Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top-ranked lawyers

TMT

Uganda
Law and Practice
Joseph Matsiko, Augustine Obilil Idoot, Leonard Businge and Bahige David Mutume
Kampala Associated Advocate

chambers.com

2020

UGANDA

Law and Practice

Contributed by:
Joseph Matsiko, Augustine Obilil Idoot, Leonard Businge and Bahige David Mutume
Kampala Associated Advocates see p.13

Contents

Contributed by: Joseph Matsiko, Augustine Obilil Idoot, Leonard Businge and Bahige David Mutume
Kampala Associated Advocates

1. Cloud Computing

Laws and Regulations

In Uganda, there are no specific laws or regulations that restrict the delegation of processes or data to a cloud. However, the Data Protection and Privacy Act, 2019 (DPPA) mandates that where data is stored or processed outside Uganda this must be in a country which has adequate measures in place for the protection of personal data, at least equivalent to those provided for under the Act or, alternatively, ensure that the data subject's consent is obtained prior to storing or processing such personal data.

Specific Industries with Greater Regulation

As far as cloud computing is concerned, the National Cloud Computing guidelines make it mandatory for all government ministries, departments, agencies and local governments (MDAs and LGs) to use the government cloud for IT-enabled services and products. But these apply only to MDAs and LGs, not the private sector.

The National Cloud Computing guidelines require MDAs and LGs to adhere to the use of "Cloud First" for the design of IT-enabled services. This means that all IT products and services must be delivered from the government cloud infrastructure.

MDAs and LGs cannot use offshore cloud computing services according to the guidelines. However, the National Information Technology Authority – Uganda (NITA-U) may allow the use of such offshore cloud computing services on application by MDAs and LGs. Consequently, where MDAs and LGs apply and are permitted to use offshore cloud services (usually provided by private players), the National Cloud Computing guidelines may apply to such private players, not only because they are offering the service to an MDA or LG, but also because they may be offering said service to the public on behalf of the MDA or LG.

In addition, the Bank of Uganda prohibits commercial banks from sharing critical customer data such as bank account details and financial statements on the cloud. Furthermore, under the National Information Security Policy (NISF), all organisations, particularly those within and/or connecting to the government (such as banks), must require internal and external entities such as cloud storage providers to show compliance with mandated NISF requirements and approved security policies, before sharing or allowing connections to protected computer assets. As a minimum requirement, organisations must:

- identify and record risks involving external parties;
- create information exchange policies and procedures;
- use formal exchange agreements such as codes of connection and memoranda of understanding;
- assess compliance of exchange partners at least annually or when required; and
- disconnect/end sharing with non-compliant entities.

Processing of Personal Data

The DPPA regulates the processing of personal data in Uganda generally. Therefore, cloud users and cloud providers must comply with the requirements under part III of the DPPA, which governs the processing of personal data. For instance, any personal information stored on a cloud must be obtained with the consent of the data subject unless:

- the processing is authorised or required by law;
- it is necessary:
  - (a) for the proper performance of a public duty by a public body;
  - (b) for national security; or
  - (c) for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law;
- it is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
- it is necessary for medical purposes; or
- it is necessary for compliance with a legal obligation to which the data controller is subject.

Under the DPPA, data subjects can stop cloud users and providers from processing any personal data if it is not obtained for any of the purposes listed above.

MDAs and LGs are required, under the National Cloud Computing guidelines, to classify all information assets as guided by the technical risk assessment and security classification standards of the NISF and submit the same to NITA-U. Any information classified as secret or top secret must be stored or processed onshore in the government cloud.

2. Blockchain

Risk and Liability

The biggest challenge and risk involved in the launch and use of blockchain technology in Uganda is the absence of a regulatory regime. Regulators and users are still grappling with how to navigate the new technology.

In Uganda, the most common technology using blockchain is cryptocurrencies. Only limited protection is offered to cryptocurrencies, which means that investing in unregulated cryptocurrencies is a huge risk. The Central Bank does not have comprehensive oversight of all financial service firms and institutions and its supervision typically spans commercial banks,

credit institutions, foreign exchange bureaus and money remittance service providers.

Fortunately, Uganda is one of the few countries on the African continent whose government has shown willingness to embrace this technology. However, the Bank of Uganda remains firmly opposed to the use of cryptocurrencies and regularly issues cautionary statements to the public against their use.

