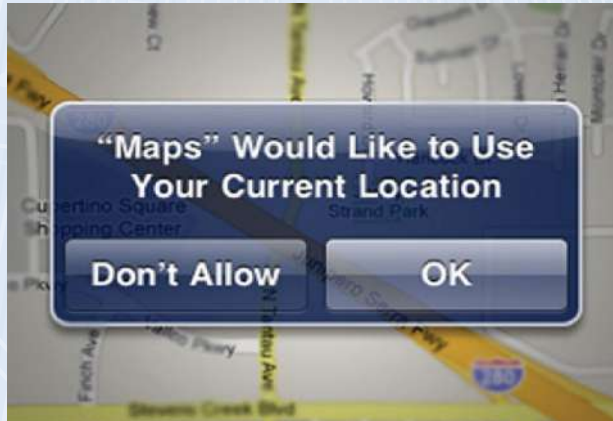
43 ibid

44 Richard Jonyo, A framework for examining usage of Location-Based Services: A case of smartphone users in Kenya<[https://www.academia.edu/91549167/A\\_Framework\\_for\\_Examining\\_Usage\\_of\\_Location\\_Based\\_Services\\_A\\_Case\\_of\\_Smartphone\\_Users\\_in\\_Kenya](https://www.academia.edu/91549167/A_Framework_for_Examining_Usage_of_Location_Based_Services_A_Case_of_Smartphone_Users_in_Kenya)> accessed 14 August 2023

45 ACLU (n 22)



## 5.0 Location Based Services in Kenya



**Figure 1: Illustration on the use of LBS<sup>46</sup>**

In Kenya, location based services include: mobile marketing apps, transportation apps, food delivery apps, digital banking apps, navigation and travel, tracking and geosocial networking, and weather apps. Most of these apps have integrated AI which enhances accuracy and efficiency.<sup>47</sup> In navigation systems for instance, traditional GPS navigation may become inaccurate or outdated because of relying on pre-programmed maps and routes but by using AI, the systems can analyse real-time traffic data and also suggest other less congested routes.<sup>48</sup>

The use of machine learning algorithms enhances accuracy and also provides users with personalised information. This is because machine learning algorithms enable computers to learn from data and formulate decisions based on patterns and trends.<sup>49</sup> To illustrate this, Uber is one of the popular transportation apps that provides taxi services in Kenya. These taxi hailing services utilise AI to match individuals with drivers, optimise routes and provide an estimate of the expected arrival time.<sup>50</sup> The algorithms integrated in the apps can analyse historical data thereby determining the suitable price to be charged.<sup>51</sup>

Location-based marketing also employs AI to analyse data like location history and search queries thus enabling businesses to personalise content and also target customers.<sup>52</sup> Social networking platforms also use AI to suggest location based content and events<sup>53</sup> for example Instagram which has gained popularity in Kenya. Digital banking apps have also gained popularity in Kenya since many banks in Kenya have now embraced technology making it easy for their customers to do transactions on their phones and other devices. A number of digital banking apps use geolocation technology that encompasses navigation, tracking and mapping technologies.<sup>54</sup> This technology also uses

<sup>46</sup> Robert Shimonski, *Cyber Reconnaissance, surveillance and Defense* (Elsevier 2015) 126 (Figure 4.12)

<sup>47</sup> Marcin Frackiewicz, *The Role of Artificial Intelligence in Enhancing Location-Based Services* (26 July 2023) <<https://ts2.space/en/the-role-of-artificial-intelligence-in-enhancing-location-based-services/>> accessed 15 August 2023

<sup>48</sup> *ibid*

<sup>49</sup> *ibid*

<sup>50</sup> *ibid*

<sup>51</sup> *ibid*

<sup>52</sup> *ibid*

<sup>53</sup> *ibid*

<sup>54</sup> Marcin Frackiewicz, *AI and the Future of AI-Powered Geolocation Services: Investing in Technologies for Enhanced Navigation, Tracking and Mapping* (14 May 2023) <<https://ts2.space/en/ai-and-the-future-of-ai-powered-geolocation-services-investing-in-technologies-for-en->

AI which enhances accuracy and also incorporates data from different sources like Wi-Fi signals, cell towers and inertial sensors.<sup>55</sup> It is useful in urban areas since structures and tall buildings can interfere with GPS signals.<sup>56</sup> The use of geolocation raises the security level of transactions by avoiding fraud since banks are able to detect any unusual transaction patterns and stop it.<sup>57</sup> In Kenya for instance, Standard Chartered Bank provides in its privacy policy that location information is among the personal data collected and one of the purposes of processing personal data is to detect crime such as fraud.<sup>58</sup>

Other commonly used apps include Facebook app for smartphones which have a feature known as Facebook places that allows users to “check-in” to specific locations.<sup>59</sup> Facebook places utilises maps, cell phone network location and satellite navigation technology to track the location of users.<sup>60</sup> Another commonly used app is Google maps which had over 2 billion monthly users as of 2018.<sup>61</sup> The app can suggest routes, restaurants and also places depending on the user’s specific location.<sup>62</sup> Besides the above mentioned apps, other commonly used apps are indicated in the table below according to the service they offer.

	Platform	Service	LBS Use
1.	Ma3route	Transportation	Provides traffic updates depending on a motorist’s location and also suggests alternative routes.
2.	Bolt	Transportation (taxi hailing service)	Geolocation is used to determine a user’s location and also locate the best route for the ride.
3.	Glovo	Delivery service	Geolocation services may be used to locate the nearest courier to the delivery point and also for security purposes.
4.	Jumia food	Online food ordering and delivery service	Geolocation used in processing and delivering orders.

