Electronic Commerce Law with A Special Emphasis on The Kenya Legal, Tax and Regulatory Challenges

By

Benjamin Musau

Managing Partner

B M & Co.
B M Musau & Co., Advocates

Table of contents

Electronic Commerce Law with A Special Emphasis on The Kenya Legal, Tax and Regulatory Challenges.

Abstract

E-commerce has experienced tremendous growth in recent years especially in developed countries. However, the sector is still nascent in developing countries like Kenya where it is encumbered by the lack of an e-commerce culture and trust in such transactions. The problem is compounded by the lack of comprehensive legal and tax provisions in Kenyan laws addressing e-commerce. These weaknesses have exposed Kenyans and Kenyan tax authorities to several problems when transacting or claiming tax income for e-commerce. International law has anticipated most of these challenges and provides a good template for developing e-commerce policies in Kenya.

Introduction

Electronic commerce (e-commerce) is a system of trading that primarily uses the internet as the main conduit of interaction with customers. E-commerce includes other functions such as customer service, collaborating with business customers or partners and conducting transactions through the internet. E-commerce took root after the advent of the internet in the 1990s. Broadly speaking, e-commerce is any form of business transaction that involves the use of electronics such as fax, telephone, electronic payments, electronic data interchange and money transfer systems. However, the most used definition is that of business transaction conducted through the internet as the main electronic platform.

The main component of e-commerce is business-to-business transaction as it generates the highest volume of transaction. The other types are collaboration with business partners such as suppliers through the internet. Another form is the business-to-consumer where a business transacts with consumers through the internet. Consumer-to-consumer transactions are transactions where consumers meet on an electronic platform and trade. Popular C2C websites include eBay and Olx.com. Consumer-to-business platforms allow consumers to sell goods to organizations and include Monster.com and Task Rabbit. Further, there is e-governance where governments use internet platforms to serve the citizens, in Kenya a great example is the eCitizen platform.

A major component of e-commerce is electronic banking where customers may conduct banking transactions using internet-enabled electronic devices. It is a convenient form of banking for customers and saves banks on operational costs. It also facilitates the transfer of foreign

currency which is an important component of international trade. E-commerce facilitates actions where traders dispose items to the highest bidder.

Electronic Commerce in Kenya

Kenya has a nascent e-commerce industry as consumers are only becoming familiar with this business model and only a few online companies exist in Kenya. Generally, Kenyan consumers are reluctant to do online shopping as they prefer to interact with the product before making purchase decisions. Further, online companies endure the problem of incompatibility between the software systems they use and the devices available to customers as well as the existing infrastructure. However, more businesses in Kenya are willing to adopt e-commerce despite the hiccups due to the benefits associated with this model. The benefits include reduced operational costs, expanded customer base, increased visibility and the opportunity to collect customer data. Most full-fledged online companies in Kenya are startups as evidenced by the fact that they attract fewer than 100,000 new visitors and fewer than 100,000 repeat visitors. Most have monthly revenues below KShs.1 million and serve fewer than 1,000 customers every month.

Kenya had minimal internet penetration in 2009 as the country relied on expensive satellite connections. However, internet penetration has increased dramatically since the country switched to submarine cables for internet connectivity. Indeed, data released by the Communication Commission of Kenya (CCK) in 2012 indicated that the country has over 14 million internet consumers. Most of the consumers access the internet through their mobile phones and this has contributed to the proliferation of low-cost smart phones in the Kenyan market.

Electronic commerce law in Kenya

The first set of laws addressing e-commerce in Kenya came in the form the Electronic Transactions Bill of 2007 and the Information and Communication Bill of 2008. The amendments recognized e-commerce as a legitimate approach to trade transactions. The full amendments were captured in the Kenya Information and Communications Act of 2009. The Act was followed by the proclamation of the Electronic Transactions Regulations of 2009 that became effective in 2010.