As far as liability is concerned, since there are no laws regulating the use of blockchain technology, it is difficult to identify where liability lies in case of a dispute. Given the different players in any blockchain system, end users may find it impossible to put the blame on any one of the players. For instance, blockchain allows various transactions to be carried out in a short amount of time through the use of smart contracts, and such transactions definitely create regulatory headaches.

Persons interested in launching or establishing blockchain systems in Uganda must, therefore, clearly define the obligations and liabilities of the various players such as developers and end users in order to create a system that guarantees remedies for any wrong done or loss caused to an end user.

Intellectual Property

There are several areas in a blockchain system that can create a number of intellectual property rights, such as patents and even trademarks. These rights may be created in developing the blockchain or using it to deliver a service to an end user. The different players in any blockchain will definitely want to protect or own these intellectual property rights as usage grows over time.

Data Privacy

Due to the various transactions that are enabled in a blockchain system, a lot of data, both personal and public, will be collected and processed within the system. The DPPA regulates the way such data must be collected and processed in Uganda.

The data aspects of blockchains are governed by the DPPA and developers must take into consideration the core rules/principles of data collection and use outlined in **6. Key Data Protection Principles**. Generally, this data must be collected in a lawful manner and personal data should only be collected with the prior consent of the data subject.

Since the blockchain enables contractual relationships between people, developers must ensure that it does not disclose any personal data without the permission of a data subject, and any collection or processing of personal data within the blockchain must not be done in a manner that infringes on the privacy of a data subject.

Jurisdictional Issues

Given that there is no law or guidelines on the use or creation of blockchain technology, as cases come to court for dispute settlement, the main problem is what legal regime would be appropriate for the aggrieved parties. There is the question of territorial jurisdiction – where the offence occurred or where the transaction took place, more so in relation to extraterritorial jurisdiction – where the act or its effects fall outside the remit of Ugandan courts.

Another pertinent question for the courts would be the applicability of existing laws on electronic transactions, like the Computer Misuse Act, to digital assets whose ownership is not always easy to ascertain. In addition, the blockchain is hosted on the internet, which is universal. As such, it will not be easy to establish territorial jurisdiction for any crimes or offences committed on the internet since they take place in cyberspace, which does not have defined territorial boundaries.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

Big data, machine learning and artificial intelligence (AI) have become an essential part of the technology industry in Uganda. While big data refers to the collection, storage, organisation and utilisation of large amounts of data, tools such as machine learning (which is a branch of AI) are used to aid the speedy processing of large amounts of data at speed. In turn, some AI systems need big data to function properly. The legal considerations for these three aspects are, therefore, intertwined and are considered concurrently below.

Liability and Insurance

There are currently no laws or regulations governing big data, machine learning and AI in Uganda. There is no legal regime or procedures by which one could attribute liability for actions performed by a machine without human involvement.

AI involves the creation of machines that emulate human performance typically by learning, understanding complex concepts, and reaching conclusions as well as decisions. Since humans are liable for their actions, the issue with AI is whether machines can be held liable for their actions to the same extent. Under Ugandan law, machines are not recognised as legal persons and cannot, therefore, sue or be sued. But it should be noted that AI machines/computer systems may be products/services which must be up to standard when used by the final consumer. Where an AI tool, system or machine causes loss or damage to a final consumer, the developer or controller of such tool or system will be liable if he or she fails to show that

reasonable care was applied while manufacturing the said tool or fails to show that the system controller exercised reasonable care while utilising the said AI tool or system to perform a given task. AI developers, controllers and users must therefore exercise reasonable care to prevent loss or damage to final consumers in order to avoid the attribution of liability onto themselves.

Data Protection

AI, machine learning and big data all require data as a raw material. This means that the risk of illegally obtaining and misusing personal data will be higher than ever for companies or persons that venture into AI and big data.

The DPPA requires all data processors and controllers to obtain the consent of the data subject before using or processing personal data. Data collectors, data processors and data controllers have to ensure that data is not collected, held or processed in a way that infringes the data subject's privacy. Under the DPPA, data subjects have the right to be forgotten. Therefore, any person who collects personal data cannot retain such data for a period longer than is necessary to achieve the purpose for which the data was collected, unless permitted by law or by consent of the data subject.

This will most certainly be a challenge for AI and big data which rely on the availability of large-scale non-structured data. It is very important for companies and other persons using AI and big data systems to abide by the strict requirements of the DPPA before collecting or processing personal data. They must note that, under part VIII of the Act, any unlawful disclosure, destruction, collection, concealment or alteration of personal data is an offence.