[hanced-navigation-tracking-and-mapping/](#)> accessed 15 August 2023

55 ibid

56 ibid

57 Jellyfish Technologies, How Banks Can Combat Fraud Using Geolocation Applications < <https://jellyfishtechnologies.com/geolocation-technology-in-banks/>> accessed 15 August 2023

58 Standard Chartered, Privacy Policy < <https://av.sc.com/ke/content/docs/ke-sc-juza-data-protection-privacy-policy.pdf>> accessed 15 August 2023

59 Jonyo (n 44)

60 ibid

61 Sina Shaham and others, On the Importance of Location Privacy for Users of Location Based Applications <[https://www.researchgate.net/publication/337047986\\_On\\_the\\_Importance\\_of\\_Location\\_Privacy\\_for\\_Users\\_of\\_Location\\_Based\\_Applications](https://www.researchgate.net/publication/337047986_On_the_Importance_of_Location_Privacy_for_Users_of_Location_Based_Applications)> accessed 16 August 2018

62 Jonyo (n 44)

## 6.0 Laws and Regulations applicable to Location Based Services in Kenya



### 6.1 The Constitution of Kenya 2010

The Constitution does not have a specific provision on Location Based Services. However, certain provisions are applicable. The right to equality and freedom from discrimination provided in Article 27 is ideal especially where AI is involved. As earlier illustrated, AI plays a pivotal role in facilitating location accuracy based on the algorithms. The algorithms used are prone to bias thereby discriminating against certain groups of people. Therefore developers should be cognisant of such ethical concerns and take appropriate measures to ensure that apps do not perpetuate discrimination or any form of bias. The Constitution provides that every person is equal before the law and both women and men have the right to equal treatment.

The right to informational privacy provided in Article 31 (c) of the Constitution plays a pivotal role in safeguarding the data that is collected and processed by LBS apps. Scholars like Daniel Solove view informational privacy as the right to ‘have one’s information “treated thoroughly,” to understand the disclosures of one’s personal data and to participate meaningfully in the use of that data.’ Location data is considered as personal information by most privacy laws across the world especially if it relates to an identifiable person. As the supreme law, the right to informational privacy plays a significant role in mandating data controllers and processors to implement appropriate safeguards for the protection of personal data shared. The right also protects users of LBS platforms



from misuse of their personal data that may infringe on their right to privacy. In order to actualise the right to informational privacy, the Data Protection Act of 2019 was enacted. The legislation is also applicable to Location Based Services since it contains the tenets fundamental to data protection.

## 6.2 The Data Protection Act, 2019

The Act defines personal data as any information relating to an identified or identifiable natural person. It further defines an identifiable natural person as an individual who can be identified directly or indirectly by reference to an identifier such as 'a name, an identification number, location data, an online identifier...'. This signifies that location data is a form of personal data. Therefore, the requisite provisions applicable to the processing of personal data should be mirrored by data processors and data controllers when handling location data.

Key provisions include section 30 which deals with the lawful processing of personal data. The processing of location data using AI systems by data controllers and data processors should fulfil the conditions enumerated in the Data Protection Act. The consent of the data subject is mandatory. In some cases processing of personal data may be necessary for the performance of a contract, for compliance purposes, in order to protect a data subject's vital interests and for legitimate interests pursued by a data controller or data processor among others.

The processing of any form of personal data by data controllers and data processors should be in compliance with the data protection principles. The integration of AI in LBSs therefore requires developers to take into consideration these principles which include: specified purposes that prohibit repurposing of data especially when training a machine learning model, accuracy which requires personal data to be accurate especially when dealing with automated systems that lack human involvement, storage limitation and processing in accordance with the right to privacy. These principles are outlined in section 25 of the Data Protection Act, 2019.

In the collection and processing of location data, data controllers and data processors should also consider the rights of a data subject, the mode of collection of the location data and also the duty to notify as provided in sections 26-29 of the Data Protection Act, 2019. The storage of location data should also take into consideration the potential risks or threats on the privacy of a data subject. This is because location data is sensitive and can be misused to track a user thereby disclosing his or her identity. To mitigate the potential risks, it is prudent for data controllers, data processors and even developers to anonymise the data. The Data Protection Act, 2019 defines anonymization as the removal of personal identifiers from personal data so that a data subject can no longer be identified. Pseudonymisation is another way of anonymising the identity of users and their location to protect their privacy. To adequately safeguard personal data, the Data Protection Act,

2019 requires data controllers or data processors to implement appropriate technical and organisation measures which also include the pseudonymisation and encryption of personal data.

### 6.3 The Data Protection (General) Regulations 2021

Alongside the Data Protection Act, 2019 are the regulations which give effect to the Act. These include the Data Protection (General) Regulations 2021 and the Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021. In a nutshell the regulations supplement the provisions in the Data Protection Act, 2019. For instance, the Data Protection (General) Regulations has a provision on data protection policy which is not contained in the Data Protection Act, 2019. The provision requires data controllers or data processors to develop, publish and regularly update a policy reflecting their personal data handling practices. The provision further describes the key elements of a policy which include the nature of personal data collected and held; mode of access to personal data by the data subject including exercise of their rights; lawful purpose for processing personal data and the retention period among others.

This provision is fundamental especially to data controllers and data processors who process location data since they are required to comply with the above legal provisions especially when formulating privacy policies.

For AI developers, they should take into consideration data protection by design or by default when designing AI systems so as to ensure compliance with data protection principles. Data protection by design ensures that privacy and data protection issues are considered during the design phase of a system, service, product or process and also in the entire lifecycle. Data protection by default ensures that only essential data that is required is processed to achieve a specific purpose. When creating LBS apps, the developers should consider this so as to provide robust safeguard on the personal data of users. The Data Protection Act, 2019 provides that data controllers or data processors shall implement appropriate technical and organisational measures that are designed to implement data protection principles effectively including the integration of essential safeguards for processing purposes. The Act also provides that data controllers or data processors shall implement technical and organisational measures by default that ensure only essential personal data is processed.