Consumers of goods who trade through e-commerce are protected by the Consumer Protection Act (CPA) of 2012. The CPA sought to address issues of consumer protection that had not been addressed by the Competitions Act of 2010. The CPA had the effect of clarifying the legal relationship between firms and consumers during electronic transactions. However, Ndanu (2016) opines that there are aspects of e-commerce transactions in Kenya that still expose consumers to unwarranted risks. For instance, the protections in the CPA do not adequately capture the pertinent issues of internet and remote transactions.

The Kenya Information and Communications Act of 2009 (KICA)

KICA as amended in 2013 is the law that governs e-commerce transactions in Kenya. The Act allows and recognizes electronic contracts made by people engaging in digital transactions. To this end, the Act creates a legal entity in the form of an electronic signature that is comprehensively defined in the body of the Act. The Act also provides for the creation of the CAK to regulate e-commerce and protect consumers. The CAK has the duty to create and

maintain public confidence in electronic transactions by implementing a set of measures meant to create a robust e-commerce space.

The Evidence Act

Section 106 of the Evidence Act outlines the legal threshold for the admission of electronic records in Kenyan Courts. It provides that the Court may direct the person bearing an electronic signature or the service provider who gave the certificate to produce the electronic certificate and verify that the signature is indeed that of the bearer. Typically, Kenyan Courts assume that electronic transactions accompanied by e-signatures are authentic unless the litigants prove otherwise.

Section 106 of the Evidence Act has been applied to several Court cases. In **Nonny Gathoni Njenga and Anor v Catherine Masitsa and Anor** [2014] eKLR, the litigants wanted the defendants incarcerated due to contempt of Court. However, the respondents objected to the admissibility of the electronic documents the litigants relied on to argue their case. The respondents argued that the DVDs had been obtained illegally in a blatant violation of property rights. The litigants countered that they had relied on sections 106A and 106B of the Evidence Act and that the obligation on them was limited to tendering a certificate from the person who provided the electronic evidence. The Court cited the decision in ***R v Barisa Wayu Matuguda*** [2011] eKLR to determine that it would treat electronic evidence like documentary evidence and may be relied on as evidence even without requiring the production of the original. However, the Court cautioned that evidence would only be admitted if it satisfied the conditions outlined in section 106B of the Act which requires electronic evidence to be accompanied by a certificate

signed by the owner or manager of the device. Thus, electronic evidence is only admissible in Kenyan Courts if it is accompanied by a valid and authentic certificate.

Contrastingly, in ***Marble Muruli v Wycliffe Oparanya*** [2013] eKLR, the Court dropped its hardline stance opting to apply constitutional principles and rules of natural justice. The respondents in the case had argued that the electronic devices used by the litigants did not meet the threshold set by section 106B and lacked credibility. The Court dismissed the objection arguing that it was based on technicalities and asserted that it would base the final verdict on the substance of the evidence contained in the devices. The Court also relied on the precedent in ***Obanda v. Republic*** [1983] eKLR, where the Court admitted electronic devices as evidence subject to confirmation that they functioned properly.

Section 83O of the Act provides that the electronic signature is reliable if it is appropriate for the purpose of the electronic content contained in a device. Section 83P provides that the signature is deemed to be authentic if it is consistent with the requirements provided by the Minister under section 83R of the Act. The signatory party has the obligation of protecting the electronic signature by vigilantly preventing unauthorized use of the signature and maintaining the integrity of the protected content.

The provisions of the Act prohibit the discrimination of electronic signatures on the basis of the place of origin providing that electronic certificates and signatures from other countries have similar legal value as those produced locally as long as they may be assessed on the basis of equivalent international standards and are compliant with the applicable law.

Legal challenges posed by electronic commerce in Kenya

Kinuthia and Akinnusi (2013) found that legal and regulatory challenges were some of the most formidable barriers faced by e-commerce firms in Kenya. These barriers are compounded by the apparent lack of political will and initiative on the part of Government and legislators. In particular, Kenya lacks robust legislation and regulatory regime relating to e-commerce. This has impeded the adoption of e-commerce in the country.

