THE REPUBLIC OF UGANDA

IN THE HIGH COURT OF UGANDA SITTING AT KAMPALA

CRIMINAL SESSIONS CASE No. 0203 OF 2014

UGANDA …… PROSECUTOR

VERSUS

KISEMBO STEPHEN …… ACCUSED

Before Hon. Justice Stephen Mubiru

JUDGMENT

The accused is indicted with two counts of Unlawful Disclosure of information C/s 10 (1) and (2) (b) of *The Security Organisations Act*. It is alleged in Count one that the accused between the year 2009 and 2010 at the External Security Organisation Headquarters in Nakasero, Kampala District, being employed by the said organisation as a filing clerk, did disclose secrets, to wit; weekly briefs plus weekly intelligence briefs to His Excellency the President of Uganda, to a one [Redacted], a [Redacted] Diplomat who is an unauthorised person. In Count two, it is alleged that the accused between the year 2010 and 28th September, 2013 at the External Security Organisation Headquarters in Nakasero, Kampala District, being employed by the said organisation as a filing clerk, did disclose secrets, to wit; weekly briefs plus weekly intelligence briefs to His Excellency the President of Uganda, to a one [Redacted], a [Redacted] Diplomat who is an unauthorised person.

The prosecution case briefly is that by a letter of appointment dated 25th May, 1988 (exhibit P. Ex.1), the accused was appointed as an Executive Officer of the External Security Organisation (ESO) with effect from 1st September, 1995. At all material time thereafter, he was deployed as the Filing Clerk / Courier at the ESO headquarters in Kampala. As part of his duties, he was responsible for delivering weekly security briefs prepared by the Director General of ESO, to His Excellency the President at the Nakasero State Lodge. The practice was that such briefs would be placed in a specialised brief case with an encoded lock. The accused would deliver the brief case

to [Redacted] at the Nakasero State House. She would call the Secretary to the Director General of ESO for the secret code, open the brief case and sign for the brief.

During or around July, 2012 a meeting was convened between the Director General of the [Redacted] Intelligence Service and the Director General of ESO at which the former promised technical assistance to the latter by way of telecommunications [Redacted] devices. As usual, the then Director General of ESO, [Redacted], prepared a security brief to His Excellency dated 20th November, 2012. It is entitled "Offer by [Redacted] to install additional Technical Equipment at ESO [Redacted] Project for Satellite Telephone and VSAT Communication [Redacted]" (exhibit P. Ex.2) In accordance with the usual practice, it was given to the accused for delivery to the State House.

Sometime in March 2013, credible information was received by ESO from sources in the [Redacted] Intelligence Service as to loss or compromise of that piece of classified intelligence information regarding cooperation between ESO and the [Redacted] Intelligence Service that had leaked to the Government of [Redacted]. This suggested that leaks may have occurred over such an extended period of time. Intensive counter intelligence began with the surveillance of all ESO staff who ordinarily would have access to that document. That surveillance yielded information that rendered the accused the key suspect. On 25th September, 2013 the accused was stopped just before he exited the ESO gate, searched and a document dated 2nd July, 2013 entitled "Brief on the verification exercise regarding [Redacted]'s allegations against Uganda, conducted by the International conference on the Great Lakes Region (ICGLR) - Joint Intelligence Fusion Centre (JIFC) team, based in [Redacted])" exhibited as P. ID.1 was recovered from underneath his shirt. Upon interrogation, the accused revealed that he had been in the practice of giving such information to a one [Redacted] and before him, a one [Redacted], both [Redacted] Diplomats in Uganda. The practice had been going on since the year 2009. He was arrested and these admissions were recorded in a charge and caution statement (exhibit P. Ex. 4 dated 9th October, 2013) and a letter of apology addressed to His Excellency the President (exhibit P. Ex.7 dated 26th September, 2013).

Consequently, ESO organised a joint operation with The Joint Anti-Terrorist Task Force (JATT) and on Saturday 28th September, 2013 the accused was taken from ESO custody, was handed the

document P. ID.1. and was driven to dark alley in Muyenga-Kisugu, being the place the ESO counter intelligence surveillance had identified as his rendezvous with the [Redacted] Diplomat [Redacted]. While there, from vantage points under cover, the JATT operatives observed him hand over the document to the diplomat. In return the diplomat gave the accused a sum of 100 US dollars and U. Shs. 50,000/= (exhibit P. ID.2). Part of that operation was videotaped and the recording was exhibited in court as P. Ex.4.