Part V of The Data Protection (General) Regulations 2021 elaborates further the provisions on data protection by design and default described in the Data Protection Act, 2019. The Regulations discuss the elements of data protection principles that are essential for the protection of personal data. For instance, the principle of purpose limitation requires the use of technical measures like hashing and cryptography to limit the possibility of repurposing personal data while the principle of data minimization requires the anonymization or deletion of personal data where the data is no longer essential for the purpose.

## 7.0 Privacy and AI Considerations



### 7.1 Privacy Considerations

When deploying LBS, the privacy of data subjects should be adequately protected to ensure that the data they share is not misused. In addition to the relevant provisions of the Kenyan laws discussed above, jurisdictions like the European Union in the past years have developed laws which have been instrumental in the protection of privacy. Some of the underlying key principles that can be derived from these legislations when deploying LBS include:

1. **Disclosure** - Companies that act as location data collectors are required to inform consumers the kind of data that is being collected and the purpose for the collection. The principle of transparency should thus be observed by the data collectors.
2. **Consent** - The consent of a data subject is required before collecting their personal data. It is also referred to as opt in and opt out for the use of location.
3. **Data Security** - Adequate security measures for instance through employing data security technologies like firewalls, data encryption and data masking among others should be put in place to safeguard the data collected against accidental loss, destruction or illegal processing.

For app developers, it is important to create a privacy policy that complies with the applicable data protection legislation requirements. Some of the key terms that should be included in the privacy policy include:



- The kind of personal data collected such as location data, contact details and transaction information.
- The purposes for collecting the information. These may include for marketing and advertising purposes, for provision of services like transportation or delivery and for enabling communication between users (An example would be between a driver and a rider to confirm the pickup location).
- Disclosure of the information to third parties which is particularly useful for service providers and business partners such as cloud storage providers and marketing partners.
- How users can control their information like consent, corrections and unsubscribing. An illustration of this would be through enumerating the rights accorded to users such as the right to rectification, the right to erasure, the right to object to processing of their information among others.
- Storage of personal data which may include the place and duration of storage of the personal data. An example of this is the Bolt app which provides in its privacy policy that the personal data collected is transferred and stored in the data centres of Zone Media Ltd or Amazon Web Services Inc. The same privacy policy also provides that personal data may be stored as long as one has an active passenger account.
- Cookies. A cookie is a small text file saved by a website on a computer or a mobile device when one visits a website. It enables the site to remember one's preferences for a certain period. For instance, Uber's app privacy policy states that cookies are used for various purposes, such as authenticating users, remembering user preferences and settings, and understanding the online behaviours and interests of people who interact with their services.

## 7.2 AI Considerations

Considering that LBS utilises AI in some platforms to enhance accuracy and efficiency, it is important for developers and companies that integrate AI into their systems to observe ethical AI before deploying the systems. Ethical AI is concerned with the development and also deployment of AI systems that adhere to guidelines like transparency, fairness, accountability, privacy and respect for human lives. In order to address the ethical concerns that may arise through the use of AI systems, international guidelines and recommendations have been adopted by some countries to ensure that people's best interests are prioritised and that operators are accountable for the functioning of AI systems. Some of these recommendations include the United Nations Educational, Scientific and Cultural Organization (UNESCO) Recommendation on the Ethics of Artificial Intelligence, adopted by 193 member states, including 46 African states such as Kenya; and

the Organization for Economic Cooperation and Development (OECD) Recommendation on Artificial Intelligence, adopted by 46 countries and open to non-OECD countries like Ghana, Nigeria and Kenya among others.

Developers of LBS that integrate AI should ensure that responsible AI principles are factored in when developing LBS platforms and before deploying them. Some of the principles for the ethical use of AI are enshrined in the UNESCO Recommendation on the Ethics of Artificial Intelligence and they include:

### **7.2.1 Safety and security**

Safety and security risks should be avoided and appropriate measures should be implemented throughout the life cycle of AI systems to ensure human, environmental and ecosystem safety and security. A secure system should keep private information secure even after facing possible attacks on the system. For instance, data poisoning may occur as a result of the modification and manipulation of the dataset that a model has been trained on leading to systematic malfunction and poor performance and therefore adequate measures must be incorporated to safeguard the location data shared by a data subject.

### **7.2.2 Fairness and non-discrimination**

AI actors should implement appropriate measures that minimise and avoid the perpetuation of discriminatory or biased applications throughout the lifecycle of AI systems. AI systems should treat everyone equal and be available to everyone without discrimination. When discussing fairness, the principle of discriminatory non-harm should be considered as the minimum threshold for fairness since there are many ways of defining fairness in the design and use of AI systems. This principle implies that the designers and users of AI systems should ensure that decisions of the systems are not discriminatory. Apart from targeting people with irrelevant advertisements, LBS apps can use location data to perpetuate discrimination against certain groups of people. Therefore, developers should ensure that the AI systems integrated in LBS apps take into consideration data fairness, design fairness, outcome fairness and implementation fairness.

### **7.2.3 Right to privacy and data protection**

Privacy should be respected and protected throughout the life cycle of AI systems. Therefore, location data shared by users of LBS apps should not be misused for surveillance purposes. AI systems integrated in LBS apps should therefore be restricted from unsolicited observation of individuals' activities or location. It is also important for data that is collected and processed to comply with data protection laws which ensure

that the personal data of an individual is adequately protected.

#### 7.2.4 Transparency

Transparency entails the determination of how and also why an algorithm made a certain decision. Transparency enables individuals to understand how each stage of an AI system is implemented. Transparency works in tandem with concepts like AI explainability and interpretability. The concept of explainability is concerned with providing understandable reasons for decisions arrived at by an AI system while interpretability is concerned with predictability of the model's outputs depending on its inputs.

Data and system transparency is fundamental because through it, users are informed that AI or an automated system will use their data. Therefore, contextualising with LBS, AI transparency is crucial because it creates trust between users and the AI systems, is key in ensuring fair and ethical AI is observed, helps to address any potential data biases; enhances performance and accuracy of AI systems and ensures compliance with applicable AI regulations.

