THE REPUBLIC OF UGANDA

IN THE COURT OF APPEAL OF UGANDA AT KAMPALA

CRIMINAL APPEAL NO. 223 OF 2021
(ARISING FROM HIGH COURT CRIMINAL SESSION CASE NO. HCT-00-AC-SC-084 OF 2021)
(ARISING FROM SUPREME COURT CRIMINAL APPEAL NO. 92 OF 2018)
(CORAM: BAMUGEMEREIRE, MADRAMA, LUSWATA, JJA)

1. GUSTER NSUBUGA}
2. ROBINHOOOD BYAMUKAMA} .....APPELLANTS

VERSUS

UGANDA} ..... RESPONDENTS

(Appeal from the judgment of Hon. Justice Paul K. Mugamba J, as he then was of the High Court, Anti – Corruption Division at Kololo delivered on 3rd April, 2013 in criminal case no. 084 of 2012).

JUDGMENT OF COURT

This is an appeal from the decision of **Mugamba J** (as he then was) of the High Court Anti – Corruption Division in Criminal Session Case No. 084 of 2021. The appellants and 2 others were indicted on 6 counts under the Computer Misuse Act, 2011 (CMA) and the East African Community Customs Management Act, 2009 (EACCMA). They were indicted in count 1 with unauthorised use and interception of computer services contrary to sections 15(1) and section 20 of the Computer Misuse Act 2012, in **count 2** with electronic fraud contrary to section 19 of the Computer Misuse Act, 2011, in **count 3** with unauthorised access to data contrary to Sections 12(2) and 20 of the Computer Misuse Act, 2011, in **count 4** with producing, selling or procuring, designing an being in possession of devices, computers, computer programs, designed to overcome security measures for protection of data contrary to Section 12(3) and 20 of the Computer Misuse Act, 2011, in **Count 5** with unauthorised access to a customs computerised system contrary to Section 191 (1) of the East African Community Customs Management Act, 2009 and in **count 6** with fraudulent evasion of payment of duty contrary to section 203(e) of the East African Community Customs Management Act, 2009.

A2 & A3 were acquitted while the appellants who were described as A1 and A4 respectively were convicted on 5 counts and acquitted on count 6. The appellants were each sentenced, on counts 1, 3 and 4 to 8 years' imprisonment, on count 2 to 12 years' imprisonment and on count 5 each convict was sentenced to a fine of US$ 4,500. All imprisonment sentences on the counters were to be served concurrently.

The appellants being dissatisfied with the conviction and sentence appealed to this court in **Criminal Appeal No. 14 of 2013** and the appeal was allowed on one ground 1 that failure to take plea to the amended indictment occasioned a miscarriage of justice. The Justices of the Court of Appeal on 23rd October, 2018 ordered a retrial and found no reason to delve into the other grounds of appeal and a retrial commenced at the high court before Hon. Justice Gidudu.

In the meantime, before the retrial could take place the Respondent was dissatisfied with the decision of the Court of Appeal and appealed to the **Supreme Court vide Criminal Appeal No. 92 of 2018** whereat they obtained a stay of proceedings of the High Court pending appeal. On the 16th August, 2021, the Supreme court delivered its judgment wherein they set aside the orders of the Court of Appeal, reinstated the orders of the trial court, cancelled the appellants bail and sent them to prison. They held that there was no miscarriage of justice by not taking plea to the amended indictment and a retrial was not called for. The appellants then had the matter in the court of appeal fixed for hearing on the merits.

When this matter came up on the 20th June, 2021, learned Counsel Mr. Lomuria informed court that they had filed **Misc. Application No. 53 of 2022** for the appeal to be struck out as being incompetent. The matter was argued and the crux of the submission of the State was that the decision setting aside the judgment of the trial judge and ordering a retrial of the Court Appeal was set aside by the Supreme Court which reinstated the conviction and sentence of the appellant by the High Court and the matter had rested having been determined by the highest Appellate Court. The appellants on the other hand argued that the Court of Appeal had not heard the appeal on merits but determined it on a point of law and concluded that the trial of the High Court was a nullity. In their judgment, the Court of Appeal, allowed the appeal on the ground that the

appellants had not taken plea to the amended indictment and this rendered the trial a nullity. They found no reason to delve into the merits of the rest of grounds of appeal on that basis the appellants should be retried. We held that when the Supreme Court overturned the Court of Appeal decision, and reinstated the High court judgment, it was on the ground that the judgment was not a nullity. This left the other grounds of appeal of the appellants intact and there is a valid appeal before this court. The Court rejected the submission of the applicant (URA) that the decision of the Supreme Court was final on the merits of the appeal or that this court lacks jurisdiction to hear this appeal. On 20th June, 2022 we dismissed Misc. Application No. 53 of 2022 and allowed this appeal to proceed on the merits on the other grounds not determined previously.

Bother parties were directed to file written submissions and judgment was reserved on notice.

GROUNDS OF APPEAL

1. That the learned trial judge erred in law when he wrongly admitted and heavily relied on the prosecution's electronic evidence and exhibits that were illegally seized, illegally extracted without a search warrant, fabricated and unauthentic contrary to the law hence wrongly convicting the appellants.

2. The learned trial judge erred in law and in fact when he convicted the appellants without the prosecution disclosing the Encase software forensic tool used and mirror images analysed to the defence, as required by the law thus occasioning a miscarriage of justice.

3. The learned trial judge erred in law and fact where he erroneously misdirected himself in evaluating evidence of the prosecution and cross examination evidence on record hence arriving at a wrong decision this occasioning a miscarriage of justice.

4. The learned trial judge erred in law when he commenced the trial and convicted the appellants without the assessors taking oath

contrary to the provisions of the law, thereby occasioning a miscarriage of justice.

5. The learned trial judge erred in law and in fact when he ignored major inconsistences and contradictions in the prosecution's evidence that the offences charged were proved beyond reasonable doubt hence occasion a miscarriage of justice.

6. The learned trial judge erred in law and in fact when he convicted and sentence the appellants twice for the same offence occasioning a miscarriage of justice.

7. The learned trial judge erred in law and in fact in ignoring and allowing the illegal conduct of the Uganda Revenue Authority to prosecute, investigate the appellants made foreign to the known legal modes of commencing prosecution thereby occasioning a miscarriage of justice.

8. The learned trial judge erred in law and in fact when he convicted the appellants passed excessively harsh sentence against the appellants on count 2 and count 5.

At the hearing of the appeal, the Appellants represented themselves while the respondent was represented by learned Counsel Mr. Lomuria Thomas Davis, an officer in charge of litigation in the prosecution unit of Uganda Revenue Authority (URA) assisted by learned Counsel Mr. Ronald Bashaba an officer from URA.

Ground one

That the learned trial judge erred in law when he wrongly admitted and heavily relied on the prosecution's electronic evidence and exhibits that were illegally seized, illegally extracted without a search warrant, fabricated and unauthentic contrary to the law hence wrongly convicting the appellants.

The appellants submitted that it is the most basic constitutional rule that searches conducted outside the judicial process, without prior approval

by a judge or magistrate are per se unreasonable (See **Coolidge vs. New Hampshire, 403 US. 443, 454-55 (1971) (Quoting Katz vs. United States, 389 US. 347, 357 (1967)).**

The appellants further submitted that the rules relating to authentication and best evidence when admitting electronic evidence defer from the rules relating to admissibility of records relied on **Kyllo vs. United States, 533 US.27,31 (2001**). Further, the trial judge's decision that the search and subsequent seizure on the arrest of A1, A2, A3 was lawful without a search warrant was erroneous for contravention of Section 28(1) of the Computer Misuse Act (CMA). This section requires a magistrate to issue a search warrant to a police officer and not an officer of URA to seize and take evidence from a computer.

The appellant submitted that Section 28(3) CMA allows seizure, search and copies to be make only under authority of a search warrant.

The appellants content that the learned trial judge based his decision on **Section 6(2)** of the Criminal Procedure Code Act yet this provision should not override the legal requirement under **Section 28(3)** CMA.

Further, they submitted that the appellants remained in custody for 4 days when the respondent was in possession of the items until when they were remanded in prison. In the premises, they submitted that the police and the prosecution had ample time to obtain a search warrant as required by the law.

Further, at the trial, the learned trial judge relied on **State vs. Alison 298 NC 135, 257 SE 2D 417(1979)** which is distinguishable from the current case. More so section **6(2)** applied where a person is in possession of anything found on the person who has been arrested. None of the witnesses including the investigating officer gave a reason why they searched without a search warrant. It is the appellant's submission that the trial judge was speculative in his decision when he held that the evidence of PW2, PW6 and PW26 the prevailing circumstances were such that instant response had to be given to a situation that had presented itself. Further, the trial judge misdirected himself when he held that the "*search and subsequent seizure was lawful*". The appellants content that section 28(3) of the CMA does not permit a police officer or a person not

authorised within the meaning of the terms "authorised officer" to conduct a seizure and extraction of electronic evidence from a computer system without the pre-requisite search warrant. They appellants relied on **McDonald V. United States, 335 U.S. 451 69 S. ct.191, 93 L.E.D 153(1948).** Where when allowing McDonald's motion for suppression of evidence and returning of the properties, the justices of the supreme court held that;

> "We are not dealing with formalities. The presence of a search warrant serves a high function. Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done not to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted. And so the Constitution requires a magistrate to pass on the desires of the police before they violate the privacy of the home".

They contend that the learned trial judge heavily relied on the evidence adduced by PW1, PW2, PW10 and PW26 which did not meet the requirements of Section 28(3) to convict the appellants. That in **Morgans V Director of Public Prosecution [1999] 1.W.L.R 968**, Justices (Kennedy L.J and Sullivan) allowed Morgan's appeal in respect of all five charges under section 1(1) unauthorised access of the Computer Misuse Act, 1990 on ground that these charges had been brought against him when they were out of time.

The appellants submitted that "**authorised officer**" under section 28(9) of the Computer Misuse Act, 2011 is defined as; "**a police officer who has obtained an authorizing warrant under subsection (1).** They submitted that from PW1 -26 none were authorised officers and none of them followed the investigation procedures that are set out clearly by the law under section 9, 10, 11, 28(3) and 28(8) of the Computer Misuse Act, 2011.

The appellants argued that the legislature intended to treat a search of a computer system without a warrant as unlawful and therefore the evidence acquired in unconventional form is inadmissible, illegal, null and void. Further, that PW2 Mr. Mwebesa Bruno, a Uganda Revenue Authority Officer who arrested and conducted the search on A1, A2, A3 and tendered exhibit P.4 (Certificate of search) testified that that Kayemba Isaac (PW10) also URA staff gave him instructions to do so and not the police. Further, detective Inspector Joseph Elyanu in his cross examination testimony said that he never had a search warrant when he searched and seized the 2nd appellant.