Intellectual Property (IP)

The emergence of AI technology has brought into question some important traditional concepts of IP in Uganda. AI technology is capable of using collected data in order to create or generate content such as videos, music, images and books or novels. AI systems will be able to use machine learning features to understand and use data which contains similar content in order to create or invent its own content. In such circumstances, there is no doubt that the AI system or machine is the inventor or author.

The current IP regime in Uganda does not recognise machines or computer systems as inventors or authors. The Copyright and Neighbouring Rights Act, 2006 defines an author as a physical person who creates work, while the Industrial Property Act, 2014 defines an inventor as a person who devises an invention and it includes the legal representative of the inventor. This means that the creators or handlers of AI systems that invent or author certain works will be recognised as the owners of such works.

Secondly, if AI systems and machines are not recognised as legal persons under the law, it follows that they cannot be held personally liable for infringing on an IP right held by another person. In reality, AI systems are very likely to infringe on trade marks, patents, copyrights and other rights held by other people. This is due to the vast amounts of data used by such systems to create output such as art, songs and writings which may infringe on the rights of another. To counter this, manufacturers and handlers of these AI systems and machines must program these machines to create or author works that are not likely to infringe on existing IP rights.

The current IP legal regime is not alert to such a reality. As such, there is a great need for the laws and regulations to evolve so that they can properly deal with the above questions in order to prevent the disruption that AI will most likely cause.

Jurisdiction

Big data, AI and machine learning will also raise questions in relation to the traditional understanding of jurisdiction and the rules that govern different jurisdictions. In Uganda, before a court determines on a matter, it must first ascertain that it has the jurisdiction to do so.

For instance, since big data, AI and machine learning systems may be hosted in one country and used in another, it may be difficult to determine whether the Ugandan courts have jurisdiction to handle any dispute that emanates from such a transaction. In fact, lack of jurisdiction is likely to be a common preliminary objection against claims involving such technology systems. As such, the Ugandan legislature must enact legislation specifically to address the issue of jurisdiction in relation to big data and AI.

Fundamental Rights

The advent of AI and big data is set to raise a number of human rights issues. For example, the requirement for large volumes of data is likely to see the right to privacy of data being forsaken since the personal data of individuals is being shared and/or processed without their knowledge or consent. To counter this, NITA-U will have to step up its regulatory function to protect the integrity of personal data.

Right to Equality and Non-discrimination

Since some AI systems make decisions based on training data fed into the system by humans, it is obvious that some data will contain certain human biases. These systems may, therefore, be forced to make biased decisions premised on religion, race, tribe or political opinion. The onus is on AI and big data developers

and users to create systems that check and ensure that such biases are eliminated in order to avoid human rights violations.

Right to Privacy

AI and big data require large amounts of data in order to function properly. As already noted above, the DPPA prohibits the control, collection and processing of personal data in a manner that infringes on the privacy of a data subject. AI and big data systems must comply with the requirements of the DPPA as far as personal data is concerned in order to avoid violating a data subject's right to privacy.

4. Legal Considerations for Internet of Things Projects

There is no law or regulation in Uganda that specifically regulates machine-to-machine communications. However, it is important that machine-to-machine communications should not result in the commitment of the following offences under the Computer Misuse Act 2011:

- unauthorized disclosure of any electronic data, record, book, register, correspondence, information, document or any other material to any other person, or use for any purpose other than that for which he or she obtained access, to any other person;
- unauthorized intentional access or interception of any program or data;
- unauthorized intentional interference with data in a manner that causes the program or data to be modified, damaged, destroyed or rendered ineffective;
- unlawful production, sale, offer to sell, procurement for use, design, adaptation for use, distribution or possession of any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performance of any of those acts with regard to a password, access code or any other similar kind of data;
- utilisation of any device or computer program specified in (d) above in order to unlawfully overcome security measures designed to protect the program or data or access to that program or data;
- access to any information system so as to constitute a denial including a partial denial of service to legitimate users;
- commission of any of the above acts with intent to commit or facilitate the commission of a further offence;
- commission of any act which causes an unauthorised modification of the contents of any computer with the requisite intent and knowledge at the time of commission of the act;
- securing access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer service;
- unauthorised interception or causing to be intercepted directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device whether similar or not;
- unauthorised interception or causing to be intercepted without authority, or using or causing to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence;
- knowingly and without authority or lawful excuse interfering with or interrupting or obstructing the lawful use of a computer or impeding or preventing access to or impairing the usefulness or effectiveness of any program or data stored in a computer;
- knowingly and without authority disclosing any password, access code or any other means of gaining access to any program or data held in any computer knowing or having reason to believe that it is likely to cause loss, damage or injury to any person or property;
- carrying out electronic fraud (deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both);
- producing child pornography for the purposes of its distribution through a computer, offering or making available child pornography through a computer, distribution or transmission of child pornography through a computer, procuring child pornography through a computer for personal use or unlawfully possessing child pornography on a computer or making available pornographic materials to a child. "Child pornography" includes pornographic material that depicts a child engaged in sexually suggestive or explicit conduct, a person appearing to be a child engaged in sexually suggestive or explicit conduct or realistic images representing children engaged in sexually suggestive or explicit conduct;
- cyber harassment (the use of a computer for making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent, threatening to inflict injury or physical harm to the person or property of any person or knowingly permitting any electronic communications device to be used for any of these purposes);
- wilfully and repeatedly using electronic communication to disturb or attempting to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues;
- cyber stalking (wilfully, maliciously, and repeatedly using electronic communication to harass another person and