It is also likely that the transparency principle will not be achieved if data subjects are not aware of where their personal data was used to train and test an AI system. Before training a model or applying it to users, they should be provided with the following information: the purpose for processing personal data, the retention period for the personal data and who it will be shared with.

#### 7.2.5 Responsibility and accountability

The UNESCO Recommendation provides that ethical responsibility and liability for decisions based on an AI system should be attributable to the parties involved and their role in the life cycle of an AI system. In simple terms accountability means being responsible for actions and decisions of an AI system and also the overall impact the AI system will have on people. To ensure AI accountability, it is crucial to document how the data is being used when building the underlying model and when the AI system is in operation. It also includes the evaluation of a system's data security and privacy. Considering that location data can be sensitive, AI accountability entails protecting the data from potential cyberattacks. This is because AI systems are susceptible to attacks and hacking that may lead to unauthorised access and use of data. Also, AI accountability can be achieved by ensuring that the training data is unbiased and protected from unauthorised access.



## 8.0 Privacy risks associated with LBS apps



Although LBS apps play a key role in providing various services, there are a number of privacy concerns that should be considered due to the location data that is shared. Therefore, it is essential to implement robust measures to secure the data. Some of the privacy risks that data subjects who frequently use LBS applications should be aware of include:

### 8.1 Information sharing by users

Many apps allow users to share their location with others and this can be done by identifying family members or friends who can access the location information. However, in some cases the default settings automatically override a user's ability to choose whom the location information will be shared with, for instance, Foursquare and Facebook places app. The disclosure of location information to a wide range of individuals without the user's knowledge exposes the user to a number of privacy risks. The sharing of location information may endanger the privacy of a user by exposing a user to unsought contact or even stalking. Information sharing about one's whereabouts, such as attending political gatherings, may expose a data subject thereby infringing on his or her privacy.

Location-enabled devices like smartphones and tablets may also end up collecting, using and disclosing location information for other purposes not related to the delivery of a specific location-based service. The storage of location information

by devices should therefore adhere to the data protection principle which requires that personal data should not be stored for longer than is necessary. For instance, in April 2011, the long storage duration of location information by iPhone 4 became a matter of concern since it was not necessary for the provision of the service. In handling location information, data controllers and data processors should therefore comply with the principles of data protection.

## 8.2 Misuse of personal data

The fact that LBS entails sharing of location data, it can be considered as sharing one's whereabouts with the service provider. The information collected can be misused to create detailed profiles of a data subject's movements, preferences and habits. The data could also be exploited for other heinous activities like identity theft or targeted advertising. Additionally, the data collected by LBS can be accessed by other parties like law enforcement agencies and used to conduct unwarranted surveillance. For example, in 2018 U.S law enforcement agencies used a technique known as geofence warrants to request location information from Google for all the devices located in a specific region for a specific period.

## 8.3 Unauthorised access of personal data

Cyberattacks on LBS can pose a potential threat to the privacy of users if the security measures implemented are not robust to safeguard the location data shared. Cybercriminals may take advantage of this and exploit the vulnerabilities in a device's software or hardware in order to access location information. As a result, the unauthorised access can result in unauthorised tracking of a user or even location based phishing attacks. It is therefore paramount for users of LBS to find out the privacy settings on their devices and the permissions given to apps that require location data. Adjusting the settings may limit the amount of location data shared with apps and also service providers. Service providers also have a responsibility of ensuring robust data security measures are put in place which may include the encryption of data and also updating the hardware and software to address any vulnerabilities.

Other privacy concerns include:

## 8.4 Lack of consent

Users may not be aware that their location is being tracked or that they may have consented for it to happen. Companies or apps may collect geolocation data of a user by using hidden tracking software or by burying disclosures concerning geolocation tracking deep in the fine print of user agreements. Additionally, investigations reveal

that location data that is identified to a specific individual is frequently monetized and sold to third parties without the individual's explicit consent. Basically, location data linked to a particular individual is regularly collected and sold by various entities for purposes unrelated to the initial transaction that justified the collection of such data. Consequently, when various entities possess an individual's location data, the risk of privacy exposure or data breach increases. Finally, access to anonymous location data may be used to identify a person without consent. To illustrate this, the New York Times obtained permission from a school teacher to accurately link anonymous location data to the teacher individually. This was achieved by analysing over four months' worth of location data from more than a million phones and by using their knowledge of the teacher's workplace and residence.

## 8.5 Third party sharing

The importance of data sharing with other organisations or companies is that it enhances efficiency, growth and innovation. However, it may expose companies to data breaches. The location data that is collected may be shared with other entities, thus, there is a potential risk of losing control over how the data is used and parties that have access to it. Geolocation data may also reveal a user's confidential and personal details therefore infringing on their privacy. To avoid misuse and also data breach, data controllers should ensure that robust data security measures are implemented. These may include secure data transfer protocols, the use of data anonymization techniques and conducting due diligence of potential partners.








## 9.0 Assessment of Privacy and AI measures by LBS Platforms in Kenya

To determine whether LBS platforms adequately protect the privacy of data subjects and adhere to the ethical principles of AI, CIPIT conducted an assessment on the privacy policies of commonly used LBS apps in Kenya. These apps include delivery and transportation services. The commonly used delivery apps in Kenya include Jumia Food and Glovo while for transportation services Uber and Bolt are popularly used as they provide taxi hailing services. The assessment involved an evaluation of the privacy policies to find out whether the privacy and AI considerations discussed above are fulfilled.