In his defence, the accused denied having leaked any secret information. He denied having been arrested at the ESO gate with the document (exhibit P. ID.2). Instead he contended that he had been arrested from the office of the then Deputy Director of ESO as he was delivering a message to him. He was forced under duress and threats to confess to having leaked secret information. He signed the charge and caution statement (exhibit P. Ex. 4 dated 9th October, 2013) and a letter of apology addressed to His Excellency the President (exhibit P. Ex.7 dated 26th September, 2013) against his will. The document (exhibit P. ID.2) was given to him by the ESO operatives with an intention to falsely implicate him in an operation they orchestrated. He considers this fabricated evidence intended to falsely accuse him in pursuit of an institutional vendetta against him for having earlier that year leaked to His Excellency the President, information regarding false accounting within ESO in matters relating to staff emoluments. This resulted in the publication of a headline article in The Daily Monitor Newspaper of 4th September 2013 to the effect that the President had directed a probe into that issue as a result of the leak of that information. He is being witch-hunted for having leaked the information.

The accused having pleaded not guilty, the prosecution has the burden of proving the case against him beyond reasonable doubt. The burden does not shift to the accused person and the accused is only convicted on the strength of the prosecution case and not because of weaknesses in his defence (See *Ssekitoleko v. Uganda [1967] EA 531*). By his plea of not guilty, the accused put in issue each and every essential ingredient of the two offences with which he is charged and the prosecution has the onus to prove each of the ingredients beyond reasonable doubt. Proof beyond reasonable doubt though does not mean proof beyond a shadow of doubt. The standard is satisfied once all evidence suggesting the innocence of the accused, at its best creates a mere

fanciful possibility but not any probability that the accused is innocent, (see *Miller v. Minister of Pensions [1947] 2 ALL ER 372*).

For the accused to be convicted for the offence of Unlawful Disclosure of information C/s 10 (1) and (2) (b) of *The Security Organisations Act*, the prosecution must prove each of the following essential ingredients beyond reasonable doubt;

1. An act or omission resulting in communication, release or disclosure of information to another person.
2. The information transferred is intelligence or secrets of the security organisation
3. The act or omission was without lawful authority and the recipient was unauthorised.
4. The act or omission was that of the accused person.
5. The accused is a person employed or formerly employed by the security organisation.

The minor cognate offence to the two counts is Attempted Unlawful Disclosure of information C/s 10 (1) and (2) of *The Security Organisations Act* and section 386 and129 (1) of *The Penal Code Act*. Since an attempt to commit a crime consists of two elements; (1) an intent to engage in crime; and (2) a conduct constituting a substantial step towards commission of the crime, it is reduced to that when the prosecution fails to prove actual unlawful communication, release or disclosure of the alleged information, but proves the accused had an intention to actually commit the crime, and proceeded to perform an act which is a substantial step toward the commission of the crime, but not the actual commission of the crime.

The first ingredient of each of the two counts requires proof of communication, release or disclosure of information to another person. Communication or disclosure may be done verbally, in writing, by conduct. There should be evidence of communication or physical transfer of information to an unauthorised recipient, i.e. evidence of an event involving the exposure of information to persons or entities not authorised access to the information in question. An unauthorised recipient can be anyone who does not possess the clearance necessary for the sensitivity of the information, as well as a legitimate need to obtain the information. The communication, release or disclosure can be through leaks, spills, espionage or improper safeguarding procedures.

Leaks are deliberate disclosures of classified information to the media. Spills are accidental or intentional disclosures of classified information that occur across computer systems. Espionage includes activities designed to obtain, deliver, communicate, or transmit information relating to the national security with the intent or reason to believe such information will be used to harm Uganda or to the advantage of a foreign nation or transnational entity. Improper safeguarding procedures may involve acts such as leaving a classified document on a photocopier, forgetting to secure classified information before leaving office, and discussing classified information in earshot of unauthorised recipients.

In the instant case P.W.2 [Redacted] stated that in March 2013 credible information was received from sources in the [Redacted] Intelligence Service as to loss or compromise of one piece of classified intelligence information regarding cooperation between ESO and the [Redacted] Intelligence Service that had leaked to the Government of [Redacted]. This suggested that leaks may have occurred over such an extended period of time as to indicate the possibility of a systemic compromise, that would potentially jeopardise intelligence activities, sources or methods. Intensive counter intelligence began for evidence of an unauthorised disclosure of classified intelligence information to a foreign power, or an agent of a foreign power, or evidence indicating possible espionage.

This was corroborated by P.W.8 [Redacted], the then Director General of the External Security Organisation who stated that that following the tip off to the effect that they were losing intelligence information, intensive surveillance of all persons holding sensitive positions in the organisation began. In his defence, the accused D.W.1. Kisembo Stephen denied such an occurrence and contended instead that this is a cover up for a vendetta against him. He is being witch hunted for being a whistleblower over false accounting relating to staff emoluments within the organisation.