making a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family).

Regarding communications secrecy, under the Regulation of Interception of Communications Act 2010, it is an offence for any person to disclose any communication or information which they obtained in the exercise of their powers or the performance of their duties under this Act, except to any other person who of necessity requires it for the like exercise or performance of his or her functions under this Act, or information which is required to be disclosed under any law or as evidence in any court of law. Similarly, service providers or protected information key holders and their employees are prohibited from disclosing any information they obtained in compliance with this Act. Any person who discloses any information in contravention of this provision is liable on conviction to a fine not exceeding 120 currency points or to imprisonment for a period not exceeding five years, or both. In addition, the minister responsible for information and communications technology, may revoke the licence of any service provider or protected information key holder who discloses any information in contravention of the above provision.

Persons interested in starting such projects should note that certain devices may have to be Type Approved by UCC as per the UCC Type Approval guidelines and the requirements therein, discussed in **8. Scope of Telecommunications Regime**.

In relation to data protection, it should be noted that data is a big component of the internet of things (IoT) projects and as such, the interconnected devices within the digital ecosystem of a particular project collect data and aggregate it in order to achieve the aim of that project. Companies and persons intending to implement IoT projects must comply with the requirements of the DPPA 2019 which seeks to protect the privacy of individuals and their personal data by regulating the collection and processing of such data.

The DPPA works to ensure the safety of the personal information of individuals interacting with these devices, a circumstance that is more prevalent in this age of technology and smart equipment. However, the DPPA defines data collectors and controllers as natural persons. This definition does not include machines and it would, therefore, be difficult to identify who the data collector, controller or processor is in this case.

It is also worth noting that in many IoT projects, the devices used may require human interference. Therefore, it could be argued that the machine is not the data controller or collector, but rather, that the human behind the machine is.

Regarding secrecy of communications, note that company and personal data may be subject to the Regulation of Interception of Communications Act which allows security agencies, after obtaining a warrant from a designated judge, to intercept calls, emails and electronic surveillance for purposes of safeguarding public interest and protecting the national economy from terrorism.

5. Challenges with IT Service Agreements

In Uganda, there is no law or regulation that regulates IT service agreements. Such agreements are governed by the Contracts Act, 2010 and best practices in the sector.

Restrictions on data storage location are provided for in the DPPA, as mentioned in **1. Cloud Computing**. There are no price revision restrictions under Ugandan law.

6. Key Data Protection Principles

Core Rules Regarding Data Protection

As already noted, in Uganda, the DPPA regulates the use, collection, control and processing of data. The DPPA is in line with international regulations such as the UK Data Protection Act, the African Union Convention on Cyber Security and Personal Data Protection and the GDPR.

Personal data is defined in the DPPA as recorded information from which a person can be identified and includes data that relates to nationality, age, marital status, educational level, occupation, ID number, symbols attached to a person, identity data or any other information in the possession of, or likely to come into the possession of, the data controller and includes an expression of opinion about the individual.

The Constitution of the Republic of Uganda 1995 as amended provides in Article 27 that: "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property." The constitution therefore guarantees the right to privacy inclusive of personal data and correspondence.

The core rules of data protection include the principles of data collection, duties of the data collector/processor/controller, rights of the data subject, dispute resolution mechanisms, prohibitions and offences under the Act.