Transactions in different jurisdictions

One of the challenges faced by e-commerce firms and consumers in Kenya is protection for transactions involving parties from foreign jurisdictions. Typically, electronic transactions involve trade in goods and services by entities in different locations. The seller then engages a third party to deliver the goods to the buyer's location. The challenge is that the buyer does not get to examine the quality and quantity of the goods or test their compatibility with his/her needs. In essence, the seller may have provided misleading information about his ability to deliver a particular good or service. This requires e-commerce laws and regulations to make provisions to allow transacting parties to examine the goods even when the supplier is at a distant location.

The CPA was enacted to protect consumers from unfair trade practices in trading transactions including electronic transactions. It captures certain aspects of electronic transactions including internet and remote transactions. The CPA has attempted to keep up with changes in e-commerce by establishing the Kenya Consumer Protection Advisory Committee that has the responsibility of advising the Trade Minister on emerging threats to consumer protection and the relevant action to be taken to increase protections. It also has the responsibility to review laws relating to business transactions involving different platforms. However, there are ambiguities in the Act relating to instantaneous transactions and formal transactions where

parties follow established protocols of e-commerce. The operating environment of electronic transactions means that it may not be possible for parties to follow formal protocols when engaging in a transaction. For instance, it may not be possible for the seller to deliver a trading agreement to the consumer for a transaction where just a click completes the money transfer.

This problem has been demonstrated in several cases that have been filed in other countries. For instance, in ***Macquarie Bank Ltd v Berg*** [1999] NSWSC 526, Macquarie Bank challenged the decision of an aggrieved former employee to defame the Bank on a website based in the US. The Court in Australia was at a loss about how to determine the case given that two jurisdictions applied to the case and they could not guarantee cooperation from US authorities. Similarly, cases such as ***Cybersell Inc. v Cybersell Inc***. [1997] 130 F.3d 414 and ***Compuserve, Inc. v Patterson*** [1996] 89 F.3d 1257, in the US demonstrate the challenge posed by transactions involving different jurisdictions as both involved one of the parties to the case using servers that were based in foreign jurisdictions. The challenge for transacting parties is whether they may obtain protection in the local or foreign jurisdiction with the implication that transacting parties may only seek redress in jurisdictions that provide such protection. Inevitably, the transacting parties are exposed if the foreign jurisdiction does not provide protection. The cases also demonstrate consumer vulnerability for transactions involving foreign entities as even seeking legal redress may not work due to jurisdictional barriers.

Taxation perspectives

Another challenge relates to data and payment security. Electronic transactions have the potential to expose the customer's confidential information in circumstances where the network is not adequately protected from security breaches that expose sensitive customer data. Further, customer data may be exposed to breaches of information integrity where cyber criminals tamper with data and manipulate the system. There are also issues relating to the validity of the information provided by the other party. Customers also need protection from role repudiation where the other party denies having participated in the transaction. This risk is especially pronounced in situations where the trader does not provide any physical identifier as a sign of integrity and commitment. Another issue relates to the authenticity of the transaction as a seemingly valid transaction may be fraudulent when the other party imitates the transactional environment of a genuine trader. The other challenge is the reliability and resilience of the system in the face of external attacks and threats.

The issue of jurisdiction is complicated when the two jurisdictions have different legal approaches to e-commerce. E-commerce is a global phenomenon but there is no standardized legal approach that is applicable to all countries involved in the transaction. The territorial component of e-commerce transactions is a pertinent issue in cases arising from such transactions as the internet is ubiquitous without territorial limitations.

The issue of jurisdiction is also relevant to taxation because different countries have different tax codes applicable to e-commerce. Countries like Kenya have to contend with the issue of the applicable tax codes to e-commerce transaction and if it has the right to levy taxes on a transaction. The concern for the parties involved in the transaction is that they may be subject

to arbitrary taxation due to inconsistent tax codes. Some may even be subjected to double taxation. Some legal scholars have proposed that a standardized global tax policy may resolve some of the taxation problems posed by cross-border transactions.

The other jurisdiction issue raised by e-commerce is the situation where transactions that are legal in one country are prohibited in another country. The issue raised by this quandary is the jurisdiction that is most suited to handle the case. For instance, in ***Minnesota v Granite Gates*** [1997] 568 N.W.2d 715, the defendant had engaged in internet gambling in Minnesota even though gambling was illegal in the province of Minnesota. Even though gambling was legal in other jurisdictions, the Court determined that the defendant was culpable for engaging in illegal activity arguing that the defendant had violated the state's consumer protection regulations.