Both P.W.2 [Redacted] and P.W.8 [Redacted] did not disclose the source of that information, who as a result was not availed for cross-examination and it is thus technically hearsay evidence. According to section 59 of *The evidence Act*, oral evidence must in all cases whatever, be direct.

That is to say, it must be based on direct personal knowledge or experience. Testimony based on what a witness has heard from another person rather than on direct personal knowledge or experience is referred to as hearsay evidence, in other words, evidence of those who relate, not what they know themselves, but what they have heard from others. A statement made out of court that is offered in court as evidence to prove the truth of the matter asserted is generally inadmissible as hearsay. This is because statements made out of court normally are not made under oath, a judge cannot personally observe the demeanour of someone who makes such a statement outside the courtroom, and an opposing party cannot cross-examine such a person. Such statements hinder the ability of the court to probe the testimony for inaccuracies caused by ambiguity, insincerity, faulty perception, or erroneous memory. Thus, statements made out of court are perceived as untrustworthy.

However, there are exceptions for example under section 30 of *The evidence Act* and the common law, none of which applies to this kind of information as stated by P.W.2 [Redacted] and P.W.8 [Redacted]. Another exception may be inferred from the provisions of section 32 (3) (c) (ii) of *The Access to Information Act, 2005*, information relating to the characteristics, capabilities, vulnerabilities, performance, potential, deployment or functions of any body or person responsible for the detection, prevention, suppression or curtailment of subversive or hostile activities may be restricted from the public. This provision is a recognition of that fact that public disclosure is not always in the public interest. It restricts public access to information relating to the characteristics, capabilities, vulnerabilities, performance, potential, deployment or functions of any body or person responsible for the detection, prevention, suppression or curtailment of subversive or hostile activities. It protects sources of intelligence from disclosure.

A source of intelligence is a person or institution that provides, has provided, or has been engaged to provide the security organisation with information of a kind the security organisation needs to perform its intelligence function effectively, yet could not reasonably expect to obtain without guaranteeing the confidentiality of those who provide it. Strict application of the rule against hearsay may be justified where there is evidence to suggest that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness. To apply the restriction on hearsay evidence to sources of this kind would be to undermine the guarantee

confidentiality necessary for obtaining information, which not only contravenes Parliament's express intention but also to overlook the practical necessities of modern intelligence gathering.

Forced disclosure of the identities of their intelligence sources could have a devastating impact on the ability of security organisations created under *The Security Organisations Act, 1987* to carry out their statutory mission. There is a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our external intelligence service. If potentially valuable intelligence sources come to think that the security organisation will be unable to maintain the confidentiality of its relationship to them, many could well refuse to supply information to the security organisations in the first place. Even a small chance that some court will order disclosure of a source's identity could well impair intelligence gathering and cause sources not to provide the required information.

Moreover, a court's decision whether an intelligence source will be harmed if his identity is revealed will often require complex political, historical, and psychological judgments. Whereas the national interest sometimes makes it advisable, or even imperative, to disclose information that may lead to the identity of intelligence sources, it is the responsibility of the security organisations, not that of a Judge, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the security organisation's intelligence-gathering process. For the foregoing reasons, it is in the public interest to allow a limited use of hearsay evidence in matters of this nature, where particularly the undisclosed source of intelligence does not, as in this case, directly implicate the accused standing trial. I therefore find that the prosecution has proved to the required standard that there was communication of information ordinarily in the custody of The External Security Organisation to unauthorised persons outside that organisation.

The second ingredient required for establishing both counts is that the information so transferred or communicated constitutes intelligence or secrets of The External Security Organisation. Under section 3 of *The Security Organisations Act*, 1987, ESO is mandated to (a) to collect, receive and process internal and external intelligence data on the security of Uganda; and (b) to advise and

recommend to the President or any other authority as the President may direct on what action should be taken in connection with that intelligence data. However, not all information in custody of the organisation is classified as intelligence or secret. In order for the information in issue to be classified as intelligence It must be shown to have been secret information about an enemy or potential enemy; or useful in planning and conducting national security policy; or to aid in formulating and implementing foreign policy, or in determining domestic policies for national security or the conduct of covert activities abroad to facilitate the implementation of foreign policy.