Principles of data protection apply to a data collector, processor, controller or anyone who collects, processes, holds or uses

personal data. This means that whenever any such person collects personal data, they are mandated to follow these principles without fail:

- accountability: the data collector or processor must be accountable for the data they collect;
- fair and lawful collection: the data must be specific, explicitly defined and for a related purpose;
- minimalism: the data collected, processed or controlled must be adequate, relevant information as contrasted to excessive or unnecessary personal data, and nothing in excess of data authorised by law or required for a specific purpose;
- the concerned persons must retain data for the period authorised by law or for which data is required;
- quality of information – quality personal data should be complete, accurate, up to date and not misleading;
- the persons collecting, processing or controlling the data must ensure the transparency and participation of the data subject (this calls for consent); and
- the persons collecting, processing and controlling the data must observe security safeguards in respect of the data.

Anyone in Uganda who intends to deal directly with data, especially personal data, whether as data controllers, collectors or processors, must adhere to the above rules and all the requirements under the DPPA.

Distinction Between Companies/Individuals
The DPPA is specifically for personal data of individuals but affects companies as well insofar as they are the data collectors, processors and controllers. It imposes upon them the duties as listed above for as long as they are in contact with personal data.

On the other hand, company data found in private documents kept or filed at a public office as per the Evidence Act becomes part of the record of public documents. This means that every public officer having custody of a public document, which any person has a right to inspect, shall give that person on demand a copy of it on payment of the required fees for a copy, together with a certificate written at the foot of the copy that it is a true copy of that document or part of the document, as the case may be, and the certificate shall be dated and signed by the officer with his or her name and official title, and shall be sealed whenever the officer is authorised by law to make use of a seal, and the copies so certified shall be called certified copies.

General Processing of Data
The DPPA requires data controllers and processors to obtain the consent of a data subject before processing or collecting data. Furthermore, they have to process data in conformity with the principles of data collection, processing and control as listed above.

Processing of Personal Data
Under the DPPA, personal data must be collected in a manner that does not infringe on the privacy of a data subject.

The data subject has the paramount right to give or withhold consent to collection or processing of personal data except where it is a requirement by law and/or necessary for:

- proper performance of a public duty by a public body;
- national security;
- prevention, detection, investigation, prosecution or punishment of an offence or breach of law;
- performance of a contract to which the data subject is a party;
- medical purposes; and
- compliance with a legal obligation to which the data controller is subject.

Where this consent is given, the rest of the principles of data collection under the DPPA shall apply, as they are auxiliary to the other rights of the data subject, that is, accessing data, being informed of the purpose for which the data is being collected, only giving accurate information, the right to complain against the data controllers, processors and collectors, and to keep the information confidential and for the lawfully recognised retention period, among others.

7. Monitoring and Limiting of Employee Use of Computer Resources

As previously discussed, Uganda protects the right to privacy both in the constitution and in international law and this right to privacy extends to the work environment.

However, labour relations are contractual in nature and the Contracts Act read in conjunction with the Employment Act of Uganda allows parties to freely contract, subject to the Employment Act. Any agreement between an employee and an employer which excludes the provisions of the Employment Act shall be void and of no effect. This means that an employer and an employee may negotiate and allow for regulation of a significant part of the content of their relations, such as monitoring of computer use.

Although Uganda has no principal law on monitoring by employers, Uganda is a member of the International Labour Organization (ILO). As such, it subscribes to the practice directives of the International Labour Office, specifically, the ILO

code of practice on the protection of workers' personal data 1997. The code provides insight on how to regulate monitoring in workplaces. It provides for the following:

- personal data should be processed lawfully and fairly and only for reasons directly relevant to the employment of the worker;
- workers may not waive their privacy rights;
- if workers are monitored, they should be informed in advance of the reasons for monitoring, the time schedule, the methods and techniques used and the data to be collected, and the employer must minimise the intrusion on the privacy of workers;
- secret monitoring should be permitted only:
  (a) if it is in conformity with national legislation; or
  (b) if there are reasonable grounds for suspicion of criminal activity or other serious wrongdoing;
- continuous monitoring should be permitted only if required for health and safety, or the protection of property; and
- workers should have the right to be regularly notified of the personal data held about them and the processing of that personal data.

Furthermore, monitoring of employee use of computers, beyond contractual terms, is permitted in Uganda insofar as it concerns reasonable suspicion of computer-related criminal activity. The Computer Misuse Act, 2011 was enacted to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers through crimes like child pornography, cyber harassment, offensive communication, and cyber stalking; and to make provision for securing electronic transactions in a trustworthy electronic environment.