It was the appellants' submissions that the trial judge misdirected himself when he convicted the appellants on the basis of the electronic evidence extracted without a warrant and the appellants relied on **NSSF & Anor vs. Alcon International Limited CA NO. 15 of 2009 page 46-47** and **Hon. Sam Kuteesa & Anor vs. AG (Constitutional reference No. 54 of 2011) [2012] UG SC 2** to support their claim for exclusion of evidence.

The appellants submitted that the electronic evidence seized and samples or copies of application or data extracted without a search warrant are inadmissible and the learned trial judge ought not to have relied on any them since they were illegally obtained. They contend that this touches the core of the prosecution evidence (See **Chalangat Andrew Milton 7 others vs. Uganda CA No. 11 of 2012** and **Makula International Ltd Vs. His Eminence Cardinal Nsubuga & Another (1982) HCB 11.)**

The appellants also contend that the prosecution evidence was widely fabricated and unauthentic. It followed the unlawful seizure and extraction of electronic evidence, the prosecution preferred in evidence several electronic records as exhibits.

In relation to Exp. P.1 and P.2 the prosecution had under Section 29(2) CMA the burden to prove that the exhibits were authentic which evidential burden they did not discharge as they had formatted the URA computers from which they purport to have obtained the log and images. It is the learned trial judge erred to rely on the testimony of PW1 and exhibit P.1. The trial judge ought to have found that Exp. 1 and Exp. 2's source did not actually exist.

On exhibit P.3 PW1 testified that he did not print the chats and the question was what the source of these chats are or is? Who printed them? How did that person get them? Who is that person? They contend that the person ought to have been subjected to cross examination on the authenticity of the exhibit. It followed that the state did not prove its authenticity as required by the law and it was erroneous for the learned trial judge to heavily rely on it to convict the appellants. They contend that reliance on the fabricated evidence to convict the appellants was not only unjust but also illegal and contrary to public policy. (see **Farm International Ltd, Ahmed Farah vs. Mohamed Hamid Farih Civil Appeal No. 16 of 1993, and Makula International (supra), Christ for all Nations vs. Apollo Insurance Co. Ltd (2002) 2 EA 366** that illegality cannot be sanctioned by court).

The appellants submitted that the trial judge erred to rely on PW1 and PW10's evidence to convict the appellants, yet they failed to authenticate their electronic evidence (exhibits) and the question is how authentic Exp. 24, 25 and Exp. 26 were? Further, that without authenticity the reports from the alleged mirror images and primary hard disks leaves court with no evidence as what is contained in the report is what actually is in the primary hard disks, unlawfully extracted. Further, the appellants/defence were not given a chance to analyse these mirror images which were allegedly made/ produced with the state's software choice Encase on which the state had monopoly to the prejudice of the defence.

Appellants invited court to suppress this evidence and to hold that it was wrongly relied on and exercise the duty of this court to evaluate the evidence and reject the same.

The appellants also challenged the chain of custody, which was preferred in evidence (Exp. 23) as fabricated with an aim to implicate the appellants. The appellants concluded that there was glaring evidence on record that prosecution's exhibits Exp. 1,2,3,8,9,10,24,25,26,36,37,38 and 39 were seized and extracted contrary to the provisions of the law, and further, they were fabricated and unauthentic and invited the court to suppress the evidence contained thereon. They pray that that court allows the appeal on this ground and acquit the appellants.

On ground 1, the respondent's counsel submitted in reply that the major complaint of the appellants is that the prosecution did not comply with **Section 28(3) of the CMA** when they searched and seized computers and other items without a search warrant. However, **Section 7 EACCMA** clothed the respondent with such power as envisaged in **Criminal Procedure Act cap. 116** and **The Police Act** and **Section 6 (1) (b) Criminal Procedure Code Act (CPCA).**

The respondent submitted that it would defeat logic to arrest the 1st appellant and the group, recover the hacking implements and then look for a search warrant as the appellants seem to suggest. The respondent maintains that it does not accept the submission of the appellants that electronic evidence is prone to alterations, modifications and fabrication where improper or unlawful search and seizure is employed. That according to the testimony of PW10 electronic evidence and image acquisition cannot be altered, modified or fabricated.

The respondent's submitted that the evidence of PW1 was corroborated by PW11 that the 2nd appellant was employed by URA.

Further that the learned trial judge was right to rely on the electronic evidence because integrity of the evidence was never compromised and all the evidence was corroborated.

The Respondents counsel submitted that the argument of the appellant that the enforcement officer who conducted the arrest and subsequently searched the appellants was not an authorised police officer was erroneous as the officers were authorised under section 7 of the EACCMA. In the premises the respondent's counsel submitted that ground 1 of the appeal is misconceived and ought to fail.

The appellants in rejoinder submitted that Section 28 of the Computer Misuse Act is clear and unambiguous that seizures, searches, extractions and samples taken and copies of data taken can only be done only by virtue of a search warrant. Further that it is not in dispute that the respondent had no search warrant to conduct the search and seizure of the computer systems as required by the law.

The appellants submitted that Section 7 of the East African Community Customs Management Act can only be invoked the Act and not under the Computer Misuse Act (the CMA). The Appellants reiterated earlier submissions and further submitted that **Section 158 (1) of the EACCMA** also requires a URA officer to obtain a search warrant to conduct searches. The appellants further reiterated earlier submissions on **Section 28 (9)** of the CMA. The appellants further relied on **Van der Merwe Et Al Information and Communication Technology Law 85**, for the proposition that a traditional requirement for proving the integrity of evidence is the chain of custody and that;

> "the prosecution needs to convince the court that the evidence was not interfered with from the time it was seized to the presentation in court. It is therefore critical that forensic investigations should ensure that digital evidence remains secure throughout the analysis."

Further, section 9 of the Computer Misuse Act which deals with preservation orders pending investigations, section 10 of the Computer Misuse Act which allows application for disclosure of preserved orders and section 11 of the Computer Misuse Act which allows orders of production of data stored in a computer system and to give access to the system, were not complied with by the respondent. For precedents on Article 27 of the Constitution of Uganda (See **Hon. Sam Kuteesa & Anor vs. AG (Constitutional reference No. 54 of 2011) [2012] UG SC 2)** The appellants prayed that the court treats sections **Section 7 EACCMA and Section 6 CPA** as void to the extent of inconsistency with the constitution and the CMA.

Further the appellants submitted in rejoinder that A1, A2 and A3 were licenced clearing agents and were at URA premises legally. Secondly that that the respondents claimed to have discovered this in January, 2011 and the arrests were in June, 2012 and therefore the respondents had ample time to obtain a search warrant and lastly that with the evidence of forensics that data cannot be erased permanent, there should be no notion that the accused/ appellants would change anything. The appellants reiterated submissions on **McDonald V. United States, 335 U.S. 451 69 S. ct.191, 93 L.E.D 153(1948)** for the proposition that evidence obtained illegally was inadmissible.

The appellants further reiterated submissions that there were serious fabrications and alterations in **Exp. 3, Exp. 23** and **Exp. 38** to implicate the appellants and this submission was not challenged by the respondents in their submission.

Ground 2

The learned trial judge erred in law and fact when he convicted the appellants without the prosecution disclosing the Encase software forensic tool used and mirror images analyses to the defence, as required by the law thus occasioning a miscarriage of justice.

The appellants submitted that the prosecution failed to discharge its legal obligation to disclose to the defence the prosecution's chosen Encase software forensic tool and mirror images. PW1 did not testify that he created a forensic copy using Encase, which copy was never tendered in evidence or disclosed to the defence nor does this form part of the summary of the case. They submitted that PW10 testified that he imaged the disks using Encase software tool meaning all those images were in Encase format. That PW 17 testified that she was called on the 25th July, 2012 to the tax investigation department to view forensic images of the two laptops and the one external disk.

They further submitted that PW20 testified that he analysed from images made by the Encase software tool. PW1, PW10, PW17 and PW20 made their analysis and produced various reports from the said mirror images, a creature of PW10. To that effect, Exp.1, Exp. 2, Exp.24, Exp.25, Exp.26, Exp.35, Exp. 36, Exp. 37 and Exp.38 were tendered in evidence. The mirror images were never tendered in evidence or disclosed and the appellants never got a chance to analyse these said mirror images. This defeated the ends of justice as the appellants were in custody through the entire trial and could not access these tools for their defence. The prosecution never availed the Encase software tool and mirror images to the defence which cast doubt on the scientific validity of the electronic evidence. The Appellants relied on **State vs. Dingman, 202 p. 39 388(WAH.CT.APP.2009) quoting State vs. Boyd, 160 WASH. 2d at 433-34, 158 p.3d 54(2007), The** justices of appeal reached a decision that; *"in sum, we conclude that the trial; court erred by the requiring that the state provide only an Encase*

mirror image of Dingman's hard drives to the defense. The remedy is to reverse and remand for a new trial". In the instant case the defense never had any opportunity to access Encase software tool and to analyse the mirror images to prepare for their defence which was a grave error to the prejudice of the defence case.

The prosecution also relied on **Thomas Patrick Gilbert Cholmondeley Vs. Republic Criminal Appeal No. 116 Of 2007,** the justices of the Kenyan court of appeal cited the decision in **R vs. Ward [1993] 2 All ER 557** for the holding that;

> "The prosecution's duty at common law to disclose to the defence all relevant material, i.e. evidence which tended either to weaken the prosecution case or to strengthen the defence, required the police to disclose to the prosecution all witness statements and the prosecution to supply copies of such witness statements to the defence or to allow them to inspect the statements and make copies unless there were good reasons for not doing so. Furthermore, the prosecution was under a duty, which continued during the pre-trial period and throughout the trial to disclose to the defence all relevant scientific material, whether it strengthened or weakened the prosecution case or assisted the defence case and whether or not the defence made a specific request for disclosure. Pursuant to that duty the prosecution was required to make available the records of all relevant experiments and tests carried out by expert witnesses".

The petitioners submitted that despite the gravity of the charge against Ward, the Court of appeal in England still allowed her appeal, quashed the various convictions against her and set her free. They submitted that failure by prosecution to disclose the Encase software and mirror images disabled the ability of the defence to make answer and defence and this rendered the trial null and void. That this material irregularity violated the appellants right to a fair hearing under Article 28 of the constitution of Uganda and which right is non derogable occasioning a miscarriage of justice. They prayed for court to allow this ground and quash the conviction of the appellants.

In reply to ground 2 the respondent's counsel submitted that the computers were recovered from the suspects upon arrest and the extraction of the hard disks from the computer was done in the presence of the appellants who witnessed the same in a forensics lab. Further the reports extracted from the exhibits (computers) was disclosed to the defence before hearing of the witnesses and relied **Soon Yeon Kong & Anor Vs. AG Constitutional Reference No. 6 of 2007** for the proposition that the prosecution complied with the law and disclosed all the evidence to the defence as required. Further the demand of the appellants for the forensic tools would be superfluous in the circumstances as they had already been given all the necessary reports and evidence extracted in their presence. Whatever documents were not disclosed to the defence were objected to and not received in evidence. The respondent submitted that in the premises ground 2 of the appeal is misconceived and ought to fail and / or to be answered in the negative.