In broad terms intelligence covers both the process of and product resulting from the collection, evaluation, collation, interpretation, and analysis of all available information concerning the intentions, capabilities and objectives of other countries which are significant to a government's development and execution of plans, policies, decisions, and courses of action. Intelligence has been defined as "the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operation and which is immediately or potentially significant to planning" (see the *Dictionary of United States Military Terms for Joint Usage* (Revision of February 1957). Another definition; " Intelligence is the collecting and processing of that information about foreign countries and their agents which is needed by a government for its foreign policy and for national security, the conduct of non-attributable activities abroad to facilitate the implementation of foreign policy, and the protection of both process and product, as well as persons and organizations concerned with these, against unauthorized disclosure" (see *Studies in Intelligence*, Vol. 2, No. 2 (Spring 1958), page 76).

As regards information deemed secret, Security Organisations ordinarily restrict the processes by which specific types of information important to national security are requested, collected, analysed, and provided to policymakers. What is secret information depends on its sensitivity which in turn determines the desired degree of secrecy. Sensitivity is based upon a calculation of the damage to national security that the release of the information would cause, hence ordinarily there are three levels of classification; "Confidential," "Secret," and "Top Secret," with each level of classification indicating an increasing degree of sensitivity.

The highest security classification "Top Secret," is ordinarily applied to information, the unauthorised disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the security organisation is able to identify or describe. Information classified as "Secret" is that whose unauthorised disclosure would cause "serious damage" to national security, while "Confidential" information is that which would "damage" national security if publicly disclosed without the proper authorisation. Special permissions would be required for handling information at each of the three levels. On the other hand, unclassified information is usually that which can be released to individuals without a clearance. The classification system is governed by administrative arrangement within the organisation rather than by law. Good practice would demand that the organisation ensures that proper classification markings appear on all classified information.

In the instant case the prosecution witnesses did not testify as to the different classifications of information in custody of The External Security Organisation. On his part, the accused in his defence admitted being aware of two categories; "Secret" and "confidential." The information in issue would be classified as "Secret" and this meant that it was for the recipient only. They never had the category of "top secret." Exhibit P. Ex.2 dated 20th November, 2012 is addressed to his Excellency the President and signed by the then Director General of ESO, [Redacted], is entitled "Offer by [Redacted] to install additional Technical Equipment at ESO [Redacted] Project for Satellite Telephone and VSAT Communication [Redacted]." P. ID.1 dated 2nd July, 2013 is addressed to his Excellency the President and signed by the then Director General of ESO, [Redacted], is entitled "Brief on the verification exercise regarding [Redacted]'s allegations against Uganda, conducted by the International conference on the Great Lakes Region (ICGLR) - Joint Intelligence Fusion Centre (JIFC) team, based in [Redacted]." According to P.W.2 [Redacted], the document P. ID.1 was generated following a meeting that took place in July, 2012 between the Director general of the [Redacted] Intelligence Service and the Director General of ESO at which the former promised technical assistance to the latter by way of telecommunications [Redacted] devices. That document was a brief to His Excellency the President written by the Director Technical Intelligence regarding the outcome of that meeting.

The information was limited to a few members of ESO who attended that meeting. The accused was responsible for delivering the briefs using a brief case with a coded lock.

The fact that the transmission of this particular category of classified information involved very specific hand-carry procedures suggests that it was in the category of the highest security classification of "Top Secret." Classification can be inferred by court from the manner in which these weekly briefings were transmitted under normal circumstances. Having examined the content of the exhibit P. Ex.2 dated 20th November, 2012 is addressed to his Excellency the President and signed by the then Director General of ESO, I have formed the opinion the it falls within the category of information, the unauthorised disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that is identifiable or describable, considering the countries involved and the subject matter of the controversy. I therefore find that it has been proved beyond reasonable doubt that the information so transferred or communicated constitutes intelligence or secrets of The External Security Organisation.

The third essential ingredient required for proving these two offences is that the act or omission that caused the communication or transfer of that information, was without lawful authority. This requires evidence of intentional communication such as that which occurs with leaks involving deliberate disclosures of classified information to the media or espionage which involves activities designed to obtain, deliver, communicate, or transmit information relating to the national security with the intent or reason to believe such information will be used to harm Uganda or to the advantage of a foreign nation or transnational entity. Proof of mere accidental communication through such occurrences as improper safeguarding procedures which may involve acts such as leaving a classified document on a photocopier, forgetting to secure classified information before leaving office, and discussing classified information in earshot of unauthorised recipients or spills by way of accidental disclosures across computer systems, would not be sufficient.

Although secrecy is critical to intelligence, it is not a universal attribute. There is overt reporting by representatives abroad, overt processing of overt materials, overt disclosure of finished intelligence. Under section 32 of *The Access to Information Act, 2005*, restrictions may be

imposed in respect of public access to information that; (a) is likely to prejudice the defence, security or sovereignty of Uganda; (b) subject to subsection (3), that is likely to prejudice the international relations of Uganda; or (c) would reveal information supplied in confidence by or on behalf of another State or an international organisation. This includes under section 32 (3) (c) (ii) of the Act, information relating to the characteristics, capabilities, vulnerabilities, performance, potential, deployment or functions of any body or person responsible for the detection, prevention, suppression or curtailment of subversive or hostile activities.