To distinguish from general personal data, the assessment centred mainly on location data. To facilitate the interpretability of the performance of key parameters assessed, a traffic light assessment tool was used. This entailed analysing the specific provisions of a privacy policy and rating the parameters as indicated in the table below. A rating of red means that the performance of the parameter analysed is inadequate or low and therefore, does not adequately protect the data subject. A rating of yellow means that the parameter meets the assessment criteria but can be enhanced, while a green rating means that adequate protection is provided and the parameter analysed is robust. An illustration of the traffic light assessment and the performance parameters is as indicated below:

-  Assessment parameter is inadequate.
-  Assessment parameter meets the criteria but can be enhanced.
-  Assessment parameter is robust thereby adequately protecting the data subject.

### 9.1 Delivery Services

The assessment below focused on the privacy policies of Jumia food and Glovo which are commonly used in Kenya especially for food delivery purposes. Acknowledging that privacy policies or privacy notices are subject to changes, the collection and assessment of the data below was conducted from 11<sup>th</sup> to 15<sup>th</sup> September 2023.

	Privacy & AI parameters	Jumia Food	Glovo
1.	A noticeable and comprehensive privacy policy	Contains a noticeable privacy policy.	Contains a noticeable and comprehensive privacy policy
2.	Consent	Consent is provided in the context of marketing	Use of the platform is deemed to constitute consent by data subjects.
3.	Purpose for processing personal data (especially in relation to location data)	Does not specifically mention location data but personal data may be used in processing and delivering orders.	Personal data may be processed for contractual purposes which involves using geolocation services to locate partners and couriers nearest to the delivery point. Geolocation data may also be used for security purposes.
4.	Mentions location data among the personal data collected	Geographic location may be obtained from third parties.	Geolocation data will be collected after authorisation.
5.	Mentions third parties with whom personal data will be shared with	Personal data may be shared for specific purposes.	Mentions third parties that personal data may be shared with including reasons for doing so.
6.	Data Security measures	Security measures implemented but not described in detail.	Security measures are in line with the European Commission recommendations.
7.	Retention period of personal data	Does not have a definite period but personal data may be processed for the minimum period necessary.	Data will be retained for the duration of the contractual relationship. A maximum of 15 years in order to comply with Glovo's legal obligations.

8.	Mentions how users can control their personal data (consent, corrections and unsubscribing)	Individuals can exercise the legal rights provided by data protection laws. They can also permanently delete their data.	Users can exercise their personal data rights which include the right to unsubscribe from any marketing communication.
----	---	--	--

*Table 1: An assessment of privacy policies of delivery services*

## 9.2 Transportation Services

The assessment on transportation services focused mainly on taxi hailing services that are now popularly used by Kenyans to move from one destination to another. Commonly used taxi hailing apps include Uber and Bolt that utilise location information to pick and drop passengers. Similarly, the assessment of their privacy policies or notices was conducted from 11<sup>th</sup> to 15<sup>th</sup> September 2023 while acknowledging that they are subject to future updates or changes.

	Privacy & AI parameters	Uber	Bolt
1.	A noticeable and comprehensive privacy policy	Contains a noticeable and comprehensive privacy policy	Privacy policy is not easily noticeable
2.	Consent	Consent is a basis of processing personal data, it is deemed essential for data protection and the use of services after updating the privacy notice amounts to consent.	Consent will be obtained for another specific purpose and the app also provides transparent cookie consent controls.



3.	<b>Purpose for processing personal data (especially in relation to location data)</b>	Location data is used to navigate rider pick-ups and order drop-offs. It is also used to track the progress of riders or deliveries and to prevent, detect and combat other types of fraud.	Personal data is processed for purposes of connecting passengers with drivers. Geolocation data is used to enable efficient pickup and drop-off. It is also used to ensure arrival to a destination and for billing purposes.
4.	<b>Mentions location data among the personal data collected</b>	Location data is collected from drivers, delivery persons, riders and order recipients.	Geolocation data such as where one needs a ride from, location of nearby scooters, time, journey progression and final destination of a trip.
5.	<b>Mentions third parties with whom personal data will be shared with</b>	A detailed description is provided as to how data is shared and the parties involved. Also a user's consent is required if their data is to be shared for other purposes not provided in the privacy notice. The company is required to notify the user.	Personal data is only shared when there is a valid reason to do so. It is also only disclosed to ride-hailing drivers and in some circumstances Bolt operations OÜ group companies. Information may also be shared with external parties to fulfil legal obligations. However a list of the external recipients is not provided.
6.	<b>Data Security measures</b>	The privacy notice does not embody security measures that will be employed to protect personal data.	Personal data is stored in the data centres and only authorised employees have access to it in order to resolve issues. Geolocation data is also anonymised for research and scientific purposes.

7.	<b>Retention period of personal data</b>	Data is retained for as long as is necessary and in order to fulfil the purposes provided in the privacy notice. Defined periods are also provided in the privacy notice and they vary e.g. For 7 years in order to comply with tax requirements.	Data is retained for as long as is necessary and in order to fulfil the purposes provided in the privacy notice. Defined periods are also provided in the privacy notice and they vary e.g. 10 years in the case of a suspected criminal offence.
8.	<b>Mentions how users can control their personal data (consent, corrections and unsubscribing)</b>	The privacy notice provides a detailed description of how users can control their personal data including location data. This can be done through privacy settings, device permissions, in-app ratings pages and marketing choices.	Users can exercise their personal data rights. However, some rights are only exercisable in certain circumstances e.g. the right to restriction of processing and the right to erasure. They also have in-app settings like marketing opt-ins and transparent cookie consent controls.

**Table 2: An assessment of privacy policies of delivery services**

## 10.0 Overall performance of the platforms

	Privacy & AI Parameters	Jumia Food	Glovo	Uber	Bolt
1.	Noticeable and comprehensive privacy policy	●	●	●	●
2.	Consent	●	●	●	●
3.	Purpose for processing personal data	●	●	●	●
4.	Mention of location data among the personal data collected	●	●	●	●
5.	Mentions third parties	●	●	●	●
6.	Data Security Measures	●	●	●	●
7.	Retention period	●	●	●	●
8.	Mentions how users can control their personal data	●	●	●	●
<b>Overall Performance</b>		●	●	●	●

The overall assessment illustrated above indicates that the privacy policies of the platforms don't meet all the criteria required to qualify as being robust and therefore need to be refined so as to align with the ethical principles of AI and also to provide adequate data protection. Although some of the parameters observed were inadequate, the overall performance of the platforms was good considering that all of them satisfied most of the criteria.