Legal redress

E-commerce users in Kenya face difficulties getting legal redress in cases when traders breach the terms of the contract. For one, such customers may face surmountable challenges when seeking refunds or compensation for poor quality product due to the huge distance between their location and the location of the trader. Second, the consumers may not be able to utilize conventional dispute resolution mechanisms as the trader may be in a location that is outside the jurisdiction of local Courts. This challenge has caused legal scholars to propose the creation of international dispute resolution systems that resolve disputes where the parties emanate from different jurisdictions.

In cases where the aggrieved party decides to seek legal redress transactions involving parties who are based in other jurisdictions, such a case may be prohibitively expensive to pursue

especially if they choose the litigation approach as the cost of hiring lawyers and travelling for Court proceedings may be quite high. The consumer may be forced to bear the loss if the cost of legal redress far exceeds the subject matter of the transaction. Indeed, due to differences in standards of living, most consumers of products from developing countries such as Kenya may find that the cost of litigation exceeds the value of the subject matter of the transaction even when the subject is a valuable product such as a car.

Research indicates that there is a growing trend among e-commerce consumers to seek legal redress through alternative dispute resolution for transactions where the trader is based in a foreign jurisdiction. However, almost a half of the customers who seek this form of redress are dissatisfied with the way the issue was handled and most of them do not seek further redress. Moreover, less than ten percent of the aggrieved parties seek redress implying that most of the aggrieved consumers do not seek any form of legal redress. Innovations such as online dispute resolution (ODR) mechanisms have emerged in recent years as substitutes to traditional Courts but ODR is still nascent in Kenyan and is not in a position to reliably resolve disputes for aggrieved customers of e-commerce.

Another concern for e-consumers is the issue of privacy. Indeed, research indicates that most Kenyan consumers are reticent to share sensitive information with strangers and this has inhibited the growth of e-commerce in the country. Others are concerned that important electronic identities such as emails may become accessible to online criminals and trolls. This concern is real as some e-commerce platforms have the obnoxious habit of selling customer details to companies that aggregate data for targeted marketing.

Information Asymmetry

E-commerce transactions are conducted in a way that makes it hard for consumers to inspect goods before making purchase decisions. The matter is then complicated by the use of third parties who are often independent contractors to deliver the goods. For instance, in Kenya, e-commerce consumers buy goods on platforms such as Jumia and have them delivered by couriers in an arrangement that does not afford the consumer enough time to inspect the goods. The consumer is further disadvantaged by internal policies of e-commerce companies that do not allow for inspection before payment. Indeed, the case of ***Consumer Federation of Kenya v Fone Express*** [2014 unreported], illustrates this situation. In this case a customer had purchased a phone and computers from Fone Express that turned out to be defective and sought the help of COFEK in getting legal redress as the internal policies at the phone company do not address consumer interests sufficiently.

The case is interesting from a legal perspective as laws on sales of goods require buyers to be granted reasonable opportunity to inspect the goods before making payment. The issue raised by the case is what comprises a reasonable opportunity as the very nature of some goods may necessitate consumers to first test them before making payment in order to ascertain their quality. This is true especially for electronic devices such as phones as the customer may have to test the phone for a few hours to determine if the phone battery is of the desired quality.

Other challenges include the asymmetric relationship between traders and consumers relating to information disclosure and verification. Buyers are required to submit personal information to entities they do not know while the traders may give insufficient information regarding the products they offer. The traders may exploit the information asymmetry to conceal

some of the transaction costs only to surcharge customers after the transaction has been completed. For instance, some traders do not disclose the cost of delivery on their websites but later include them in the transaction cost after the deal has been closed and the customer has purchased the goods. Similarly, banks do not always disclose the cost of online transactions in a single statement but conceal the costs in other statements.