Other than for the purpose of monitoring criminal activity, the employee must be notified that their use of the computer will be monitored and that the employer will have access to the computer. Where an employee has not been notified and has not consented to the monitoring and access of their computer use, the employer may be found culpable under the Computer Misuse Act.

8. Scope of Telecommunications Regime

In Uganda, all equipment intended for use in public radio and telecommunication networks, provided it meets national regulations and requirements, is granted what is known as "type approval". The process of type approval is intended to ensure that radio communication and telecommunications equipment complies with a set of national and international regulatory standards and requirements.

Type approval of radio and telecommunications equipment in Uganda is defined as one of the functions of the Uganda Communications Commission (UCC) under the Communications Act, Cap 106 Laws of Uganda and the regulations made thereunder (specifically the UCC Regulations of 2005).

Type approval is regulated by the Uganda Communications (Equipment Type Approval) Regulations, 2019. Any persons (individuals and business entities) intending to use radio communication and telecom equipment should first ensure that the equipment has been type approved for use in Uganda. UCC maintains a database of all radio communication and telecom equipment that has been type approved for use in Uganda.

Technologies That Require Approval
According to the type approval regulations, telecommunication terminal equipment that requires approval includes (but is not limited to):

- telephones (ordinary, cordless, executive, secretarial sets);
- telephone answering and recording systems;
- mobile and fixed line network system components;
- cellular telephones;
- payphones (coin and card operated);
- call monitoring and logging systems;
- subscriber private meters (SPMs);
- facsimile transceivers;
- call routing apparatus;
- private and public branch exchanges (PBXs);
- key telephone system (KTS);
- internet protocol telephone sets;
- small business system (SBS);
- multi-line systems;
- voice messaging systems; and
- data and fax modem devices.

Vendors and manufacturers of telecommunication equipment must check with the UCC type approval database to confirm devices that have been type approved by UCC.

Type approval for RFID is dependent on the use of the equipment, the service and co-existence with other users within the same frequency band. The equipment must meet UCC recommendations.

Requirements to Bring a Product/Service to the Market
All applications for type approval should be made in writing to the executive director of the Uganda Communications Com-

mission. Applications for type approval of radio communications and telecom equipment should include the following:

- a sample of the equipment to be marketed and/or installed (the applicant bears the cost of transporting the equipment sample to UCC);
- a letter from the equipment manufacturer or manufacturer's representative authorising the vendor to act as an agent, if the vendor is an agent of an equipment manufacturer;
- technical/operational documentation (including details of transmission parameters, operating media, interface specifications, fulfilment of service technology requirements, etc) in English;
- a copy of a test report from the manufacturer or an accredited test laboratory, if available;
- proof of previous type approvals granted by other regulators, if available; and
- the type approval application processing fee, which is non-refundable.

UCC then assesses and evaluates the application. Where necessary, laboratory tests are carried out on the sample terminal. After the laboratory tests, UCC may provide the test results to the applicant, but it is under no obligation to return the sample equipment. This is because of the high probability of destruction of the sample equipment during the testing process.

UCC compiles an evaluation report for each piece of equipment submitted and provides an appropriate technical decision as to whether the equipment complies with mandatory standards and requirements. This is an internal report and is not usually made available to the applicant.

If the application satisfies UCC requirements in all aspects, then UCC advises the applicant within 21 working days from the date of submission of the application on the type approval fee to be paid. (If laboratory tests are required, then the number of days may increase, but the applicant will be duly informed in advance.) Please note that the type approval fee is paid after the evaluation of the application and is different from the application processing fee which is paid upfront and is non-refundable.

If the applicant pays the type approval fee, then UCC grants the equipment type approval and a type approval letter is issued to the applicant. If the application is rejected, UCC informs the applicant of the rejection and advises the applicant to re-export all sets of the rejected equipment within 30 days.

9. Audio-Visual Services and Video Channels

Requirements for Providing an Audio-Visual Service

In Uganda, it is an offence to install or operate a television station, radio station or any related broadcasting apparatus without a licence issued by the UCC under the Uganda Communications Commission Act 2013 (UCCA 2013).

Under the UCCA 2013, before such licence is granted, UCC must take into account proof of existence of adequate technical facilities, the location of the station, the social, cultural and economic value, as well as the environmental impact assessment.