### 10.1 Jumia Food

An overall rating of yellow was observed in Jumia Food. This indicates that the privacy policy meets the evaluation criteria, but it can be enhanced so as to adequately protect the data subjects. Although the platform contains a privacy policy, it is not comprehensive enough



to address all the aspects essential for the protection of personal data and especially location data. Consent is a fundamental ingredient to the processing of personal data, which the platform lacks as a key requirement for processing the collected personal data. Although it is also essential in marketing, data controllers or data processors require consent before processing any personal data. This should be clearly indicated in the privacy policy.

The platform also needs to include location data as a type of personal data that will be processed considering that it is utilised in the delivery of services. It should also be indicated as one of the main types of personal data collected. According to the privacy policy, location data may be obtained from third parties. This is not sufficient considering that precise location is needed for various purposes. This needs to be clearly indicated in the privacy policy so as to fulfil the duty to notify requirement provided in the Data Protection Act 2019. The requirement provides that a data controller or data processor should inform the data subject of the fact that personal data is being collected and the purpose for collecting the personal data.<sup>63</sup> Other parameters that need to be improved include the mention of third parties with whom personal data will be shared with, the data security measures that will be implemented and the retention period of personal data.

## 10.2 Glovo

The overall performance of Glovo is green indicating that the privacy policy is robust. Therefore, most of the privacy & AI parameters have been fulfilled and thus, data subjects are adequately protected. The data security measures however need to be enhanced since the privacy policy only mentions that necessary steps have been taken as recommended by 'the European Commission and the competent authority to maintain the required security level...'<sup>64</sup> By providing granular information as to how this will be done, data subjects are assured of adequate data security measures implemented that prevent the circumvention of privacy measures.

## 10.3 Uber

Just like Glovo, Uber's overall performance is green, and this arises from the fact that its privacy notice is comprehensive, fulfilling most of the assessment parameters. This indicates that the platform has integrated robust measures to ensure that personal data including location data is adequately protected. The platform's privacy notice however does not embody the data security measures that will be implemented to protect the personal data collected. This fails to meet the Data Protection Act, 2019 provision that requires data controllers or data processors to inform data subjects of the technical and organisational security measures taken to ensure the integrity and confidentiality of the

<sup>63</sup> Data Protection Act 2019, section 29 (b) and (c)

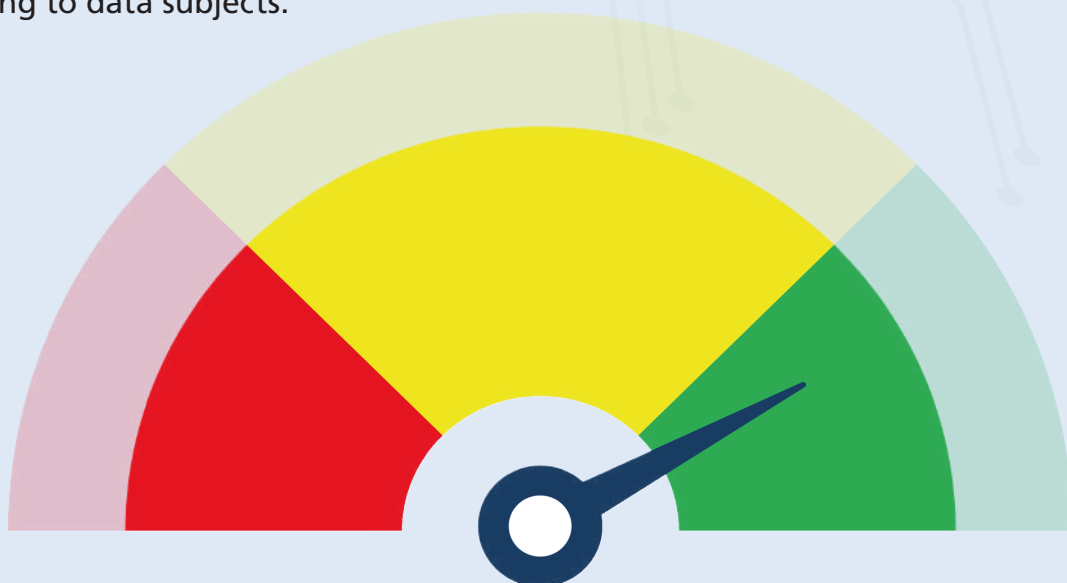
<sup>64</sup> Glovo, Glovo Privacy Policy <<https://glovoapp.com/docs/en/legal/privacy/>> accessed 3 October 2023

data.<sup>65</sup>

## 10.4 Bolt

The overall assessment of Bolt is yellow indicating that most of the parameters have been fulfilled but are not robust enough to adequately protect data subjects. The privacy notice therefore needs to be refined and enhanced. The privacy notice of the platform has been encapsulated in “Legal and Compliance” and is therefore not easily noticeable by users of the platform. It needs to be displayed clearly for users to easily access it and subsequently analyse it. The privacy notice also indicates that under certain circumstances personal information may be shared with external recipients. However, an exhaustive list of recipients is not provided. This is important for transparency purposes and it also builds trust between data subjects and the specific platform(s).