By reason of the three levels of classification, i.e. confidential, secret, and top Secret, with each level of classification indicating an increasing degree of sensitivity, special permissions would be required for handling information at each of the levels. Authorisation requires two basic components; (i) the user of the information must possess the clearance necessary for the sensitivity of the information, and (ii) as well as a legitimate need to obtain the information. Cleared personnel are legally bound not to view or share classified information in the public domain and may be subject to sanctions if they seek out such information, acknowledge its accuracy or existence, or disseminate the information in any way. Even when classified information has been put in the public domain, cleared employees are not permitted to freely share it. They must be careful not to make any statement or comment that confirms the accuracy of or verifies information requiring protection. Once an employee discovers or suspects unauthorised disclosure, that employee is under a duty first to protect the classified information to prevent further unauthorised disclosure. Then the employee must report the unauthorised disclosure to the appropriate authorities who will, in turn, investigate the incident and impose sanctions, if warranted.

In his defence, the accused stated that the information contained in exhibit P. Ex.2 dated 20th November, 2012 addressed to his Excellency the President, signed by the then Director General of ESO, [Redacted], and entitled "Offer by [Redacted] to install additional Technical Equipment at ESO [Redacted] Project for Satellite Telephone and VSAT Communication [Redacted]," was classified as "Secret" and that this meant that it was for the recipient only, His Excellency the President. Accordingly, when evidence is adduced that it was communicated or transferred to persons other than the intended recipient, the presumption is that it was not done after securing the special permissions for handling such information. The burden then rests on the person found

to have communicated or transferred it to show that it was done with the necessary permission and that the person to whom it was communicated or transferred possessed the corresponding clearance necessary for the level of sensitivity of the information, as well as a legitimate need to obtain the information. Since the prosecution will have discharged its burden once it evidence to show that the information was communicated or transferred to persons other than the intended recipient, I accordingly find this ingredient too has been proved beyond reasonable doubt.

The next essential ingredient required for proving these two counts is that the accused is a person employed or formerly employed by the security organisation. The evidence implicating the accused must show that he is in the current employment of the organisation or was its former employee. By implication, *The Security Organisations Act*, *1987* imposes an obligation on a cleared employee, to protect classified information by following proper classification procedures, applying classification instructions, physically safeguarding classified information, and complying with guidelines for publishing information. Employees are required to protect classified information throughout their lives, even after they are no longer employees of the organisation.

The admitted evidence of P.W.1 David Pulkol and exhibit P. Ex.1 dated 25th May, 1988 show that the accused was appointed to the organisation as an Executive Officer with effect from 1st September, 1995. P.W.3 [Redacted] the then Deputy Director, ESO testified that he knew the accused as the Filing Clerk / Courier at the ESO headquarters in Kampala. P.W.2 [Redacted], the then Director of Administration and Finance, ESO testified too that he knew the accused as the Filing Clerk / Courier at the ESO headquarters in Kampala. P.W.8 [Redacted] the then Director General of ESO stated that he too knew the accused as the Filing Clerk / Courier at the ESO headquarters in Kampala. He was an exemplary employee until this incident. In his defence, the accused admitted that he was the Filing Clerk / Courier at the ESO headquarters in Kampala. I accordingly find this ingredient too has been proved beyond reasonable doubt.

Lastly, it must be proved in respect of each of the counts that it was the accused who communicated or transferred the intelligence information or secrets of the security organisation in issue. Unauthorized disclosure of classified information can happen in various ways. It can be

disclosed either intentionally or accidentally and can occur through leaks, spills, espionage, or not following proper safeguarding procedures. The evidence implicating the accused must show the factum of intentionally conveying classified documents, information, or material to any unauthorised person. In his defence, the accused denied having committed the offences with which he is indicted. He stated that he was coerced to make the confession and to write the letter of apology and that the entire accusation is based on retaliatory fabrication of evidence. He is being witch-hunted for having leaked information regarding false accounting in matters relating to staff emoluments.