The Uganda Communications (Licensing) Regulations, 2019 (2019 Licensing Regulations) provide the procedures to be followed when applying for licensing of telecommunications and telecommunication services, broadcasting and broadcasting services, radio communication and radio communication services, installation of television and radio stations as well as licensing of film, video halls and cinematograph theatres, among others.

Under these regulations, any person who intends to provide telecommunications or telecommunication services regionally or nationally in Uganda must apply to UCC for either a public infrastructure provider licence or a public service provider licence, or both, depending on the nature of the project. The applicant must pay the prescribed application processing fee of USD2,500 and an annual fee of USD30,000 for a public infrastructure provider licence or USD10,000 for a public service provider licence.

A person who intends to broadcast or provide broadcasting services must apply to UCC for either a public infrastructure provider licence, a public service provider licence or a distributor licence depending on the nature of his/her project. The application processing fee for broadcasting services for television stations is USD2,500.

An application for a broadcasting licence must be made to UCC in Form B set out in Schedule 2 to the 2019 Licensing Regulations. The application must include:

- the category of broadcasting technology applied for;
- evidence of the applicant's legal status in Uganda;
- a physical address that shall serve as the official address of the service;
- a statement of ownership, disclosing the full identities of the shareholders;
- a viable business plan;
- the minimum capital requirements;

- evidence of financial solvency and the ability to fund the business venture;
- evidence of technical capability in terms of the personnel and equipment to carry out broadcasting;
- evidence of relevant experience and expertise to carry out broadcasting services;
- proof of possession of an interconnect agreement, signal distribution agreement or access agreement with a public infrastructure provider or public service provider; and
- evidence of proprietorship of premises where programming and distribution of content will be done.

Note that unless otherwise required by UCC, an applicant for a licence to provide subscription broadcasting services may apply to UCC for authorisation to provide broadcasting services to members of the public on behalf of a person licensed to provide land satellite broadcasts in Uganda. Such applicant shall satisfy UCC that it has the capacity to offer a minimum of ten channels to each subscriber and shall submit a copy of the agreement entered into between the person licensed to provide land satellite broadcasts in Uganda and the applicant.

In addition, UCC may, at any time after the filing of an application for a licence, require from an applicant further written statements of fact to enable it to determine whether the application for a licence should be granted or denied. Accordingly, an applicant for a licence shall be bound by all terms, commitments, offers, presentations, proposals, plans and obligations stated in the application and shall ensure the accuracy of the information and representations submitted in the application.

Furthermore, in order to operate specified radio communications on an assigned radio spectrum or a specified part of the spectrum, an applicant must apply for a radio communications licence based on the classification of services provided. Radio communications services are classified into two: services for non-commercial spectrum uses for socially desirable services and commercial spectrum uses. The application processing fees for radio stations are UGX6.24 million for non-commercial radio stations and UGX9.4 million for commercial radio stations.

Subject to the provisions of the UCCA 2013, the following persons are prohibited from applying for a broadcasting licence:

- a person who ceases to be an eligible person within the meaning of Section 2 of the Act;
- a person to whom the granting of a licence is not in the public interest;
- a person convicted of an offence under the Computer Misuse Act, 2012; and
- a person convicted of broadcasting prohibited content under the Uganda Communications (Content) Regulations, 2019.

An application for a radio communications licence must be made in Form C set out in Schedule 2 to the 2019 Licensing Regulations. The application must include:

- details about the character and the financial, technical and other qualifications of the applicant to operate the station;
- the ownership and location of the proposed station and of the stations, if any, with which the proposed station intends to communicate;
- the frequencies and the power required;
- the hours of the day or other periods of time during which it is proposed to operate the station; and
- the purposes for which the station is to be used.

The 2019 Licensing Regulations prohibit persons from operating cinematograph theatres, video halls or film libraries without a cinematograph licence granted by UCC under these regulations and the licence must be displayed in a conspicuous place at the premises for which it is issued. A licence for an exhibition premises cinema costs USD270.

According to the same regulations, it is illegal for a person to carry on the business of distributing films or video works or other content for commercial display to the public without a licence granted by UCC. A national distributor licence costs USD270.

Requirements for Providing Online Data Communication Services

All online data communication service providers, including online publishers, online news platforms, and online radio and television operators in Uganda must apply and obtain authorisation from UCC.