The appellants submit in rejoinder that the reports generated from a scientific process by the help of the encase software tool producing mirror images which were analysed solely by the respondent and the appellants not being given a chance to find out how this evidence made its way to the alleged hard disks. This denied the appellants an opportunity to challenge the evidence adduced and make a full answer (See **R vs. Ward [1993] 2 All ER 557** to support the argument that providing a copy of the image and encase tool would have enabled the appellant to get an expert and this would have revealed how the evidence made its way to the computer. Failure to do this occasioned a miscarriage of justice). The appellants submitted that failure to disclose the mirror images and encase forensic software tools rendered the trial a nullity and void. The appellants pray that this court rejects the respondent's response because it lacks legal support. Further ordering a retrial would occasion a miscarriage of justice since the appellants have served part of their 15 months' sentence.

Grounds 3 and 5

The appellants argued grounds 3 and 5 jointly and submitted that on counts 1,3, 4 and 5 the learned trial judge misdirected himself in evaluating evidence as a whole on record and ignored the major inconsistences, contradictions, and fabrications in the prosecution evidence.

The appellants factored out **Exp. 8 (Samsung laptop), Exp. 9 (Lenovo laptop), Exp. 10 (external hard disk) and Exp. 39 (Dell laptop).**

These computers were allegedly recovered from the appellants who have demonstrated in **ground 1** that they were unlawfully seized. Further, the evidence of PW6 and PW26 demonstrate that these items were seized without a search warrant as earlier submitted. Further the computers were not returned within 72 hours as required by the law.

The appellants submitted that the evidence of PW 6 is that he had custody of EXP.8, EXP.9, EXP.10 and he was instructed by Nakyagaba (PW 26) to hand them over to PW 10 who allegedly took custody and returned them on the 30th June, 2012. PW6 testified that he was not present when PW 10 was opening the laptop and removing the hard disks. According to the appellants PW 6 lost sight of the exhibits and this raised a question as to whether the exhibited hard disks are actual hard disks that were inside the alleged laptops. Further, PW6 testified that he could not confirm that the hard disks that he tendered in court were removed from any of the respective laptops. Further Exp. 4 clearly reflect that none of the hard disks were recorded from the 1st appellant. He testified that he did not know what happens or what happened in the lab and strongly objected to the admissibility of the hard disks. In the premises, the appellants contend that the learned trial judge misdirected himself on the movement of these exhibits in his judgment. That whereas the trial judge listed these items as received from PW10 to PW6 there is nowhere in the testimony of PW6 that the exhibits were extracted in his presence nor did he admit that he gave both the laptop and the hard disks to PW10. They submitted that PW10 could not have analysed the mirror images on 27/07/2012 before he had acquired them on 28/07/2012. PW10's evidence that he took the Samsung hard disk to south Africa for removal of password and imaging was without a warrant or order of court as required by law. Further, the appellants submitted that the prosecution

did not bring the south African witness who acquired the images and the judge simply relied on the evidence of PW10 and convicted on evidence that was extracted without the perquisite search warrant.

The appellants argued that since URA had formatted the computers which were not produced in court, there is no way the court can ascertain that there was unauthorised access to the URA computer systems. Because of the inconsistences in the evidence adduced by PW10, PW17 and PW20 and no forensic report was done on all URA computers and none was tendered in evidence the learned trial judge ought not to have relied on the evidence.

Further, the appellants submitted that the learned trial judge misdirected himself on the evidence on record to that it was the 1st appellant who gave the cards to PW8 and pinpointed out the evidence of PW4 and isolated PW8, PW3, PW5's testimony and did not properly evaluate the evidence on record. The appellants submitted that there were inconsistences in the testimonies of PW3, PW 5, PW 8, PW4, PW10 and PW17 and had the trial judge considered all evidence and not just the cross examination testimonies, he would have noticed the inconstancies and arrived at a different conclusion. He would have found that the witnesses of the prosecution were telling lies and had fabricated evidence to achieve their goal of circumstantial evidence that was adduced by PW1, PW10, PW17, PW18 and PW20 to incriminate the appellants. The appellants relied on **Twehangane Alfred vs. Uganda Criminal Appeal No. 139 of 2001** for the proposition that inconsistencies lead to rejection of evidence and prayed that the court allows the appeal on this ground and acquits the appellants.

The respondents counsel submitted that the court established a prima facie case against the appellants and the trial judge proceeded to explain the options available to the appellants who opted to keep quiet and the only evidence that was available for analysis was that of the prosecutions' twenty-six witnesses.

Further the evidence presented by PW1 was obtained before the arrest of the appellants and was submitted as independent evidence. That the piece of evidence that linked the appellants to the commission of the

offences was provided by PW10. The other evidence that linked the appellants was the evidence of PW4, PW12, PW13, PW18 in addition to circumstantial evidence that was adduced that implicated the appellants like the arrest of the 1st appellant with others near URA and the recovery of hacking implements, purchase of spy hardware, presence of the email chats between the appellants in the audit logs recovered in the URA servers among other things.

The respondent relied on **Simoni Musoke vs. R [1958] E. A 715 and Bogere Charles Vs. Uganda, SCCA NO. 10 of 1998** for the proposition that conviction can be based on circumstantial evidence. In the premises, the respondent's counsel submitted that the trial judge rightly and effectively evaluated evidence and rightly convicted the appellants.

In rejoinder, the appellants submitted that the burden of proof does not shift throughout the trial even on appeal. Further the email bmugishaura@gmail.com which was used to incriminate the appellants was never owned by the appellants and were mere allegations that lacked evidence. Further emails address rbyamukama@gmail.com and guxzguster@gmail.com were also contested through Exp. 3 that the appellants contend was a fabricated document obtained in unconventional form by PW1 who claimed to have hacked the same and nowhere do the appellants admit that they owned the emails.

With reference to the respondent's submissions on PW 10's testimony and especially the contents of the reports Exp. 24, 25 and 26 the appellants submitted that these reports are full of falsehoods and fabrications and were obtained in unconventional form to that extent, they are inadmissible.

The appellants further contest the testimony of PW17, PW4 and PW3 as being untruthful and witnesses having been coached. The pray that the court to be pleased to reject the response of the respondent on ground one and allow grounds 3 and 5.

Ground 4

The learned trial judge erred in law when he commenced the trial and convicted the appellants without the assessors taking oath contrary to the provisions of the law, thereby occasioning a miscarriage of justice.

The appellants submitted that the learned trial judge tried and convicted the appellants without the assessors taking the oath of impartiality before taking on their role in breach of **Section 67 of the Trial On Indictment Act**. They submitted that the legislature intended the taking of oath by assessors to be a mandatory prerequisite in the trial process. Further **Section 3** of the **TIA** requires the number to be 2 or more and that the participation of assessors is vital and mandatory and failure to comply goes to the legality of the trial which cannot be cured by Section 139 if the TIA. The appellants relied on **Alenyo Marks vs. Uganda SCCA NO. 08 of 2007** for the proposition that a trial which proceeds without assessors taking oath is a nullity (See also **Abdu Komakech vs. Uganda SCCA. NO. 1 of 1988).** Similarly, the appellants submitted that another illegality was that one assessor concluded the trial and had not taken oath. They pray that the court acquits the appellants and quashes their conviction and sentence.

In reply to ground 4 the respondent's counsel submitted that there was no miscarriage of justice occasioned on the appellants as the two assessors were present throughout the entire trial. At a closer perusal of the record shows that on the 19/12/2012 that both assessors were present and a summing up by the trial judge was done. Further it would appear that the record was not put in a proper manner and be that as it may, there was no miscarriage of justice occasioned on the appellants by reason that the advice opined by the assessor was based on full attendance of the hearing of the case (See **Sitende Sebalu vs. Sam K. Njuba and the Electoral Commission SC Election Appeal No. 26 of 2007.)**

Further, counsel submitted that **Section 67 TIA** given the circumstances of this case has to be construed as directory and not mandatory. The respondent's counsel further relied on **Article 126 (2)(e) of the Constitution** and submitted that justice should be administered without undue regard to technicalities. In the premises, counsel contended that failure by the assessors to take oath or failure to record that the assessor took oath did not affect the rights of the appellants. From the

time of arraignment, the appellants pleaded not guilty, they were fully represented and their lawyers extensively cross examined the prosecution witness and, in the end, based on evidence, the assessor advised the trial judge to acquit some of the accused persons which the judge did based on reason and evidence adduced during trial. In the premises, counsel prayed that ground 4 should be dismissed.

In rejoinder the appellants submitted that it is an illegality for assessors to operate without taking oath as required by law and reiterated earlier submissions.

Ground 6

The learned trial judge erred in law and in fact when he convicted and sentence the appellants twice for the same offence.

The appellants argue that being charged on counts 1-4 of the CMA and count 5 from the EACCMA, 2004 was double jeopardy. They contend that court imposed more than one punishment for the same offence contrary to Article **28 (9) of the constitution of the Republic** of Uganda. They cited to the case of **State vs. Reiff, 14 wash 664, 667,45 P.38 (1896)** for the "same evidence test "at 667 (quoting **Morey vs. Common Wealth, 108 MASS, 433 434 (1874)**. The appellants submitted that the ingredients of the offences they were charged under the Computer Misuse Act when read together with Section 3 leads to the conclusion that the offences are inseparable and intertwined. They submit that unauthorised use or interception contrary to section 15(1), Unauthorised access to data contrary to section 12(2), unauthorised access to customs computerised system contrary to section to 191(1)(a), unauthorised access contrary to section 12(3) and electronic fraud contrary to section 19 are all directed at the same act or conduct and only differ in their result by the conduct. When unauthorized access leads to a conviction in all offences, the offences are the same in the circumstances. They submitted that the judge erred when he convicted and sentenced the appellants to the same offences contained in counts 5, 1, 3, 4, and 2 and this exposed the appellants to double jeopardy in violation to Article 28(9) of the constitution. The appellants rely on **State Vs. Potter,31 WASH APP.883, 887-88, 645 P 2D 60(1982) and**

Criminal Appeal No. 037 of 2017, Patrick Sentongo vs. Uganda for this submission.

The appellants pray that the court allows this ground, quashes the conviction in count 5 and vacates the sentence therein.

In reply, the respondent's counsel submitted that the appellants argued that they were charged, convicted and sentenced under the CMA and the EACCMA for the same offence. The respondent's submission is that this is lawful under Section 23 of the TIA Cap. 23.

Further all the necessary evidence to sustain all the charges was presented and evaluated by the trial judge, who convicted and sentenced the appellants and where the evidence was not sufficient the judge acquitted A2 and A3.