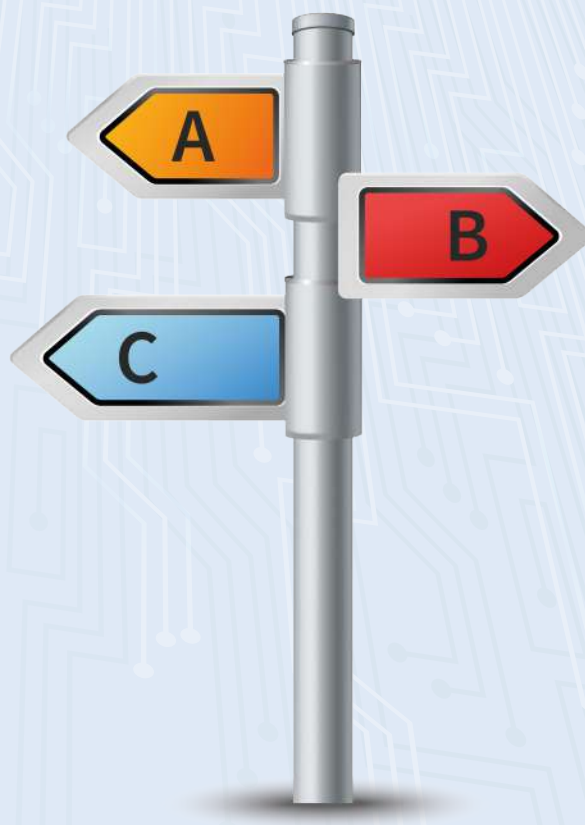
Additionally, the Data Protection Act, 2019 provides that data controllers or data processors should inform data subjects of third parties whose personal data has been or will be transferred to, including details of safeguards adopted.<sup>66</sup> Although users can control their personal data, the platform limits the exercise of some rights to certain circumstances. This includes the right to erasure and right to restriction of processing. It is imperative that a data subject is accorded all the rights without limitation to ensure that they are in full control of their personal data. The data security measures should also be enhanced by indicating clearly the measures that will be integrated to secure personal data. However, the de-identification measures taken to protect geolocation data by the platform sets it apart from the other platforms assessed above. This is because the platform mentions in its privacy policy that when utilising data for research and scientific purposes, all data including geolocation data will be anonymised so that users cannot be identified. Finally, the platform should clearly indicate what amounts to consent when using the platform. This is because it is a key requirement when processing personal data belonging to data subjects.



<sup>65</sup> Data Protection Act 2019, section 29 (f)

<sup>66</sup> *ibid* section 29 (d)

## 11.0 Recommendations



### 11.1 General recommendations from the privacy policies assessment

The analysis of the individual LBS platforms indicate that the privacy policies still need to be enhanced in order to meet the privacy and AI standards required to protect users. From the analysis above it is imperative that privacy policies comply with the applicable data protection legislations and also developers should factor in AI principles when creating the LBS platforms. To address the gaps identified some of the recommendations that can be implemented to improve the privacy policies are as discussed below:

1. The LBS platforms should have a noticeable and comprehensive privacy policy. From the analysis above, one of the platforms did not have an easily noticeable privacy policy which may cause users to struggle to access it. It is crucial for the privacy policies to be easily noticeable so that users are aware how their personal data is collected, used and also protected. Also, they should capture all relevant details including detailed information on the collection of location data and how it will be used. This not only makes the privacy policies comprehensive but also ensures that transparency is achieved.
2. The LBS platforms should indicate clearly what amounts to consent. This is because some of the identified platforms do not specify that it is fundamental in the processing of personal data which includes location data. Although it is still



important in other aspects like direct marketing, the Data Protection Act, 2019 provides that a data subject should consent before processing their personal data.

3. The purpose of processing personal data should also include location data. This is because LBS platforms heavily rely on location data to provide services and although general personal data may be processed for other purposes, it is fundamental that data subjects know why their location data is being processed. This builds trust between the users and the relevant companies responsible for developing the platforms. A good example of this is Uber which processes location data for receipt generation and even fraud detection.
4. Privacy policies should exhaust the list of third parties that will have access to the personal data. This is because of the risks associated with accessing location data like location tracking or location-based phishing attacks. Providing this information ensures there is accountability of the personal data shared.
5. The data security measures that the platforms will integrate need to be comprehensive and include intricate details if need be, in order to comply with the Data Protection Act, 2019. This also assures data subjects that the location data they share with the platforms are adequately protected therefore building trust. The inclusion of data security measures in privacy policies is also an indicator that responsible AI, especially the principle on safety and security, is adhered to.
6. The retention period of personal data should be comprehensively stipulated in the privacy policy. This is because it ensures that once the personal data has achieved its purpose, it is destroyed. A comprehensive privacy policy should indicate defined periods especially when the data is required to achieve a certain purpose for example personal data may be retained for 10 years where there is suspicion that a criminal offence occurred.
7. The privacy policies of LBS platforms should be continuously updated. The updates should capture and elaborate important aspects of location data. This includes the collection, use and third parties that will have access to the data. This ensures compliance with data protection legislations and it is also an indicator that data collectors or data processors are transparent about the data they collect.

## 11.2 Policy Recommendations

### 11.2.1 Location data legislations

Considering that having robust policies are essential to adequately protect data subjects, it is essential that standalone legislations are enacted to regulate location data. In Kenya, the Data Protection Act 2019 incorporates location data into its framework, as it is classified as an identifier in the definition of “identifiable natural person.” This falls under the umbrella of personal data. To ensure detailed elaboration of location data, it is imperative that legislators enact dedicated legislations specifically addressing location

data. There have been efforts globally to enact location data legislations for instance in the United States there is the proposed Geolocation Privacy and Surveillance Act (the GPS Act) and the Location Privacy Protection Act of 2014. In the United Kingdom (UK) the Privacy and Electronic Communications (EC Directive) Regulations 2003 imposes certain restrictions on the processing of location data.<sup>67</sup> Other legislations include the California Consumer Privacy Act of 2018 and the California Privacy Rights Act 2020.<sup>68</sup>

### 11.2.2 Key Terminologies

To ensure adequate protection of location data in legislation, legislators should also include key terminologies associated with location data like geolocation. This should further be classified under sensitive personal information. For instance, the California Consumer Privacy Act of 2018 defines sensitive personal information as personal information that reveals a consumer's precise geolocation.<sup>69</sup> This is captured in the definitions section of the Act. The classification of geolocation data as sensitive personal information is also reiterated in the California Privacy Rights Act of 2020.<sup>70</sup> Likewise, in Kenya considering the proliferation of LBS, it will be ideal to include essential definitions associated with location data.