Typically, shipping costs do not include import duty imposed on goods imported into a particular country. For instance, a consumer who is importing a car from the US may not be aware of the import duty imposed at the point of entry. The buyer will be shocked to be slapped with additional costs when he goes to claim the car.

Data protection

The Kenya Constitution emphasizes the right of citizens to privacy and requires legislative agencies to create laws that safeguard citizen privacy including e-commerce consumers. However, Kenya has not enacted laws to safeguard citizen privacy as the Data Protection Bill of 2013 that was meant to activate Article 31(c) and (d) of the 2010 Constitution is yet to be debated in Parliament. The Bill introduces provisions to regulate the collection, processing, storage and use of personal data collected by entities operating in the digital environment. This implies that Kenyan citizens who are now transacting online have no legal protections for violations of their right to privacy unless they are protected in the foreign jurisdiction.

Experts note that the Kenya Government does not appreciate the fact that e-commerce thrives on consumer data and that personal data is a valuable asset in the digital economy. Indeed, some of the largest internet corporations offer their services for free with the implicit

concession by the consumer that the firm collects and uses the personal data collected for marketing purposes. Currently, Kenyan consumer laws do not have a provision to control the use of personal data or even obligate firms in possession of such data to give consumers the right to select the type of personal data to be used for marketing purposes. Typically, websites contain cookies and other software that collects personal data including user identity, age, interests, income and online transactions. Experts note that Kenyan consumers do not realize that they are not protected by the current laws and systems from the abuse of personal data even as they browse the internet. Other countries such as the EU group of nations have made it illegal for internet firms to collect and aggregate user information. EU consumers reserve the right check data that is collected about them and sanction its use.

Security challenges

Kenya has several laws created to improve the security of digital data and electronic transactions. Section 83 of the National Payment Systems Act of 2011 makes it an offense for one to access electronic systems unauthorized with a nefarious intention. The Act also makes it an offence for anyone to be in possession of data or codes that enables one to infiltrate electronic systems belonging to others. The Act also makes it an offense to supply sensitive information such as passwords and access codes that enable intruders to gain access to third party electronic systems. Security experts note that the Act does not appreciate the fact that some of the disclosures of passwords and access codes occur under duress. As such, there is a need for the law to provide exemptions for persons who disclose sensitive information under conditions of duress.

Section 84B of the National Payment Systems Act of 2011 treats electronic fraud that causes the loss, damage or suppression of electronic data with the intention of interfering with the proper functioning of electronic devices for personal advantage an offence. The Act further makes it an offense to deliberately reproduce, publish or avail an electronic signature certificate for fraudulent or other nefarious intentions. The law also makes it an offense to re-program electronic devices with the intention of changing the identity of the owner. This provision was meant to curb the rampant theft of portable electronic devices that are later sold after changing the owner's identity. However, despite this provision theft and trade in stolen electronic devices is rampant in Kenya.

The ever-evolving nature of electronic technology exposes consumers to different types of fraud. E-commerce facilitates the proliferation of consumer fraud due to lack of awareness, anonymity on the internet, lack of technology skills and the complex legal process of prosecuting cases of electronic fraud. In Kenya cases of data and payment fraud have featured prominently in recent years. The most salient case is the manipulation of the Integrated Financial Management Information System (IFMIS) to divert public funds. In the NYS I case, the password of the deputy director was stolen by nefarious actors. Such incidences dent public confidence in electronic transactions when the target is the Government which consumers rely on to protect them from fraud.

E-commerce tax law in Kenya

Article 201(2) of the Kenya Constitution provides that the Government and the legislative organ may develop appropriate tax laws to be applied to e-commerce. However, e-commerce poses several challenges to conventional tax laws as such as tax codes enforced on the basis of residence or source of income. This is because e-commerce is detached from physical provision of goods or services. Tax laws provide that taxes may only be imposed if there is a nexus between the taxing authority and the income claimed. The main connectors are residence and sources of income. The source principle implies that people are taxed on income that is generated within particular geographical or jurisdictional confines irrespective of the tax payer's residence.