In the premises counsel for the respondent contends that the argument of the appellants on ground 6 is spurious, misplaced and ought to be rejected by this court and the ground dismissed.

In rejoinder the appellants submitted that the trial judge in convicting the appellants on counts 1 and 5 erred in principle and the learned trial judge in giving a consecutive sentence of a fine of US$ 4500 erred in law. The appellants reiterated earlier submission on ground 6.

Ground 7

The learned trial judge erred in law and in fact in ignoring and allowing the illegal conduct of the Uganda Revenue Authority to prosecute, investigate the appellants made foreign to the known legal modes of commencing prosecution thereby occasioning a miscarriage of justice.

The appellants submitted that there are three main requirements of natural justice which ought to be met in every case. These are adequate notice, fair hearing and no bias and that these are enshrined in Article 28 of the constitution. In the instant case URA made the arrests, investigations and prosecuted the matter. They contend that this was illegal, unconstitutional and violated the right to a fair hearing of the appellants.

The appellants submitted that there was no fair trial accorded to the appellants and pray that court rejects the evidence and witnesses on grounds of fairness.

They also relied on **Section 7** of the **East African Community Customs Management Act** and submitted that that the powers thereunder can only be exercised under the EACCMA and not the CMA and such powers cannot in any way override the constitution and the laws of Uganda.

They reiterated submissions that URA officers are not police officers under section 28 of the CMA. Further they contravened constitutional provisions including Article 120(5) and Article 120(4)(a) of the Constitution that empowers the DPP to authorise any person to act on his behalf in accordance with "general or specific instruction" but does not cover investigations as done in the appellants' case. In **R vs. Horseferry Road Magistrates Ex parte Bennet (1994) 1 A.C. 42** where the lords stated: "

> The judiciary accept a responsibility for the maintenance of the rule of law that embraces a willingness to oversee executive action and to refuse to countenance behaviour that threatens either basic human rights or the rule of law. (authorities in the field of administrative law contend) that it is the function of the High Court to ensure that executive action is exercised responsibly and as Parliament intended. So also should it be in the field of criminal law and if it comes to the attention of the court that there has been a serious abuse of power it should, in my view, express its disapproval by refusing to act upon it. ... The courts, of course, have no power to apply direct discipline to the police or the prosecuting authorities, but they can refuse to allow them to take advantage of abuse of power by regarding their behaviour as an abuse of process and thus preventing a prosecution".

The appellants contend that it was erroneous for the learned trial judge to hold in his judgement that "the signature of the person authorised to sign for the DPP suffices and there should be nothing amiss". That the learned trial judge erred in allowing the illegal conduct of URA and occasioned a miscarriage.

In reply, the respondent's counsel submitted that the prosecutor Mary Kamuli Kuteesa was at all times licensed to prosecute the appellants by the Director of Public Prosecutions. The DPP has authority to delegate to

an officer power to act on his or her behalf except in matters where the law expressly requires the consent of the DPP. The appellants' argument that URA acted illegally is misconceived and ought to be rejected and this ground ought to fail.

In rejoinder, the appellants submitted that the argument is about URA being legally authorised to prosecute, investigate the appellants and the same time be the complainant but there was no challenge to the powers of the DPP. The respondent failed to provide to court the scope of their authority and/ or instructions which the appellants cannot force them to do. The burden squarely lay on them which burden was not discharged. That secondly that URA is not a gazetted investigator and they were the ones in charge of the investigations including the forensic analysis making them partisan in the case and this defeated the ends of justice.

Ground 8

The learned trial judge erred in law and in fact when he convicted the appellants passed excessively harsh sentence against the appellants on count 2 and count 5.

The appellants argued that 12 years' imprisonment on count 2 and a fine of US$4500 imposed on count 5 are manifestly harsh. While sentencing is at the discretion of the trial court, it must be exercised judiciously and not capriciously. The seriousness of the offense was mitigated by facts the appellants presented in their mitigation statements. Appellants invited the court to consider its decision in **Nisiima vs. Uganda, CACA NO. 8 OF 2010**, where it was held that courts should take into account past precedents of court on sentencing. (See cases of **Adam Jino vs. Uganda (2010) CACA NO. 50 OF 2006, Kenneth Kaawe vs. Uganda CA No. 103 of 2011, Rwabugande Moses vs. Uganda CA NO. 25 of 2014 and section 15(b) of the Constitution (Sentencing Guidelines for Courts of Judicature) (Practice) Directions, 2013).**

The appellants invited court to consider the principle of consistency in sentences for similar offence as held in **Livingstone Kakooza vs. Uganda, SCCA NO. 17 of 1993** and in **Serunkuma Edrisa & 5 others CA. NO. 147 of 2015** and **Aharikunda Yustiina vs. Uganda SCCA NO. 27 of 2015**.

The appellants prayed that this court exercises its discretion and reduces the sentence in count 2 and to a sentence of 7 years' imprisonment as appropriate. Further on count 2 the sentence ought to be reduced to enable the appellants reform and be reintegrate in society.

The appellants pray that the appeal is allowed and the conviction and sentence be set aside or in the alternative the sentences in count 2 and 5 be reduced in the interest of justice.

In reply, the respondent's counsel submitted that the sentences passed are valid sentences and the learned trial judge considered the aggravating and mitigating factors. The trial judge was alive to the fact that the appellants had spent one year on remand and deducted the period spent on remand. The sentence was with the intention to reform the appellants. The learned trial judge also considered the fact that the appellants were relatively young and they had young families and were remorseful. The judge also considered the tremendous loss to the exchequer of URA and compromised security systems of the country and the judge was right to reach the conclusion he did.

In the premises, counsel prayed that this ground ought to fail and the appeal be dismissed and orders of the trial court be upheld.

In rejoinder, the appellants reiterated their earlier submission and added that they appealed against the sentence for only counts 2 and 5.

They further submitted that section 19 of the MCA (count 2) does not fall under those penalties prescribed in Section 20. The respondent's submission that count 2 carries a maximum sentence of life imprisonment is misconceived. Section 19 of the CMA (on count 2) carries a maximum of 15 years' imprisonment.

The appellants further contend that the trial judge was manifestly harsh on count 2 and count 5 when he did not consider the mitigating factors. That the sentences handed down in counts 2 and 5 were not reformatory and that this court be pleased to reduce the sentences on the 2 counts.

Resolution of Appeal

This is a first appeal from the decision of the High Court in the exercise of its original jurisdiction and we are to reappraise the evidence on the printed record of appeal by subjecting it to fresh scrutiny and arriving at its own independent inferences of fact. A first appellate court should be cautious of the fact that it did not have the opportunity or advantage of hearing the witnesses testify and to treat with deference the observations of the trial judge on matters of credibility of witnesses where it is in controversy (See **Pandya v R [1957] EA 336, Selle and Another v Associated Motor Boat Company [1968] EA 123,** on the duty of a first appellate court by the East African Court of Appeal and the decision of the Supreme Court of Uganda in **Kifamunte Henry v Uganda; SCCA No. 10 of 1997**). The duty of court to reappraise the evidence is enable by rule 30(1)(a) of the **Judicature (Court of Appeal Rules) Directions, S.I No. 13-10**, which provides that on appeal from the decision of the High Court in the exercise of its original jurisdiction, the court may reappraise the evidence and draw inferences of fact.

Grounds 1 of the appeal challenges the admission of evidence obtained from computers, flash discs and hard drives seized and searched by the officials of URA without due process provided for under section 28 of the Computer Misuse Act, 2011 as well as article 27 of the Constitution. The evidence formed the core of the prosecution case and is pivotal in consideration of this appeal and therefore ought to be considered first. If this ground succeeds, issues relating to evaluation of evidence would be affected and considered according to the outcome of the case.

Ground 1 of the appeal arises from the decision of the learned trial judge when the appellants objected to admission of computer generated evidence for non-compliance with section 28 of the Computer Misuse Act, in so far as the computers which was used to obtain information used in the prosecution was seized and searched without a search warrant. The learned trial judge considered article 27 of the Constitution which guarantees the right to privacy and whether such derogation to the right of privacy by seizing the computer without a search warrant,

was justifiable under article 43 of the Constitution which provides that the fundamental rights and freedoms of the individual should not be exercised to the prejudice of the public interest or the fundamental or other human rights and freedoms of others. He found that it was necessary to balance these interests particularly in light of section 6 (2) of the Criminal Procedure Code Act which provides that a public officer may search any person who has been arrested and may take possession of anything found on the person which might reasonably be used as evidence in any criminal proceedings. Further, the learned trial judge was persuaded by judicial precedents from USA which consider the balancing of the public interest and the fundamental and other freedoms of the individual Vis-à-vis the right to privacy (**See GM. Leasing Corp Vs United States, 429 U.S. 338. 352 - 53, 355; McDonald Vs United States, 335 U.S. 451, 456 (1958)**) for the provision that exceptions to the requirement for search warrants are generously and carefully drawn and that those who seek exception to the requirement should show that the exigencies of the situation make the course imperative). Further that a search without a warrant was not unconstitutional when probable cause exists and the government satisfies its burden of demonstrating that the circumstances of the situation made it imperative. He found that if section 28 (3) of the Computer Misuse Act is applied to the letter, it would have a chilling effect on the enforcement of the law literally making law enforcement agencies powerless in certain situations. He found that certain exceptions must be made where evidence shows the exigencies of the situation could not await a search warrant. Lastly the learned trial judge held that:

> "given the evidence of PW2, PW3 PW6 and PW26 the prevailing circumstances were such that instant response had to be given to a situation that had presented itself. They did not act unreasonably in the circumstances and as such I hold the search and subsequent seizure done on the occasion of the arrest of A1, A2 and A3 to be lawful."

From the holding, the learned trial judge admitted certain laptop computers and the external hard drives and hard disks whose stored information had been used in investigation and evidence. Further these laptops and hard discs had been subjected to computer forensic analysis after the seizure and the evidence was used in the prosecution.

Section 28 of the Computer Misuse Act 2011 deals with searches and seizure. It provides under section 28 (3) that:

> "A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant."

It is not in dispute that computers and hard drives which were used as evidence against the appellants were seized without a search warrant.

One basic rule of interpretation of statutes is that every statute has to be read on the basis of its own language before dealing with any other issue (See **Lall v Jaypee Investments Ltd [1972] E.A. 512** at page 516 where the East African Court of Appeal cited with approval the holding in **Attorney General Vs Prince Ernest Augustus of Hanover, [1957] AC 436** for the proposition that; "each statute has to be interpreted on the basis of its own language as words derive their colour and content from their context; and secondly, the object of legislature is of paramount importance..."). It is therefore necessary to first examine the wording of the Computer Misuse Act on the subject of "search and seizure" and the object of legislature in its enactment.