### 11.2.3 Location Data Definitions

It is also important to distinguish personal data and location data by providing separate definitions of what they entail. This is because location data may involve the geographical information of a device. In the Kenya regulatory landscape, we can borrow a leaf from the Privacy and Electronic Communications (EC Directive) Regulations 2003 of the United Kingdom which gives a detailed definition of location data. According to it, location data is "any data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service including data relating to: the latitude, longitude or altitude of the terminal equipment, the direction of travel of the user or the time the location information was recorded."<sup>71</sup> According to the Information Commissioner's Office this does not include GPS-based location information obtained from smartphones, tablets or other devices since it is collected independently of the service provider.<sup>72</sup> Although it may not be directly associated with GPS based location information, incorporating the definition in the applicable legislation is fundamental.

67 Geoffrey White, Off the Grid: Pinpointing Location-Based Technologies and the Law < <http://www.piac.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report.pdf> > accessed 12 October 2023

68 DataGuidance, USA: Location tracking data: current legislation and future obligations < <https://www.dataguidance.com/opinion/usa-location-tracking-data-current-legislation-and#:~:text=Furthermore%2C%20the%20California%20Privacy%20Rights,considered%20sensitive%20personal%20information> > accessed 12 October 2023

69 California Consumer Privacy Act of 2018, § 1798.140 (ae) (1)(c)

70 FPF, Policy Brief: Location Data Under Existing Privacy Laws < [https://fpf.org/wp-content/uploads/2020/12/FPF\\_Guide\\_Location\\_Data\\_v2.2.pdf](https://fpf.org/wp-content/uploads/2020/12/FPF_Guide_Location_Data_v2.2.pdf) > accessed 9 May 2024

71 The Privacy and Electronic Communications (EC Directive) Regulations 2003, Regulation 2 (1)

72 a ICO, What is Location Data? < <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/communications-networks-and-services/location-data/> > accessed 12 October 2023

### 11.2.4 Location Data Rules and precise location requirement

In the formulation of regulations governing location data, it is important for policy makers to factor in strict rules on processing of location data considering the sensitivity of the information. Generally, key ingredients required for processing location data should be enshrined in the respective legislations. For instance, the Privacy and Electronic Communications (EC Directive) Regulations 2003 provides that location data associated with a user or subscriber of a public electronic communications network or a public electronic communications service may only be processed where that user or subscriber cannot be identified from such data or where the consent of a user has been obtained where it is necessary to provide a value added service.<sup>73</sup>

Finally, considering that most LBS apps utilise the precise location of a user or data subject to provide services, it is essential to incorporate this in the applicable legislations and elucidate what precise location information entails. This enables users and the public to be aware of the type of geographical information they share with data controllers or data processors of these platforms. For example, the California Consumer Privacy Act of 2018 defines precise geolocation as “any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle within a radius of 1850 feet...”<sup>74</sup> Additionally, guidelines like the Digital Advertising Alliance (“DAA”) Self-Regulatory Principles (“DAA Principles”) in the United States define precise location data as “data obtained from a device about the physical location of the device that is sufficiently precise to locate a specific individual or device.”<sup>75</sup>

<sup>73</sup> The Privacy and Electronic Communications (EC Directive) Regulations 2003, Regulation 14 (2)(a) and (b)

<sup>74</sup> California Consumer Privacy Act of 2018, § 1798.140 (w)

<sup>75</sup> FPF (n 167)





## 12.0 Conclusion

This study has illustrated that LBS platforms are indeed being used in Kenya and are fundamental in providing essential services to the public. The analysis in this report indicates that commonly used LBS apps in Kenya provide transportation and delivery services. The rate at which AI is being incorporated into digital devices implies that developers, including data controllers or data processors, should factor in the ethical principles of AI when processing location data alongside data protection principles and requirements. It is equally fundamental to craft robust privacy policies that meet AI and privacy standards to adequately protect users of LBS platforms.

Furthermore, the study highlights that despite the absence of a legislation specifically addressing location data, users' privacy remains safeguarded through existing laws in Kenya, which also address ethical considerations in AI. Notably, in the absence of a specialised law on location data, it is fundamental to incorporate key terminologies concerning location data into existing privacy laws, such as the Kenya Data Protection Act 2019. Moving forward, as evidenced by other jurisdictions, it is advisable to formulate a standalone legislation specifically addressing location data, encompassing all essential aspects to ensure robust protection for LBS users.



This study was made possible by a grant provided by the **Hewlett Foundation**. We thank the organisation for their continued support.



© 2024 by

**Centre for Intellectual Property and Information Technology Law (CIPIT).**

This work is licensed under a Creative Commons Attribution – NonCommercial – ShareAlike 4.0 International License (CC BY NC SA 4.0). This license allows you to distribute, remix, adapt, and build upon this work for non – commercial purposes, as long as you credit CIPIT and distribute your creations under the same license:

<https://creativecommons.org/licenses/by-nc-sa/4.0>



## **Strathmore University**

*Centre for Intellectual Property and  
Information Technology Law*

Ole Sangale Rd, Madaraka Estate.  
P.O Box 59857-00200, Nairobi,  
Kenya.

**Tel:** +254 (0)703 034612

**Email:** [cipit@strathmore.edu](mailto:cipit@strathmore.edu)

**Website:** [www.cipit.strathmore.edu](http://www.cipit.strathmore.edu)