In his statement to the police dated 29th September, 2013 (exhibit D. Ex.1), P.W.3 [Redacted], the then Deputy Director, ESO stated that "sometime in September a secret document leaked and was found in town and we became suspicious and we zeroed on Kisembo."This was based on analysis of call data that indicated the accused had been in communication with a one Swaibu Butengenene who was on the run for leaking government secrets. He briefed the Director General who authorised him to organise with JATT and interrogate Kisembo. On interrogation, Kisembo admitted that he had been selling Government secrets to the Khartoum Government. JATT then organised an operation in which the accused was handed a document and he was then video-taped handing it over to a [Redacted] Diplomat, [Redacted], at Muyenga-Kisugu on the night of 28th September, 2013 at around 8.00 am, and in return, receiving a sum of 100 US dollars and U. Shs. 50,000/= (exhibit P. ID.2).

The part of that operation that was videotaped was presented to court by way of (exhibit P. Ex.4). P.W.3 [Redacted] stated that before that operation, he had placed the accused under surveillance for a considerable period of time and the reports he received from the field operatives were to the effect that every Saturday at around 8.00 pm the accused would meet [Redacted] at that location in Kisugu-Muyenga. Three days prior to that operation, the accused had been arrested on 25th September, 2013 at 4.00 pm at the ESO gate and on being searched the document (exhibit P. ID.2) was recovered from him. P.W.5 D/AIP Bonny Rwantare testified that he was present during the operation at Kisugu-Muyenga, and made the video recording (exhibit P. Ex.4).

It is generally acceptable for the police to engage in deception to try to catch persons who are committing crimes. A sting operation, for example where an undercover law enforcement officer, detective, or co-operative member of the public plays a role as criminal partner or potential victim and goes along with a suspect's actions to gather evidence of the suspect's wrongdoing, is a an acceptable deceptive operation designed to catch a person committing a crime. On the other entrapment is the practice whereby a law enforcement officer induces a person to commit a criminal offense that the person would have otherwise been unlikely or unwilling to commit, except for the trickery, persuasion or fraud of the officer. As a matter of principle, evidence which is obtained improperly or even unlawfully remains admissible, subject to the power of the trial judge to exclude it in the exercise of his common law discretion, for example where the evidence is obtained under duress or Police incitement. The rule against accepting evidence obtained under duress originated in the principle expressed as "*nemo debet prodere se ipsum*," "*nemo tenetur se ipsum accusare*," or "*nemo tenetur prodere seipsum*," i.e. the right against self incrimination (see *Regina v. Sang [1980] AC 402, [1979] 3 WLR 263, [1979] 2 All ER 1222, (1979) 69 Cr App R 282*).

Police incitement occurs where the law enforcement officers involved do not confine themselves to investigating criminal activity in an essentially passive manner, but exert such an influence on the subject as to incite the commission of an offence that would otherwise not have been committed. To determine whether or not the conduct in issue crossed the line, the court considers whether or not the police did more than present the accused with an unexceptional opportunity to commit a crime. When entrapment occurs, then evidence obtained by those means may be excluded as being unfair (see *R v. Foulder [1973] Crim LR 45*; *R v. Burnett [1973] Crim LR 748; R v. Shannon [2001] 1 WLR 51, 68, para 39* and *R v. Ameer [1977] Crim LR 104*), or the proceedings may be discontinued altogether if the conduct of the law enforcement officers was so seriously improper that the administration of justice was brought into disrepute (see *R v. Loosely; Attorney-General's Reference (No.3 of 2000) [2001] All ER (D) 356* and *Sherman v. United States (1957) 356 US 369, 372*). The court has to carry out a balancing exercise between the benefit to the court of having all the evidence available and the consideration of the improper way in which the video evidence was obtained.

The primary question for the court is not whether or not to give approval to the method whereby evidence was obtained. It is whether justice and fairness require that the evidence be admitted. The overriding objective in a criminal trial is that court should deal with a case justly. The position in criminal proceedings now is that when evidence is wrongly obtained the court will consider whether it adversely affects the fairness of the proceedings and, if it does, may exclude the evidence. Of these two remedies, the exclusion of evidence at the trial rather than the grant of a stay, should normally be regarded as the appropriate response in a case of entrapment. I find that when the law enforcement officers took the accused out of custody, handed to him the document (P. ID.2), drove him to the scene in Kisugu-Muyenga, he was not acting on his own volition. The law enforcement officers did not merely present the accused with an unexceptional opportunity to commit a crime but instead they exerted such an influence on him as to incite the commission of an offence that would otherwise not have been committed. The video recording (exhibit P. Ex.4) made at Kisugu-Muyenga on 28th September, 2013 tendered by P.W.5 D/AIP Bonny Rwantare is accordingly rejected and excluded.