Section 28 of the Computer Misuse Act 2011 provides that:

> 28. Searches and seizure.
>
> (1) Where a Magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing—
>
> (a) that an offence under this Act has been or is about to be committed in any premises; and
>
> (b) that evidence that such an offence has been or is about to be committed is in those premises, the Magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary.
>
> (2) An authorised officer may seize any computer system or take any samples or copies of applications or data—
>
> (a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within Uganda or elsewhere;

(b) that may afford evidence of the commission or suspected commission of an offence, whether within Uganda or elsewhere; or

(c) that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

(3) A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant.

(4) The provisions of section 71 of the Magistrates Court's Act apply with the necessary modifications to the issue and execution of a search warrant referred to in subsection (3).

(5) An authorised officer executing a search warrant referred to in subsection (3), may—

(a) at any time search for, have access to and inspect and check the operation of any computer system, application or data if that officer on reasonable grounds believes it to be necessary to facilitate the execution of that search warrant;

(b) require a person having charge of or being otherwise concerned with the operation, custody or care of a computer system, application or data to provide him or her with the reasonable assistance that may be required to facilitate the execution of that search warrant; and

(c) compel a service provider, within its existing technical capability—

(i) to collect or record through the application of technical means; or

(ii) to co-operate and assist the competent authorities in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system.

(6) In seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in subsection (5), an authorised officer shall have due regard to the rights and interests of a person affected by the seizure to carry on his or her normal activities.

(7) A person who obstructs, hinders or threatens an authorised officer in the performance of his or her duties or the exercise of his or her powers under this section commits an offence and is liable on conviction to a fine not exceeding twelve currency points or imprisonment not exceeding six months or both.

(8) A computer system seized or samples or copies of applications or data taken by the authorised officer shall be returned within seventy-two hours

unless the authorised officer has applied for and obtained an order in an inter party application for extension of the time.

(9) In this section—

"authorised officer" means a police officer who has obtained an authorising warrant under subsection (1); and

"premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hover craft.

The following highlights should be set out for purposes of analysis of section 28 of the Computer Misuse Act. The first is that it is a magistrate who is supposed to be satisfied by information given by a police officer before issuing a warrant of search and seizure. The information expected is to the effect that an offence under the Computer Misuse Act, is or is about to be committed in any premises. Alternatively, that such an offence has been or is about to be committed in the premises. It is upon the magistrate to issue a warrant authorising a police officer to enter and search the premises, using reasonable force. Further, an authorised officer who is armed with a search warrant, may seize and take any computer system or take any samples or copies of applications or data on the grounds indicated. Particularly section 28 (3) provides that the seizure of computers or samples of copies of application or data may be taken only by virtue of a search warrant. Further, section 71 of the Magistrates Courts Act cap 16 is supposed to be applied with the necessary modification in that it provides that:

> "Every search warrant may be issued and executed on Sunday, and shall be executed between the hours of sunrise and sunset; but the court may, by warrant, in its discretion, authorise the police officer or other person to whom it is addressed to execute it at any hour".

Section 28 (5) of the Computer Misuse Act deals with the inspection and access to the data. Last but not least, where computer systems seized or samples or copies of application or data have been seized or taken, it is supposed to be returned within 72 hours unless the court extends the time in an interparty application. Specifically, the word "authorised officer" means a police officer who has obtained an authorising warrant. It is further necessary to note that under section 28 (9), the word

"premises" includes vehicles, vessels, aircraft and hovercraft as well as movable structures, buildings and land.

The learned trial judge considered the right to privacy enshrined under article 27 of the Constitution of the Republic of Uganda in relation to the right to seize under section 28 of the Computer Misuse Act and found that a balance between the right of privacy and the right of the public interest and fundamental and other human rights of other people was necessary to cater for situations where the warrant could not be obtained in time to carry out the seizure. Article 27 of the Constitution provides that:

> 27. Right privacy of person, home and other property.
> (1) No person shall be subjected to –
> (a) unlawful search of the person, home or other property of that person; or
> (b) unlawful entry by others of the premises of that person.
> (2) no person shall be subjected to interference with the privacy of that person's phone, correspondence, communication or other property.

Clearly there is a tension between the right of privacy and the right of the state and of state agencies to arrest any person who is about to commit an offence or who is committing an offence in terms of the right of seizure contained in section 28 of the Computer Misuse Act. The learned trial judge relied on article 43 of the Constitution to find that the seizure without a warrant was in the circumstances justified. Article 43 of the Constitution provides that:

> 43. General limitation on fundamental and other human rights and freedoms.
>
> (1) In the enjoyment of the rights and freedoms prescribed in this Chapter, no person shall prejudice the fundamental or other human rights and freedoms of others or the public interest.
>
> (2) Public interest under this article shall not permit—
>
> (a) political persecution;
>
> (b) detention without trial;
>
> (c) any limitation of the enjoyment of the rights and freedoms prescribed by this Chapter beyond what is acceptable and demonstrably justifiable in a free and democratic society, or what is provided in this Constitution.

We have carefully considered the decision of the trial judge on whether it was lawful to admit the seized computer evidence pursuant to seizure

of the computers and hard drives and discs of the appellants without a search warrant as stipulated by section 28 of the Computer Misuse Act. The first point to be made is that the decision did not rest on the express provisions of section 28 of Computer Misuse Act which gives the procedure to be followed which prescribes that a search cannot be conducted unless it is conducted by police officer who is authorised by search warrant. The Computer Misuse Act does not purport to be an Act to protect the privacy of anybody. The preamble to the Act provides that it is an act to make provision for the;

> "safety and security of electronic transactions on Information Systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters."

It can be discerned from the decision of the learned trial judge that he considered section 28 of the Computer Misuse Act to provide for or enforce the right to privacy as proceeding under article 27 of the Constitution. It followed that he considered article 43 of the Constitution as justifying a search without a warrant on the basis of justifiable derogation from compliance with article 27 of the Constitution to the letter. Nevertheless, the preamble to the Computer Misuse Act is clear that it is to provide for the safety and security of electronic transactions and Information Systems to prevent unlawful access, abuse and misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters. It not only provides for the right of privacy but also security of electronic transactions and Information Systems and prevention of unlawful access and abuse and misuse of Information Systems. The objectives of the Computer Misuse Act are wider than those found under article 27 of the Constitution in that it does not only enable protection of the freedom from interference of home, property and communication but has other objectives. The computer Misuse Act 2011 is a relatively new Act in Uganda and has not been the subject of much jurisprudence particularly on the question of admissibility of evidence where such evidence is obtained unlawfully. It was erroneous and undesirable to link section 28

of the Computer Misuse Act with article 27 of the Constitution without considering the context in which its laws enforce and perhaps, as we will determine, ensure compliance with article 27 of the Constitution.

Secondly we have considered the reference to section 6 of the Criminal Procedure Code Act which provides for search of a person arrested and stipulates that:

> 6. Search of person arrested.
>
> (1) Whenever a person is arrested—
>
> (a) by a police officer under a warrant which does not provide for the taking of bail, or under a warrant which provides for the taking of bail but the person arrested cannot furnish bail; or
>
> (b) without warrant, or by a private person under a warrant, and the person arrested cannot legally be admitted to bail or is unable to furnish bail, the police officer making the arrest or, when the arrest is made by a private person, the police officer to whom he or she makes over the person arrested, may search that person and place in safe custody all articles, other than necessary wearing apparel, found upon him or her.
>
> (2) Notwithstanding subsection (1), a police officer may search any person who has been arrested and may take possession of anything found on the person which might reasonably be used as evidence in any criminal proceedings.

We have carefully considered section 6 (1) of the Criminal Procedure Code Act cap 116. It provides only for the searching of a person who has been arrested with or without a warrant of arrest. The person arresting may search that person and place in safe custody, all articles, other than necessary wearing apparel, found upon him or her. Clearly section 6 (1) does not apply in the circumstances of this appeal. Secondly, the learned trial judge relied on section 6 (2) of the Criminal Procedure Code Act which provides *inter alia* that the police officer may search any person who has been arrested and may take possession of anything found when the person which might reasonably be used as evidence in any criminal proceedings. The expression "found on the person" seems to denote items found in possession of that person or on his or her body or around that person upon arrest. There is no need to explore the extent of the application of the words "found on the person". Clearly this does not

apply to items or objects found in a house where the person is arrested or in the premises as defined under the Computer Misuse Act. Notwithstanding, the items of computers and accessories could be seized in the circumstances and this does not per se amount to search of the computer or cell phones as demonstrated below. We find that seizure of an electronic gadget such as a computer or hard disc was not distinguished from search of the computer or hard disc in the judgment in the admissibility of electronically generated evidence. This is the crux of ground 1 of the appeal.

In **McDonald v. United States 335 U.S. 451, 69 S.Ct.191; 93 L.Ed. 153** the petitioners had been convicted by the District Court on evidence obtained by a search made without warrant. The decision was affirmed by the Court of Appeal and a petition for certiorari was brought seeking to nullify the order for inconsistency with an earlier decision in **Johnson v, United States, 333 U.S. 10, 68 Ct. 367**. Mr. Justice Douglas who delivered the judgment of court said that:

> We are not dealing with formalities. The presence of a search warrant serves a high function. Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done not to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted. And so the constitution requires a magistrate to pass on the desires of the police before they violate the privacy of the home. We cannot be true to the constitutional requirement and excuse the absence of a search warrant without showing by those who seek exemption from the constitutional mandate that the exigencies of the situation made the course imperative.

Mr. Justice Jackson stated that:

> Even if one were to conclude that urgent circumstances might justify a forced entry without a warrant, no such emergency was present in this case. The method of law enforcement displays a shocking lack of all sense of proportion. Whether there is a reasonable necessity for search without waiting to obtain a warrant certainly depends somewhat upon the gravity of the offence thought to be in progress as well as the hazards of the method of attempting to reach

> it. In this case the police had been over two months watching the defendant MacDonald. His criminal operation, while a shabby swindle that the police are quite right in suppressing, was not one which endangered life or limb or the peace and good order of the community even if it continued another day or two; neither was the racket one the defendant was likely to abandon. Conduct of the numbers racket is not a solitary vice, practised in secrecy and discoverable only by crushing into dwelling houses.

The court considered that it may be necessary in some instances of arrest and search to be conducted without a warrant. What are such grave circumstances? The decision was made on 13 December 1948 and may not be directly relevant to admissibility of electronic data because as far as Uganda is concerned, there is a specific statute that deals with the matter. Nonetheless, in general exceptions in the public interest may be considered. I have accordingly considered several other authorities on the question of search of premises without a warrant in more modern times when assessing admissibility of electronic data.