The residence principle implies that residents of a particular country or jurisdiction are taxed on their net income irrespective of where the income is made. The nature of e-commerce is such that one may be said to not to have a permanent home thereby exempting them from taxation in Kenya under the relevant provisions of the Income Tax Act. Indeed, tax experts observe that a person may be absent from a given jurisdiction for a sufficient number of days to exempt him from tax codes while continuing to work uninterrupted through telecommunications.

The source rule has been challenged in Court in cases involving e-commerce in Kenya. In ***R v Commissioner of Domestic Taxes Ex parte Barclays Bank of Kenya*** [2015] eKLR, the Kenya Revenue Authority (KRA) argued that it had a right to extract withholding taxes from Barclays Bank on the payments it made to Card companies for the interchange fee it charged to Issuers. The Court was of the view that KRA should clarify the tax category and that the claim

that the payments charged to Issuers was equivalent to professional or management fee lacked sufficient clarity for taxation purposes.

Similarly, in ***Kenya Commercial Bank Ltd v KRA*** [2016] eKLR, KRA argued that KCB owed it withholding taxes for the income it generated through its software partner Infosys Technology. The Court held that there was a lack of clear categorization of the payments for which tax was claimed. However, in ***Stanbic Bank of Kenya v KRA*** [2009] eKLR, the Court was of the view that the services provided by Reuters International could be categorized as professional fees and was taxable as per the tax code.

Section 2 of the Tax Act provides that the permanent establishment of a taxable entity is a fixed location where the entity conducts business and which has been in use for at least six months. E-commerce challenges this provision as transactions may be conducted through servers or websites whose location may be virtual or highly transient. These are not permanent residences as they have no link with a specific physical location. Some scholars opine that an enterprise server may only be said to be at a permanent location if it is owned by the enterprise and located at a specific physical location. They are of the view that the time requirement may not be applied to servers.

However, the tax authorities have to contend with servers located abroad as the provision for permanent establishment requires business to be carried out at the location of the server. Moreover, servers that are only used for auxiliary services may not be considered to be permanent locations. However, if the server performs core business functions then it may be considered to be a permanent location. Unfortunately, very few businesses in Kenya have servers that satisfy these conditions as most use leased servers meaning that they may exonerate

themselves of tax obligations since they do not have a permanent residence in Kenya. Thus, e-commerce defies the tax code in ways that may facilitate tax avoidance.

The Value Added Tax Act (VAT Act) has provisions that may apply to e-commerce. The VAT Act recognizes e-commerce as a trade mediated by information technology in section 8(3) that defines electronic transactions as transactions conducted through a telecommunications network. However, the Act fails to comprehensively cover e-commerce as a unique business environment and create suitable provisions to regulate e-commerce transactions. Further, tax experts note that the Kenyan government does not allocate adequate resources to the tax authorities to monitor and regulate the sector.

Research indicates that it is hard to apply the Kenya VAT law to electronic transactions especially those that are cross-border. For instance, in ***Stanbic Bank v Kenya Revenue Authority*** [2009] eKLR, the Court held that the VAT law applies to withholding tax for electronic transactions although it observed that it is incredibly hard to trace electronic transactions that are liable to taxation.

E-commerce also impedes the enforcement of tax laws as tax authorities only collect tax income on the basis of accurately identifying and locating taxpayers and their assets. They must also clearly identify and verify taxable transactions and provide proof of a nexus between taxable transactions and the entities required to pay tax. E-commerce complicates this process by obscuring the identity of the transacting entities and their locations. E-commerce encourages anonymity through features such as electronic money that allows transactions that are hard to trace and enforce tax laws.

This problem has been partly addressed in international tax law such as the EU directive 2002/38/EC that facilitates the levying of VAT by resolving the net-neutrality issue between transacting entities especially when the trader is not a EU citizen. The directive addresses the challenges associated with establishing the location of the trader. The EU created this directive after realizing that it was a net buyer in electronic transactions. Kenya is in a similar position and would benefit from adopting this directive.