Exclusion of such evidence from the trial will often have the same result in practice as an order staying the proceedings. Without, for instance, the evidence of the undercover police officers the prosecution will often be unable to proceed. But this is not necessarily so. There may be real evidence, or evidence of other witnesses. In the instant case there is the letter of apology to the President dated 8th October, 2013 (exhibit P. Ex.7) and a confession obtained from the accused and recorded by P.W.4 D/AIP Mawa Emmanuel which was admitted in evidence as P. Ex.5. At the hearing, the accused retracted both the letter of apology and the confession. The law regarding retracted confessions is that it a matter of practice or prudence for the trial court to direct itself that it is dangerous to act upon a statement which has been retracted in the absence of corroboration in some material particular, but that the court might do so if it is fully satisfied in the circumstances of the case that the confession must be true (*Tuwamoi v. Uganda [1967] EA 84*). There is also the letter of apology dated 26th September, 2013 (exhibit P. Ex.7) in which he requested His Excellency the President for forgiveness for having leaked State secrets and promised never to do it again.

Possible corroboration of the confession and the apology may be found in the fact that in his defence, the accused admitted having leaked to a field officer, a document relating to unpaid ESO staff gratuity earlier that month, with the intention that it is brought to the attention of His Excellency, the President. P.W.2 [Redacted], the then Director of Administration and Finance, ESO confirmed this when he testified that within 30 minutes of the accused photocopying a document relating to unpaid gratuity, it had leaked to the Auditor General. That the accused had leaked a document before would suggest that he had the propensity to breach restrictions on communication of classified information.

This in law is regarded as "similar fact evidence." It is evidence pertaining to similar conduct of the accused on other occasions or of the commission by the accused of similar offences. Similar fact evidence in its strict sense refers to evidence which reveals that on another occasion, the accused acted in a particular way in a particular situation, which is tendered to prove that the accused acted in similar way on the occasion in question. It is essentially evidence of propensity. Subject to a few exceptions, evidence which is adduced solely to show that the accused is the sort of person likely to have committed an offence is, as a rule, inadmissible. The underlying rationale for the rule excluding similar fact evidence is that to allow it in every instance is to risk the conviction of an accused not on the evidence relating to the facts but because of past behaviours or disposition towards crime.

Whether the evidence in question constitutes an exception to this general rule depends on whether the probative value of the proposed evidence outweighs its prejudicial effect (see *Makin v. Attorney General for New South Wales [1894] AC 57; Mohammed Said Akraby v. R. [1956] 23 EACA 512* and). Admissible similar facts evidence falls into three categories which depend on what it is directed towards.; (i) to establish state of mind with which some act proved to have been done was done i.e. what motivated the act; (ii) to prove the identity of the perpetrator or doer of an act; or (iii) to establish the commission of the act itself and therefore rule out an act of nature or miracle.

For such evidence to be admissible, there has to be substantial connection or similarity of what the person did. It is not competent for the prosecution to adduce evidence tending to show that

the accused has been guilty of criminal acts other than those covered by the indictment for the purpose of leading to the conclusion that the accused is a person likely from his criminal conduct / character to have committed the offence for which he is being tried. On the other hand, the mere fact that the evidence adduced tends to show the commission of other crimes does not render it inadmissible if it be relevant to an issue before the court and it may be so relevant if it bears upon the question whether the acts alleged to constitute the crime charged in the indictment were designed or accidental or to rebut a defence which would otherwise be open to the accused.

Similar fact evidence is admissible "when there is a question whether an act was accidental or intentional, or done with a particular knowledge or intention" i.e. where evidence it is overwhelming that the accused committed the crime but it is not clear what his state of mind was (see section 14 of *The Evidence Act*). It is under those circumstances that the fact that such act formed part of a series of similar occurrences, in each of which the accused was concerned, that similar fact evidence becomes relevant (see *R v. Bond [1969] 2 K.B. 389* and The *R v. Harold Whip and Another (1955) 28 KLR*). Furthermore, probative value is not provided by mere repetition of similar facts. There has to be some features in the evidence sought to be adduced which provided an underlying link. The existence of such a link is not to be inferred from mere similarity of facts which are themselves so common place that they can provide no sure ground for saying that they point to the commission by the accused of the offence under consideration (see *R v. Scarrot [1978] 1 ALL ER 672*). The similarity would have to be so unique or striking that common sense makes it inexplicable on the basis of coincidence (see *Regina v. Boardman, [1975] AC 421; [1974] 3 All ER 887; (1975) 60 Cr App R 165; [1974] 3 WLR 673*).

Similar fact evidence relating solely to disposition may not be admissible to prove guilt. Because similar fact evidence is admitted on the basis of an objective improbability of coincidence, the evidence necessarily derives its probative value from the degree of similarity with the acts under consideration. The probative power of the similar fact evidence is derived from the improbability of the strikingly similar facts having any rational explanation other than the guilt of the accused. The acts compared must be so unusually and strikingly similar that such similarities could not be attributed to coincidence. There must be sufficient similarity to constitute a unique trademark or signature or a number of significant similarities.