In **Kevin Fearon Vs Her Majesty the Queen [2014] 3 S.C.R.621** two men armed with handguns robbed a merchant and were arrested by the police. The police found a cell phone in one of the pockets of the alleged robbers. The police searched the phone at the time and again within less than two hours of arrest. They found a draft text message which read inter alia: *"we did it where the jewellery at nigga..."* and some photos including of a hand gun. About 36 hours later, the police had a search warrant to search the vehicle and recovered the handguns used in the robbery which was depicted in the photo. Once later, police applied for and were granted a warrant to search the contents of the phone but no new evidence was discovered. The learned trial judge found that the search of the cell phone incidental to the rest had not breached section 8 of the Charter which guaranteed the right to privacy. She admitted the photos and text message and convicted the appellant of robbery. The Court of Appeal dismissed an appeal by the appellant and on further appeal to the Supreme Court, the issue considered was whether the police have a common law power to search incidental to lawful arrest. Secondly, whether this power permits the search of cell phones and similar devices found on the suspect. The Supreme Court held that to resolve the issue, a balance must be stricken between the demands of

effective law enforcement and everyone's right to be free of unreasonable searches and seizures. The court must identify the point at which the "public interest" would give way to the government's interest in intruding on an individual's privacy to advance its goals of law enforcement. They found that to achieve the balance, can be done with a rule of law which permits search of cell phones incident to arrest, provided the search of both what is searched and how it is searched is strictly incidental to the arrest and the police keep detailed notes of what has been searched and why. the Judgment of McLachlin C.J and Cromwell, Moldaver and Wagner JJ were read by Cromwell J who held inter alia that:

> [51} it is well settled that the search of cell phones, like the search of computers, implicates important privacy interest which are different in both nature and extent from the search of other "places"... It is unrealistic to equate a cell phone with a briefcase or document found in someone's possession at the time of arrest.... And I would add cell phones – may have immense storage capacity, may generate information about intimate details of the user's interests, habits and identity without the knowledge or intent of the user, may retain information even after the user thinks that it has been destroyed, and may provide access to information that is in no meaningful sense "at" the location of the search.
>
> ... [55] in this respect, a cell phone search is completely different from the seizure of boarding samples in the *Steel man* and the strip search in *Golden*. Such searches are invariably and inherently very great invasions of privacy and, in addition, a significant affront to human dignity. That cannot be said of cell phone searches incidental to arrest.
>
> [56] Second, we should bear in mind that a person who has been lawfully arrested has a lower reasonable expectation of privacy than persons not under lawful arrest: ...
>
> [57] Third, the common law requirement that the search be really incidental to a lawful arrest imposes some meaningful limits on the scope of a cell phone search. The search must be linked to a valid law enforcement objective relating to the offence for which the suspect has been arrested. This requirement prevents routine browsing through a cell phone in an unfocused way.
>
> [58] All of that said, the search of a cell phone has the potential to be a much more significant invasion of privacy than the typical search incident to arrest. As a result, my view is that the general common law framework for searches

incident to arrest needs to be modified in the case of cell phone searches incident to arrest. In particular, the law needs to provide the suspect with further protection against the risk of wholesale invasion of privacy which may occur if the search of a cell phone is constrained only by the requirements that the arrest be lawful and that the search should be truly incidental to arrest and reasonably conducted. The case law suggests that there are three main approaches to making this sort of modification: a categorical prohibition, the introduction of a reasonable and probable grounds requirement, or a limitation of search to exigent circumstances...."

The court rejected the idea that section 8 of the Canadian Charter categorically precluded any search of a cell phone seized incidental to a lawful arrest and found that the question was what safeguards should be added to the law of search of cell phones incidental to arrest in order to make the power compliant with the right to privacy under section 8 of the Canadian charter.

Secondly on the ground of imposing a reasonable and probable grounds requirement the court found that investigations may lead to possible leads or dead ends and restrict cell phone search restrictions which the authors of reasonable and probable cause believe the evidence of the offence to be found in cell phone record for prompt access to what may be very important information which is required for the immediate purpose of the unfolding investigation. For instance, a prompt search of a cell phone may lead investigators to other perpetrators. They found that the standard of reasonable and probable grounds would or has the potential to unreasonable compromise the safety of the police, the accused or the public. It strikes an inappropriate balance between those important law-enforcement objectives of the accused privacy interests.

On the third ground of exigent circumstances, it may allow cell phone searches only in exigent circumstances. The approach gives almost no weight to law-enforcement objectives served by the ability to promptly search a cell phone incidental to the arrest. By imposing a requirement of urgency, this basis failed to strike a balance between privacy interests of the individual and the interests of the state in protecting the public. They found that the above rationales do not change anything in relation to search without a warrant in exigent circumstances.

The court found that the appropriate approach is to concentrate on measures to limit the potential invasion of privacy that may, but does not inevitably result from a cell phone search.

In other words, even if a computer is seized during the arrest, it can still be searched upon obtaining a warrant for that purpose. Search of a computer immediately after arrest or seizure may not be necessary. The court noted that:

> [76] First, the scope of the search must be tailored to the purpose for which it may lawfully be conducted. In other words, it is not enough that the cell phone search in general terms is truly incidental to the arrest. Both the nature and extent of the search performed with the cell phone must be truly incidental to the particular arrest for the particular offence. In practice, this will mean that, generally, even when a cell phone search is permitted because it is truly incidental to the arrest, only recently sent or drafted emails, texts, photos and the call log may be examined as in most cases only those sorts of items will have the necessary link to the purpose for which prompt examination of the device is permitted. But these rules are not rules, and other searches may in some circumstances be justified. The test is whether the nature and extent of the search are tailored to the purpose for which the search may lawfully be conducted. To paraphrase Caslake the police must be able to explain, within the permitted purposes, what they searched and why.

In **Thomas Reeves Vs Her Majesty the Queen [2018] 3 R.C.S 531** the police discovered child pornography on the home computer that the accused/appellant shared with his spouse and the police officer did not have a warrant. The question was whether the police obtained the child pornography evidence in a manner that infringed privacy rights under section 8 of the Canadian Charter of Rights and Freedoms. The trial judge excluded the evidence on the ground that it infringed the appellant's rights. The appellant was acquitted and on appeal, the decision was overturned and the evidence admitted and a retrial ordered. On further appeal the issue arising was whether the police infringed the appellant's charter rights by entering the home without a warrant and secondly by taking the shared computer without a warrant.

Section 8 of the Canadian Charter provides inter alia that "*everyone has the right to be secured against unreasonable search or seizure.*" The court found that the essence of searches under section 8 of the Charter

was the taking of an item from a person by a public authority without that person's consent. In contrast, a valid consent is a waiver of the claimant's rights. Where there was no consent, the duty of the court is to determine whether the search procedure was reasonable. It is presumed that a search procedure is unreasonable and the burden is on the state to rebut this presumption. The question raised in the matter was whether police infringed the appellant's Charter rights by entering the shared home without a warrant and taking the shared computer without a warrant. The Judgment of Wagner C.J. and Abella, Karakatsanis, Gascon, Brown, Rowe and Martin JJ were read by Karakatsanis J who found inter alia that the police detained the computer without a warrant for more than four months but did not search it during that time. They failed to report the seizure of the computer to a justice as required by the law. The police finally obtained a warrant to search the computer and executed it two days later. The learned trial judge in the application concluded that the police had violated section 8 Charter rights because of the search without a warrant for the home and seizure of the home computer. This was overturned on appeal. She held that:

> [30] Here, the subject matter of the seizure was the computer, and ultimately the data it contained about Reeves usage, including the files he accessed, saved and deleted. I acknowledge that the police would not actually search the data until they obtained a warrant... Nevertheless, while the privacy interests engaged by a seizure may be different from those engaged by a search, Reeves informational privacy interests in the computer data were still implicated by the seizure of the computer. When police seized a computer, they not only deprive individuals of control over intimate data in which they have a reasonable expectation of privacy, they also ensure that such data remains preserved and thus subject to potential future state inspection.
>
> ... [34] Personal computers contain highly private information. Indeed, computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities.... Computers act as portals – providing access to information stored in many different locations... They "contain information that is automatically generated, often unbeknownst to the users" ... They retain information that the user may think has been deleted... By seizing the computer, the police deprived Reeves of control over this highly private information, including the opportunity to delete it. They also obtained

the means through which to access this information. Indeed, these are the reasons why the police seized the computer.

> [35] Given the unique privacy concerns associated with computers, this court has held that specific, prior judicial authorisation is required to such a computer.... And that police officers cannot search cell phones incident to arrest unless certain conditions are met.... The unique and heightened privacy interest in personal computer data clearly warrant strong protection, such that specific, prior judicial authorisation is presumptively required to seize a personal computer from their home. This presumptive rule fosters respect for the underlying purpose of section 8 of the charter by encouraging the police to seek lawful authority, who accurately accord with the expectations of privacy Canadians attached to the use of personal computers and encourages more predictable policing.

The court found that no statutory or common law authority could have justified the computer search in the case because if it had been done with a warrant and they had a warrant to search the home, it would have justified this but not the search of the computer. Further in the course of the search by warrant, police can come across a group computer that may contain material for which they are authorised to seize but the warrant does not give them specific prior authorisation to search computers. They may seize the device but must obtain further authorisation before it is searched. She found no basis why they detained the computer for four months without respecting the reporting requirements under the law. The police must report a search without a warrant to a justice as soon as practicable.

In the circumstances of section 28 of the Computer Misuse Act, 2011, it is specifically provided that the computer system seized or copies of application or data taken by the authorised officer shall be returned within 72 hours unless the authorised officer has applied for and obtained an order in an interparty application for extension of time (see section 28 (8)). It is a further requirement that the magistrate has to be satisfied by information given by a police officer that there are reasonable grounds for believing that an offence under the Computer Misuse Act has been or is about to be committed in any premises. Secondly that evidence that such an offence has been or is about to be committed is in those premises. Clearly the law requires a warrant for searching premises. The

word "premises" includes a vehicle as indicated above. Further the authorised officer is clearly defined as a police officer who has obtained the necessary warrant. Search of the premises is not necessarily the search of computers or electronic devices such as cell phones. In other words, the officer may not know that such a device is in the premises. That is where section 28 (2) of the Computer Misuse Act, becomes relevant because it provides that an authorised officer may seize any computer system or take any samples or copies of application or data and grounds for doing this is provided for in the law.

As far as the ground is concerned, it is provided that the seizure is based on reasonable grounds where the devise is believed to be concerned in the commission or suspected commission of an offence, whether within Uganda or elsewhere. Secondly, that the computer system or samples or copies of applications or data that may afford evidence of the commission or suspected commission of an offence, whether within Uganda or elsewhere is present. That it is intended to use the seized data or system which is intended to be used for, on reasonable grounds believed to be intended to be used, in the commission of an offence. The section is further entrenched by section 28 (3) where it is clearly provided that the computer system referred to which may be seized by an authorised officer may be seized with samples of copies of application or data and may be taken only by virtue of a search warrant. Clearly an additional warrant to search the computer which has been seized pursuant to a search warrant is required. This in a nutshell, codifies the common law principles of interpretation of charter rights in Canada which are also enshrined in article 27 of the Constitution of the Republic of Uganda.