Filling the gaps with international law

The relevant laws relating to e-commerce in Kenya is contained in KICA section 83B. Contract law provides that a contract must involve an offer and an acceptance implying that consensus has been reached by the two parties. Section 83J states that both the offer and the acceptance may be expressed through electronic messages and that such a contract is valid and enforceable. Section 2 of KICA defines electronic as media that has electronic capabilities. The most common method of making electronic contracts is through emails transmitted through internet service providers such as Safaricom.

In the absence of specific provisions in KICA relating to some aspects of electronic transactions, international law may offer respite. International law recognizes emails as valid means of entering and closing a contract as demonstrated in ***Rosenfeld v. Zerneck*** [2004] 776 N.Y.2d 458, where the New York Supreme Court conceded that email is a valid form of communicating and accepting an offer. The case of ***Bernuth Lines Ltd v High Seas Shipping Ltd*** [2005] EWHC 3020, stated that even if acceptance mail is treated as spam it is still a legally valid acceptance of an offer. In ***Jafta v Ezemvelo KZN Wildlife*** [2008] ZALC 84, the Court stated that an SMS has the same legal weight as an email or a written document. Electronic

contracts may also involve webwraps or clickwraps where one accepts the offer by clicking on the accept button on a webpage. Some companies enhance the validity of the process by sending confirmatory emails.

In ***Entores v Miles Far East Corp.*** [1955] 2 QB 327, the Court determined that acceptance prevails over the long standing rule of mail delivery. The displays appearing on websites are invitation to buy rather than offers. The acceptance rule is the most preferred approach to assessing contractual validity of transactions conducted in an electronic environment. The rule is that consensus is reached when the trader gets the customer's acceptance. The precedent for the terms and conditions of the contract as set by ***Gary Patchett v. Swimming Pool and Allied Trades Association Ltd*** (SPATA) [2009] EWCA Civ 717, is that it is the obligation of the customer to read the entirety of the terms and conditions documents before signing the contract. One challenge electronic consumers endure is the fact that customers may make a mistake on the basis of an erroneous representation on a website only for the website to correct the error after the transaction with the effect that the customer may not prove that the information on the website at the time was misleading as the website owners have full control of the content on the website.

Article 14 of the UN Convention on Electronic Contracts requires the offeror to notify the offeree of the error if he has not benefited from the misrepresentation of facts. Article 14(1) further provides that the website owner should create a backstop logic system that flags errors before accepting the customer's offer. Article 6 of the Convention provides guidelines for determining the locations of the parties to a contract. Further, Article 15 of the model law of electronic commerce provides that the location of the parties to a transaction is the place that has

the closest relationship to the contract. Further, Article 10(3) of the UN Convention provides the means of determining the place of dispatch of contractual obligations and the place of receipt of the electronic communications.

One way of tax avoidance involves incorporating a company in a low tax jurisdiction. However, the international tax code overcomes this loophole by taxing firms on the basis of where the management and control of the firm is based rather than its place of incorporation, a principle which applies in Kenya. This provision is encoded in Article 4(3) of the OECD Model Tax Convention.

Kenyan law neither provides a clear definition of what constitutes aggregating and processing personal data nor does it offer specific provisions to facilitate consumers to monitor the use of their personal data. International law may provide valuable insights on protecting consumer privacy during electronic transactions. For instance, in ***Bodil Lindqvist*** [2003] C101-01 the Court defined aggregating personal data as referring to visitors by their name on an internet page in a manner consistent with the provisions of Article 3(1) of Directive 95/46.

Conclusion

Kenyans have not readily embraced e-commerce as a reliable means of conducting business transactions. However, Kenyans are ardent users of the internet and other electronic devices. E-commerce law in Kenya is lacking in several aspects that may expose consumers to several risks during electronic transactions. The limitations of Kenyan laws are attributable to the fact that Kenya commerce laws are vestiges of paper based trade and the fact that most e-commerce laws are rudimentary. Kenya may benefit immensely from borrowing standards of e-commerce set by international law and laws applied in other jurisdictions. Overall, Kenya needs

to comprehensively address the glaring deficiencies in e-commerce law while borrowing best practices from international law.