Having compared the leak involving false accounting in staff gratuity payments and the one charged in the two counts, I find wide disparities. Although in both situations disclosure would be driven by personal interest, in the former the leak was to a filed operative, hence within the organisation itself, while in the latter it is alleged to be to persons outside the organisation. He complained to the system itself and not outside it. While both counts relate to classified information, the leak involving staff gratuity relates to unclassified information. The facts are not so strikingly similar as to have no other rational explanation other than the guilt of the accused. Being mere evidence of propensity, it cannot be used to corroborate the confession. I therefore have not found independent evidence to corroborate the letter of apology and the confession.

Although it is trite that the court might rely on a retracted confession even without corroboration, if fully satisfied in the circumstances of the case that the confession must be true, I have found exhibit P. Ex.5 to be unreliable in a fundamental aspect. In his charge and caution statement recorded by P.W.7 D/AIP Makhoha Thomson, (exhibit P. Ex.5 dated 9th October, 2013), the accused stated that "I passed the information to [Redacted] and to [Redacted], both of [Redacted] Nationality. I started in the year 2009 with one [Redacted] whose term at [Redacted] Embassy ended around 2010. When [Redacted] took over, he was introduced to me by [Redacted] so that I continue passing the intelligence information to him... I was arrested yesterday 25th September, 2013 when I had gone to deliver a message to [Redacted]," (alias P.W.3 [Redacted]).

Had this statement been true, considering that it was recorded on 9th October, 2013 reference to "yesterday 25th September, 2013" is clearly erroneous since the previous day was 8th October, 2013. The disparity in dates of more than a week points to deliberate falsehood rather than mistake. Moreover, the Investigating Officer P.W.6 D/ASP Mutabaazi John Bosco never inquired into the circumstances before and leading to the arrest of the accused on 28th September, 2013. The defence raised by the accused has consequently cast a reasonable doubt on his guilt.

In the two counts, the accused is alleged to have unlawfully disclosed weekly briefs plus weekly intelligence briefs to His Excellency the President of Uganda, to a one [Redacted], a [Redacted] Diplomat who is an unauthorised person. The only distinction is that whereas in Count one the

period in question is between the year 2009 and 2010, in Count two, the period is between the year 2010 and 28th September, 2013. In both counts, the offence is alleged to have been committed at the External Security Organisation Headquarters in Nakasero. The allegations made in Count one are in essence based on the retracted apology letter and confession, both of which I have no independent evidence to corroborate them, yet they are not reliable as true statements. The allegations made in Count one are in essence based on evidence obtained by entrapment. Whereas the person to whom the information is alleged to have been disclosed is named as a one [Redacted], a [Redacted] Diplomat, the evidence adduced in the video recording during the operation of 28th September, 2013 at Kisugu-Muyenga (exhibit P. Ex.4), is identified as a one [Redacted], another [Redacted] Diplomat. Not only is the evidence adduced in respect of this count inconsistent with the particulars of the offence stated in the indictment, but it has been rejected for violating the fundamental principles of justice.

The alternative would be the minor cognate offence of Attempted Unlawful Disclosure of information C/s 10 (1) and (2) of *The Security Organisations Act* and section 386 and129 (1) of *The Penal Code Act*, based on the testimony of P.W.3 [Redacted] to the effect that the accused had been under surveillance for a considerable period of time before he was arrested on 25th September, 2013 at 4.00 pm at the ESO gate, whereupon being searched, the document P. ID.2 was recovered from him. An attempt to commit a crime consists of two elements; (i) an intent to engage in crime; and (ii) conduct constituting a substantial step towards commission of the crime. However evidence relating to this too is unsatisfactory. P. ID.2 was never exhibited in evidence. It was never marked at the point of recovery and neither was a search certificate prepared. The Organisation had the capacity to adduce real evidence of the alleged surveillance before the arrest and the actual arrest at the gate. Failure to do so invokes an adverse inference against the prosecution in light of the version by the accused that he was arrested from the office of P.W.3 [Redacted] while on official errand and not at the gate.

In the final result, I find that the prosecution has not proved any of the two counts against the accused beyond reasonable doubt and I hereby acquit the accused for the offence of Unlawful Disclosure of information C/s 10 (1) and (2) (b) of *The Security Organisations Act*, on each of

the two counts. He should be set free forthwith unless he is being held in custody for other lawful reasons.

Dated at Kampala this 8th day of February, 2019.

Stephen Mubiru

Judge

8th February, 2019.