Going by the specific paragraphs and clauses of article 27 of the Constitution, article 27 (1) provides that no person shall be subjected to (a) unlawful search of the person, home or other property of that person. There are three prohibitions here. The first is the unlawful search of the person. The second is the unlawful search of the home and the third is the unlawful search of other property. Like the Canadian Charter, the law goes on to provide specifically that no person shall be subjected to unlawful entry by others of the premises of that person. Thirdly, it is provided that no person shall be subjected to interference with the

privacy of that person's home, correspondence, communication or other property. By providing for privacy of correspondence, communication or other property, it is clearly the case that even if somebody has a warrant to search a home, it is another matter specifically to interfere with the communication or correspondence or other property of the person. Section 28 of the Computer Misuse Act, captures all the elements of article 27 of the Constitution in that it provides for no search of the home person or other property without a warrant. It provides that there shall be no unlawful entry by others of the premises of that person. Thirdly, no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property. In other words, a judicial officer is required to authorise such interference with the privacy of personal, home or other property, in the circumstances of this appeal, under the Computer Misuse Act.

The judicial precedents we have reviewed immediately above deal with the common law right of search and found that it is modified by article 8 of the Canadian Charter which is similar to article 27 of the Constitution in that it protects the same right of privacy in similar words. The question is what is the unlawful search of a person, home or other property? The learned trial judge as indicated above relied on article 43 of the Constitution which allows derogation or limitation on fundamental and other human rights and freedoms. Article 43 clearly provides in clause 1 that in the enjoyment of the rights and freedoms prescribed in the Bill of Rights, no person shall prejudice the fundamental or other human rights and freedoms of others or the public interest. What is the "public interest" is not provided for except by exclusion of what it is not. Public interest does not permit political persecution, detention without trial and any limitation of the enjoyment of the rights and freedoms prescribed in the Constitution beyond what is acceptable and demonstrably justifiable in a free and Democratic society or what is provided for in this Constitution.

As far as what is provided for in the Constitution is concerned, article 43 clearly provides that what is prohibited is what is unlawful. It implicitly allows lawful search of the person, home or other property. We have carefully considered article 27 (2) provided separately from article 27 (1)

in that in article 27 (2) is provided that "no person shall be subjected to interference with privacy of that person's home, correspondence, communication or other property. On the other hand, in article 27 (1) it is provided that no person shall be subjected to unlawful search of the person, home or other property of that person or unlawful entry by others in the premises of that person. The question as to whether interference with the privacy of the person's home, correspondence communication or other properties provided separately the subject matter is better left for further interpretation by the constitutional court and cannot be and does not need to be decided in this matter.

For purposes of this appeal, because Parliament is authorised under article 79 of the Constitution to make laws on any matter of the peace, order, development and good governance of Uganda. We have examined section 28 of the Computer Misuse Act which allows seizure of computers and search of premises. In the context of article 27 of the Constitution, for any search of any premises or computer to be lawful, it has to be authorised by the law. The trial judge was concerned about the chilling effect section 28 of the Computer Misuse Act may have on the powers of law enforcement agencies to pursue investigations as and when the need arises including the power to search a computer or cell phone for data which may be relevant to the investigation of a criminal offence.

Indeed, that is what is envisaged under section 28 of the Computer Misuse Act. The standard is the requirement of a reasonable belief of a judicial officer that an offence under the Computer Misuse Act has been or is about to be committed in any premises or that evidence that such offence has been or is about to be committed is in those premises. The magistrates upon being satisfied with the matters set out in the law would issue the warrant for the search of the reported premises. Where a police officer has been authorised to enter and search the premises using reasonable force which may be necessary, that authorised officer may cease any computer system or take any samples of copies of application or data. Thereafter, that police officer may obtain a warrant to search the computer or the cell phone found in the searched "premises". The reason why the second warrant is necessary is because

the first search warrant is for discovery that is why section 28 (2) of the Computer Misuse Act envisages the seizing of any computer system or samples of copies of application or data found on the premises which are searched and a search warrant for the same reason that there are reasonable grounds to believe that it was concerned in the commission or suspected commission of an offence within or without Uganda. Or that the computer or electronic device may be evidence of the commission or suspected commission of an offence within or without Uganda. Or that the computer is intended to be used on reasonable grounds believed that it is intended to be used in the commission of an offence. In other words, the arrest and seizure of the appellants' electronic devises may have been on exigent grounds but this did not per se prove that the search of their devises was exigent. When the computers were in custody, a search warrant ought to have been obtained immediately to open them and spill open their contents.

We have carefully considered the evidence and particularly the testimonies of PW1, PW2 and PW 10 and PW 20 regarding the electronic evidence in the way of computers drives as well as flash disks. PW1 testified that certain information was found in the hard drive of the first appellant (in his laptop).

A license file was found in the laptop of the first appellant. He also found hacking tools. Evidence was retrieved from that laptop. There was an external hard disk which was also recovered. It had usernames and passwords. It had Uganda Revenue Authority hashes. It had hacking tools matasbite and fraudulent accounts. PW1 gave a detailed testimony about the data which was recovered. In cross examination PW1 testified that he got information around March 2011 about an ongoing scheme, which was considered in the prosecution case.

PW2 Mwebesa Bruno, Customs enforcement officer testified that on 19 June 2012, he got instructions from enforcement operations Daniel Arora to impound a vehicle registration number UAG 342R and arrest its occupants. They were suspected to be hacking into the URA computer system. He went with five enforcement officers and found three occupants holding three laptops. The fourth was watching and besetting. These people included the first appellant who had a laptop, Farouk (A2)

and Kibalama Richard also had laptops. The occupants of the car were arrested and their laptops removed and handed over to him (PW2). Thereafter he presented the vehicle, suspects and laptops to the enforcement office of URA. Among the things impound were an external hard drive, inverter, flash disk, five mobile phones, and iPhone and other documents. The laptops were Lenovo laptop, Samsung laptop and HP laptop. At the time of the arrest, he had a search certificate dated 19th of June 2012 the search certificate was admitted in evidence as exhibit P4.

In cross examination, he testified that none of the people who went to arrest the appellant's and other suspects were police officers. There were five army officers who participated in the arrest. Before moving on, the respondent relied on section 7 of the East African Customs Management Act for the provision that customs officers are police officers who can carry out searches and seizures. We reject this notion from the outset. Section 7 of the EACCMA reads as follows:

> **7.** For the purpose of carrying out the provisions of this Act, every officer shall, in the performance of his or her duty, have all the powers, rights, privileges, and protection, of a police officer of the Partner State in which such officer performs his or her duty.

Clearly every officer has powers of a police officer in carrying out duties under the East African Customs Management Act 2004 and not under the Computer Misuse Act. Further an "officer" under section 2 of the East African Customs Management Act is defined to mean:

> "officer" includes any person, other than a laborer, employed in the service of the Customs, or for the time being performing duties in relation to the Customs;

Clearly the customs officers or enforcement officers carry out duties under the East African Customs Management Act and not the Computer Misuse Act. In addition, we accept the submissions of the appellants that under section 158 and 159 of the EACCMA, searches are still conducted after a search warrant is obtained from a Magistrate. Sections 158 and 159 follow each other provide that:

> **158.**---(1) Without prejudice to any other power under this Act, where any officer declares on oath before any magistrate that he or she has reasonable grounds to believe that there are in any premises any uncustomed goods or

documents relating to any uncustomed goods, then such magistrate may by warrant under his or her hand authorize such officer to enter upon and search, with such force as may be necessary and by day or by night, such premises and to seize and carry away any uncustomed goods or documents relating to any uncustomed goods found therein.

(2) An officer in possession of a search warrant may require any police officer to assist him or her in the execution of such warrant and any police officer so required shall render assistance accordingly.

Power to require production of books, etc.

159.---(1) Where-

(a) information has been given to the proper officer that any goods have been, or are intended to be, smuggled, or undervalued, or dealt with in any way contrary to this Act; or

(b) any thing or goods have been seized under this Act, the proper officer may require the owner of the goods or thing to immediately produce all books and documents, whether in written form or on micro-film, magnetic tape or any other form of mechanical or electronic data retrieval mechanism relating in any way thereto, or to any other goods imported, exported, carried coastwise, manufactured, purchased, sold or offered for sale by that owner within a period of five years immediately preceding the requirement.

(2) On the production of such books or documents the proper officer may inspect and take copies of any entries in the books or documents; and the proper officer may seize and detain any such book or document if, in his or her opinion, it may afford evidence of the commission of an offence under this Act.

The above two sections demonstrate that powers of officers under the East African Community Customs Management Act apply in the clear context of application of East African Community Law. Where a person is charged under a national, law, the laws of Uganda such as the Computer Misuse Act is applicable and enforceable on its own terms. It is a national law as opposed to a community law relied on by the respondent. Community Laws take precedence over national laws in case of conflict under section 253 of the EACCMA, 2004. In any case, the precedence relates to community laws and not national laws. Section 253 provides that:

This Act shall take precedence over Partner States' laws with respect to any matter to which its provisions relate.

In this appeal the appellants were charged under the Computer Misuse Act and the charge under the East African Community Act did not succeed and was not appealed. The matter is therefore solely governed by national laws.

In the premises, there is clearly no evidence that a search warrant was obtained from a magistrate. The items were recovered from a vehicle which fits the definition of "premises" under section 28 (8) of the Computer Misuse Act. Further the learned trial judge in a ruling pursuant to the submissions of the defence that section 28 of the Computer Misuse Act was not complied with and that without a search warrant no one can seize the article specified therein ruled on the matter. He found that given the circumstances pursuant to the evaluation of evidence of PW2, PW6 and PW 26, the prevailing circumstances where such that instant response to act in the circumstances had presented itself. They did not act unreasonably in the circumstances and the seizure on occasion of the arrest of the appellants was lawful. They seized items were eventually handed over by PW2 and the manager of forensic investigations of URA tendered it in evidence.

We agree with the learned trial judge that the seizure of the items upon suspicion could have been lawful. However, the items were supposed to be returned within 72 hours under section 28 (8) the Computer Misuse Act 2011. They were not. Secondly, upon seizing the computers, flash disks, external hard disk et cetera, that was not a right without authorisation to search the items for information. The state had sufficient time to obtain a search warrant from a magistrate. The items were seized on 19 June 2012 but the evidence of PW1 indicated that investigations began around March 2011. Even if the computer was found in the commission of an offence, there was no evidence adduced by the people who seized the computer of any activity that was going on at the time the computer was seized other than speculative evidence. The computers were not examined there and then as items found in possession of the arrested persons under section 6 of the Criminal Procedure Code Act so as to provide further clues in investigations. In the premises, the search of the computers while in the custody of the state and without the sanction of court violated article 27 of the Constitution of the Republic of

Uganda because it was unlawful. Secondly, it violated the section 28 of the Computer Misuse Act in that there was no police officer involved in the seizures or the search of the computers. It was not carried out by an authorised officer.