Bibliography

Covotta, B. (1998). *Personal Jurisdiction and the Internet: An Introduction.* 13 BerkeleyTech. L.J. 265 Available at: http://scholarship.law.berkeley.edu/btlj/vol13/iss1/17

Garcia, F. (2005). *Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators.* 15 Fordham Intell. Prop. Media &Ent. L.J. 1204 Available at: https://ir.lawnet.fordham.edu/iplj/vol15/iss4/10

GoK Ministry of Trade (2017). *Study on Kenya retail sector prompt payment. State department for trade.* Kenyatta Avenue, Telposta Towers

Kalow, G. (1997). From the Internet to Court: Exercising Jurisdiction over World Wide Web Communications, 65 FordhamL. Rev. 2241 Available at: http://ir.lawnet.fordham.edu/flr/vol65/iss5/8

Kenya ICT Federation (2008). *Legislation and Regulation for e-Commerce in Kenya.* Report – Public Panel 19 June 2008

Kilonzo, K. (2007). An Analysis of the Legal Challenges posed by Electronic Banking. *Kenya Law Review*, 1: 323-341.

Kinuthia, J. and Akinnusi, D. (2013). The magnitude of barriers facing e-commerce businesses in Kenya. *Journal of internet and information systems,* 4(1), 12-27.

Ndanu, M. (2013). *E-commerce in Kenya: A case of consumer protection.* A thesis submitted in partial fulfilment of the requirements for Degree of Master of laws (LLM).

Nthuli, M. (2016). *Legal and regulatory challenges facing the growth of e –commerce in Kenya.* A thesis submitted in partial fulfillment of the requirement for the degree of masters of laws university of Nairobi

Nzomo, V. (2017). *E-Commerce and the Law in Kenya: Electronic Contracting.* Available at: https://blog.cipit.org/2017/11/01/e-commerce-and-the-law-in-kenya-electronic-contracting/ (Last accessed on 25th June 2018)

Nzomo, V. (2017). *E-Commerce and the Law in Kenya: Taxation.* Available at: https://blog.cipit.org/2018/02/15/e-commerce-and-the-law-in-kenya-taxation/#more-6554

Phan, T. (1999). Cybersell, Inc. v. Cybersell, Inc., 14 Berkeley Tech.. L.J. 267 Available at: http://scholarship.law.berkeley.edu/btlj/vol14/iss1/15

Rogers, K. (2011). *The Internet and the Law.* New York: Macmillan International Higher Education

Sylvia, P. (2010). *Short message services and e-contracting: Jafta v Ezemvelo KZN Wildlife [2008] 10 BLLR 954 (LC)* Available at: https://repository.up.ac.za/handle/2263/15697

Case law

Bernuth Lines Ltd v High Seas Shipping ltd, 2005.

Bodil Lindqvist v Åklagarkammaren i Jönköping (2003)

Compuserve, Inc v Patterson, 89 F. 3D 1257 (6th Cir. 1996)

Consumer Federation Of Kenya (Cofek) v Minister For Information & Communications & 2 Others [2013] eKLR

Cybersell Inc. v Cybersell Inc., 1997

Entores v Miles Far East Corp. 1955.

Gary Patcherr v Swimming Pool and Allied Trades Association Ltd (SPATA), [2009] EWCA Civ 717

Jafta v Ezemvelo KZN Wildlife [2008] ZALC

Kenya Commercial Bank Ltd v Kenya Revenue Authority [2016] eKLR

Mable Muruli v Wycliffe Ambetsa Oparanya & 3 Others [2013] eKLR

Macquarie Bank Ltd v Berg Unreported

Minnesota v Granite Gates, 1997

Nobert Oluoch Obanda v Republic [1983] eKLR

Nonny Gathoni Njenga & Anor v Catherine Masitsa & Anor [2014] eKLR

Republic v Barisa Wayu Mataguda [2011] eKLR

Republic v Commissioner of Domestic Taxes (Large Taxpayers Office) Ex parte Barclays Bank of Kenya Ltd [2015] eKLR

Rosenfeld v Zerneck, (2004, NY Slip Op 24143)

Stanbic Bank of Kenya v KRA (2009) eKLR