The UCCA 2013 gives UCC the mandate to monitor, inspect, license, supervise, control and regulate all communications services which include audio, visual or data content. Data is defined to mean the electronic representation of information in any form. Therefore, provision of any services that involve communication to the public of any content, whether by way of audio, video, sound, still or moving pictures, is a communication service that is subject to the regulatory control of the commission.

Through a public notice in 2018, UCC exercised its mandate under the UCCA 2013 and classified online data communication services as a communication service for which one requires authorisation from UCC.

This means that anyone who wants to operate an online video channel like YouTube in Uganda must apply to UCC for approval and licensing. On 2 April 2018, UCC embarked on enforcement activities against all non-compliant providers of online data communication services. UCC may direct internet service providers (ISP) to block access to any website or streaming service that is non-compliant.

10. Encryption Requirements

There are no legal requirements in Uganda that govern the use of encryption and there are no circumstances under which a company in Uganda is required to use encryption. Companies can therefore use encryption without any restrictions in Uganda. For instance, WhatsApp introduced end-to-end encryption without any resistance or restriction.

The use of encryption in Uganda does not exempt an organisation from any rule or law.

Contributed by: Joseph Matsiko, Augustine Obilil Idoot, Leonard Businge and Bahige David Mutume
Kampala Associated Advocates

Kampala Associated Advocates is a full-service law firm that advises clients on a range of legal matters, from litigation and arbitration; banking and finance; oil and gas; to intellectual property; telecommunications, media and technology. It has a total of 11 partners with varied areas of specialisation, assisted by over 16 lawyers and legal consultants, which arguably makes KAA the largest law firm by partner head count in Uganda. KAA's team of top lawyers has proven expertise and knowledge of the Ugandan legal and regulatory spectrum as well as background within the TMT sector, and is able to offer relevant and incisive legal and business advice to suit each client. The team represents providers, clients and regulators of communications services, IT services and infrastructure in regulatory compliance, intellectual property, telecommunications, licensing within the sector, data protection and privacy, fintech, e-payments, e-commerce, software licensing, domain name registrations and dispute resolution. KAA partnered with the Commonwealth Telecommunication Organisation (CTO) in a consultancy commissioned by the National Information Technology Authority (NITA-U) to conduct a gap analysis of the policy, legal and regulatory framework for Uganda's information and communications technology (ICT) sector. KAA also acted as a consultant on the review of the telecommunications licensing framework and has represented Ugandan telecommunications regulators in various matters.

Authors

Joseph Matsiko is currently managing partner at the firm. He is recognised as one of the best litigation, arbitration and disputes lawyers in Uganda and is acclaimed in the legal industry for his excellent litigation skills. He has been engaged in the representation of a leading telecom operator in Uganda, MTN Uganda, since 2007 and has handled multimillion-dollar disputes for them. He has also represented the Uganda Communications Commission (UCC) since 2010, acting as lead counsel in handling their legal work and disputes. Joseph is a member of the Uganda Law Society and the East African Law Society.

Augustine Obilil Idoot is currently a partner at KAA, with expertise in technology, media and telecommunications law. Through his litigation practice, he has been involved in some of the most interesting disputes in the country touching on various technology and telecommunications issues. He has also advised a number of private organisations on legal and regulatory compliance issues in relation to some of the emerging technologies. He is a member of the Uganda Law Society and East African Law Society, as well as the Chartered Institute of Arbitrators (CIArb).

Leonard Businge is a senior associate in the corporate and finance, and technology, media and telecommunications departments. He has worked with KAA since 2013. Leonard was part of the team that advised a mobile telecommunications company on the potential acquisition of its radio frequency spectrum by another telecommunications company in a deal valued at USD16 million. He advises various entities on structuring their operations to comply with the recently enacted Data Protection and Privacy Act, 2019, as well as the new licensing legal regime recently enacted by the UCC. Leonard is a member of the Uganda Law Society and East African Law Society.

Bahige David Mutume is a paralegal in the litigation department of KAA whose experience extends to the corporate advisory department, and technology, media and telecommunications law. He was part of the KAA team that advised the National Information Technology Authority in Uganda and the Ministry of Information and Technology on the gap analysis of the policy, legal and regulatory framework in Uganda's information and communications technology sector.

Contributed by: *Joseph Matsiko, Augustine Obilil Idoot, Leonard Businge and Bahige David Mutume*
Kampala Associated Advocates

Kampala Associated Advocates

KAA House
Plot 41 Nakasero Road
9566 Kampala
Uganda

Tel: +256 312-244100
Email: info@kaa.co.ug
Web: www.kaa.co.ug