The fact that the computer could have contained incriminating evidence does not justify search without a warrant. It was not exigent or urgent once the items were in the custody of the state. The state even had the time to send one computer to south Africa for forensic analysis but did not seek leave of a magistrate. The conclusion that the search of the computers was exigent in the circumstances was an erroneous conclusion of the learned trial judge. We find that the search of the computers and hard discs which were in custody was an unlawful search forbidden by article 27 of the Constitution of the Republic of Uganda. The search of the computers could not be justifiable in a free and Democratic society because it was not done in accordance with the law which allowed search and instances when it would be made. The arrest of the appellants was lawful but clearly there was non-compliance with section 28 of the Computer Misuse Act, the very law under which the appellants were charged. It is section 28 of the Computer Misuse Act which authorises a magistrate upon being satisfied that an offence was being or is about to be committed only to issue a warrant authorising a police officer to enter and search premises which include a motor vehicle. Secondly, the authorised officer may seize any computer system found in such a vehicle or premises. In other words, the very law which authorises the seizure of the computers specified how it is to be done. If the appellants were about to escape, it was sufficient to arrest them and impound the computers and obtain a search warrant so that the contents of the computers can be established. The investigation had taken a long period of time. We would find that the evidence extracted from the computers ought to have been excluded for violation of section 28 of the Computer Misuse Act as well as article 27 of the Constitution of the Republic of Uganda. We do not agree with the trial judge that compliance with section 28 of the Computer Misuse Act, would make it difficult for the police to enforce the law or to investigate crime. This is because even if the appellants were arrested in the heat of the moment when

committing the offence, there was still sufficient time within 48 hours when they were arrested to obtain the warrant of search so that the computers can be investigated. Further, if any warrant of search is not sufficient to keep the computer for several months. It was necessary in any interparty application, to apply to the court to extend the period of 72 hours within which to carry out forensic analysis. Breach of the law rendered the evidence obtained in violation of it an illegality and therefore the search of the computers was unlawful and forbidden by article 27 of the Constitution of the Republic of Uganda.

In the premises, we would allow ground 1 of the appeal.

Ground 2 of the appeal is that **the learned trial judge erred in law and fact when he convicted the appellants without the prosecution disclosing the Encase software forensic tool used and mirror images analysed to the defence, as required by the law thus occasioning a miscarriage of justice**.

Ground 2 of the appeal ought to have been argued in the alternative because it deals with information obtained from the laptops from which forensic evidence was admitted. In the absence of such evidence on the ground that it is excluded for noncompliance with article 27 of the Constitution and section 28 of the Computer Misuse Act, there is no need to consider or view forensic images of two laptops and one external hard disk which cannot be admitted in evidence.

Grounds three & five.

Having allowed ground 1 of the appeal, the issue of evaluation of evidence and inconsistencies and contradictions does not add any weight to the prosecution evidence or the appellants defence as the foundation of the evidence is the forensic evidence erroneously admitted. We find it unnecessary to evaluate the evidence whose foundation has been excluded.

Ground 4

The learned trial judge erred in law when he commenced the trial and convicted the appellants without the assessors taking oath and contrary to the provisions of the law, thereby occasioning a miscarriage of justice.

The effect of failure to take oath has been the subject of numerous decisions.

As a matter of fact, the appellant submitted that the assessors were not sworn and therefore the trial was a nullity. He relied on Alenyo Marks v Uganda; Supreme Court Civil Appeal No. 08 of 2007 for the proposition that a trial that proceeds without swearing in of assessors is a nullity. (See also Abdu Komakech v Uganda; Supreme Court Civil Appeal No. 1 of 1994). On the other hand, the respondent submitted that no prejudice had been occasioned to the appellant because the assessors participated throughout the trial and there was a summing up to them before they gave their opinion.

We have carefully considered the controversy as to whether the assessors were sworn in before taking the seat as assessors in the trial of the appellants. We have carefully considered the record and find that the matter initially proceeded before the principal magistrate grade 1. Mrs Mary Kamuli Kuteesa on behalf of the state applied for the case to be tried by the High Court because of the seriousness of the case. The accused were committed to the High Court under section 168 of the Magistrates Courts Act.

We have carefully considered the Computer Misuse Act and section 31 thereof which deals with the jurisdiction of the courts provides that:

> 31.Jurisdiction of courts.
>
> A court presided over by a chief magistrate or magistrate grade 1 has jurisdiction to hear and determine all offences in this Act and, notwithstanding anything to the contrary in any written law, has power to impose the full penalty or punishment in respect of any offence under this Act.

We find it quite strange that a magistrate grade 1 does not try such an offence with assessors. When it is sent to the High Court for trial, there is a requirement for assessors the procedure for swearing in and conduct of the trial with assessors.

It cannot be the case that a magistrates' court which tries without assessors cannot be objected to on the ground that the matter was tried without assessors and when it is remitted to the High Court for trial, it becomes an issue that the trial proceeds without assessors having been

sworn in. What was the seriousness of the case that required the matter to be tried by the High Court? Section 166 of the Magistrates Courts Act provides that:

> Where a charge has been brought against a person in a court having no jurisdiction to try the offence with which he or she is charged, the magistrate shall remand the accused person in custody to appear before the court having jurisdiction to try that offence.

Section 167, a magistrates' court on the application of the DPP may transfer a case which ought to be tried by a Superior Court for trial by the Supreme Court.

Section 168 deals with committal for trial by the High Court clearly provides that it applies to cases to be tried by the High Court. What is a case to be tried by the High Court? We think that offences that are triable by other courts are not triable by the particular magistrates' court in terms of its jurisdiction. For the moment we are not concerned with territorial jurisdiction of Magistrates and limit the judgment to jurisdiction of Magistrates Courts to try the kind of offence. The jurisdiction in criminal matters is provided for under section 161 of the Magistrates Courts Act which is clear and provides that:

> 161. Criminal jurisdiction of magistrates.
>
> (1) Subject to this section, a magistrate's court presided over by—
>
> (a) a chief magistrate may try any offence other than an offence in respect of which the maximum penalty is death;
>
> (b) a magistrate grade I may try any offence other than an offence in respect of which the maximum penalty is death or imprisonment for life;
>
> (c) a magistrate grade II may try any offence under, and shall have jurisdiction to administer and enforce any of the provisions of, any written law other than the offences and provisions specified in the First Schedule to this Act;
>
> (d) a magistrate grade III may try any offence under, and shall have jurisdiction to administer and enforce any of the provisions of, any written law other than the offences and provisions specified in the First and Second Schedules to this Act.

(2) In this section, references to an offence shall be taken as including references to attempts to commit, aiding and abetting or inciting the commission of that offence.

(3) Nothing in this section shall derogate from the provisions of any written law which provide that any offence shall be triable, or any provision shall be administered or enforced, only by a particular grade of magistrate or by a particular court.

(4) For the removal of doubt, it is declared that no magistrate's court shall have jurisdiction to take cognisance of any offence of robbery as defined in section 285 of the Penal Code Act and punishable under section 286(2) of that Act.

It is clear that the offence charged is not a capital offence and a magistrate could try the offence. The application of the DPP is envisaged under section 167 of the MCA and provides for the DPP to apply at any stage of the proceedings upon finding that it is the case that ought to be tried by a court superior to that of the Magistrate's Court. This is not one of those cases that ought to be tried by the High Court. The above notwithstanding section 169 of the MCA allows the DPP to make an application for a transfer of a matter to the High Court and the application is not to be refused on the ground that the magistrates court has jurisdiction to try the offence. Section 169 of the MCA provides as follows:

169. Director of Public Prosecutions to determine offences to be committed to High Court.

Subject to section 168, for the avoidance of doubt it shall be within the discretion of the Director of Public Prosecutions which offences are to be proceeded with under section 168 for trial before the High Court or to be tried by a magistrate's court; and trial by the High Court of an offence committed to that court under section 168 shall not be refused merely on the ground that a magistrate's court has jurisdiction to try the offence.

It is our finding that this was a case that was triable by the magistrates' court and the procedure for trial did not require the participation of assessors. Secondly, we have considered the jurisdiction of the High Court. The High Court is an appellate court for purposes of appeals from the decision of a Magistrate Grade 1 or a Chief Magistrate. The above notwithstanding, the High Court has jurisdiction under section 1 of the Trial on Indictments Act try any offence under any written law and

purpose in his sentence authorised by the law. The High Court would not try any offence under any law unless the accused person has first been committed for trial to the High Court in accordance with the Magistrates Courts Act.

Having carefully considered the law, we are of the firm view that the appellants suffered no prejudice when they were tried with assessors and the only allegation is that the assessors were not sworn in. There is no clear record as to what actually happened at the preliminary stage when the matter was remitted to the High Court. In our view it is a question of scanty records since the learned trial judge complied with all the procedures of trial with the participation of assessors under the Trial on Indictments Act. Section 3 of the TIA provides that except as provided by any other written law, all trials before the High Court shall be with the aid of assessors, the number of assessors shall be two or more as the court thinks fit. In the circumstances of this appeal, it would be absurd to find that a magistrates' court which had jurisdiction in the matter could try without assessors and it would be an invalid trial if the High Court tries the same matter with assessors due to irregularity of not having sworn in for purposes of trial by the High Court. It would also be absurd, to grant bail to such accused persons triable by a magistrates' court on the same footing as persons charged with a capital offence which is exclusively triable by the High Court.

In light of our decision on the ground of trial on the basis of evidence that ought to have been excluded, we find no need to rule on ground 4 of the appeal.

Ground 6 of the appeal that **the learned trial judge erred in law and fact when he convicted and sentenced the appellants in violation of the Constitution prohibition against double jeopardy.**

Having allowed ground 1 of the appeal, we find no need to try the rest of the grounds against sentence.

We find that failure by the learned trial judge to exclude evidence extracted from computers which evidence was accessed without an order of search of the computers by a magistrate violated article 27 of the Constitution rendering the trial a nullity. The material evidence used

to convict the appellants was the primary and unlawfully procured evidence relied on by the prosecution.

The appellants had been charged in 2012 and were sentenced in 2013. The matter then went on appeal and the Court of Appeal ordered a retrial. The matter was further appealed to the Supreme Court which restored the order of the High Court. Thereafter this appeal was argued in June 2022. It is now October 2022, a period of about 10 years. The appellants had been sentenced to a maximum of 12 years' imprisonment and eight years' imprisonment to run concurrently.

We find that ordering a retrial in the circumstances is impracticable and would be prejudicial to the appellants. We accordingly allow the appellants appeal against conviction and sentence and acquit the appellants. We order that the appellants be set free unless held on other lawful charges.

Dated at Kampala the 14th day of October 2022

Catherine Bamugemereire

Justice of Appeal

Christopher Madrama

Justice of Appeal

Eva K. Luswata

Justice of Appeal