CONSENT SEARCHES AND SEIZURES IN E-ENVIRONMENT AND THE CONSEQENCES OF COVERTLY OBTAINED EVIDENCE UNDER CAMEROONIAN LAW

By ***Patricia Asongwe Ngeminang***

ABSTRACT

Given the huge amount of information stored on computers and archived in documentary records, the potential for governmental abuse is deeply troubling. This article evaluates Consent electronic searches and seizures under the Cameroonian law and the consequences of covertly gathered evidence . Information gathered from books, journals, and internet, together with consultation and observations on the subject reveal that advances in technology and the use of lengthy, legalistic privacy policies have too often served to make consent nothing more than illusory. Given that reasonable consent is an essential element for the collection, use and disclosure of personal information,. this article proposes consent should remain central, but flexible to breathe life into the conventional ways in which consent is obtained under Cameroon's Conventional laws. The alternative standard of macro reasonableness for consensual searches is going to balance the interests of law enforcement against individual liberty and privacy .

The article provides a blueprint for a workable, comprehensive mechanism for consent search and seizures in the digital environment;

Keywords: Consent, electronic, search and seizures, Cameroon

INTRODUCTION

Multiple writers have estimated that consent searches comprise more than 90% of all warrantless searches by police,[i] and that they are "unquestionably" the largest source of searches conducted without suspicion.[ii] .Agents may search a place or object without a warrant or even probable cause if a person with authority has voluntarily consented to the search. Whether consent was voluntarily given is a question of fact that the court must decide by considering the totality of the circumstances.[iii] Therefore while no single aspect controls the

ISSN 2581 3382

result, the Cameroonian Law seem to rely on factors like: the age, education, intelligence, physical and mental condition of the person giving consent; and whether the person was under coercion. The burden of proving that consent was voluntary lies on the investigating agent.[iv]

This focus on the coerciveness of the police conduct, and its subsequent impact upon volition, is not the same standard of reasonableness that is the touchstone in an electronic environment. In this era of "Internet of Things."[v] the constitutional language protecting "persons, houses, papers, and effects" from unreasonable searches and seizures must confront this change. -The subject matter of an offence may be in a digital form. The changing notions of document to include digital information and other virtual products, and electronically carried out services require changes in definitions and paradigms. Although through the premise of the consent-search doctrine, people are free to decline, the reality is that nearly everyone "consents,"5 In many cases, investigators may seize electronic devices without a warrant, but must obtain a warrant in order to conduct a search on the device(s). Multiple warrants may need to be obtained if a particular device is connected to multiple crimes. Technology and techniques frequently change and may cause existing legislation to be inadequate or obsolete. Hence, as far as possible, electronic consent laws should be drafted in a technologically (and technique) neutral manner as possible. Otherwise the only alternative is to be alert to the requirement for constant and evolving natures of evidence : This article examines consent search and seizure, assesses Cameroon's laws on the subject , appreciate the nature of consent , explain the implications of covertly obtained evidence, The article ends with an appraisal and some proposal for effective electronic consent searches and seizures in Cameroon.

UNDERSTANDING CONSENT SEARCH AND SEIZURES

Consent searches are the most common form of warrantless searches. A search warrant or probable cause is not necessary if consent is given by someone with proper authority.

A consent search assumes the individual, whose person or property is being searched, is aware that they have the right to refuse a search in a situation when confronted by law enforcement agents. By giving consent they are assumed to waive, freely and voluntarily, his or her constitutional rights, granting the officer permission to perform the search. Where consent is obtained through "deception" on the part of the police officer, the search may be determined to be an unreasonable search in violation of the Constitution.

ISSN 2581 3382

No warrant, probable cause or reasonable suspicion is required to perform a search if a person, or someone else with the proper authority, consents to a search.

A consent search assumes the individual, whose person or property is being searched, is aware that they have the right to refuse a search in a situation when confronted by law enforcement agents. By giving consent they are assumed to waive, freely and voluntarily, his or her Constitutional rights rights, granting the officer permission to perform the search. Where consent is obtained through "deception" on the part of the police officer, the search may be determined to be an unreasonable search in violation of the Constitution.

The person has the right to refuse to give consent, and except in limited cases may revoke consent at any point during the search. In addition, the prosecution in any trial using the search results as evidence is required to prove that the consent was voluntary and not a result of coercion.[vi]

According, consent searches have the following features:

- Consent searches are permitted without warrant or exigent circumstance as long as it is 'reasonable' in how consent obtained and the scope of the search undertaken.
- Government "has burden of proving that necessary consent was obtained and that it was freely and voluntarily given, and not the result of duress or coercion, express or implied."
- Showing a mere acquiescence or "submission to a show of authority" does not satisfy burden.
- 'Totality of circumstances' test applied to determine whether proper consent given..
- Officers are not required to inform citizens of their right to refuse permission or to leave scene of interaction with police…but it is part of 'totality' of the circumstances court should consider.
- The scope of the search permitted is determined by applying the 'objective reasonableness test': "What would the typical reasonable person have understood by the exchange between the officer and the suspect."
- Common authority to consent to search – By sharing control over a place or object, a person assumes the risk that the other person will allow the government to search it.

ISSN 2581 3382

- Apparent authority—Consent may be valid if the police reasonably believe the third party granting permission to search actually had authority, even if after the search it is proven he/she *did not have such authority.*
- Third parties may give consent in limited cases. The person granting consent must have common authority over the premises in order for the search to be valid.
- Once a consent search has started, the person whose property is being searched may, at any time, revoke his or her consent.
- Consent may be revoked by comments or actions; for example, saying 'I want you to stop,' or attempting to retrieve property from the officer has been found by the courts to be a valid withdrawal of consent.
- It is important to note that withdrawal of consent must be clearly stated; expressing dislike or impatience is not enough to revoke consent
- There are two exceptions where consent may not be revoked once a search has begun. These include airport screenings and searches of prison visitors. The courts have stated that allowing people to revoke consent during these situations would have a negative impact.

CONSENT SEARCH AND SEIZURES UNDER CAMEROONIAN LAWS

Consent search and seizure is not a new concept under Cameroonian law.

Accordingly, the Cameroon Constitution[vii] in its Preamble provides the following:

- No search may be conducted except by virtue of the law;
- the privacy of all correspondence is inviolate. No interference may be allowed except by virtue of decisions emanating from the Judicial Power;
- no person may be compelled to do what the law does not prescribe

Implicit in the above provisions is that the Cameroon's constitution protects a citizen from being forced to give the government self-incriminating testimony.[viii] In cases where the police do not have a search warrant, searches may take place only with the explicit consent of the person being searched. In this regard, Section 94 of the Criminal Procedure Code [ix]states that:

1. In the absence of a search warrant, searches, and seizures of exhibits may be carried
2. out only with the consent of the occupant or of the person in possession of the objects to be seized.

ISSN 2581 3382

3. The consent shall be a written declaration signed by the person concerned, and if he cannot sign he shall make a thumb-print at the bottom of the declaration.
4. The consent of the person concerned shall be valid only if he had been informed before hand by the judicial police officer of his right to object to the search.[x]

Section 3 further states **;**

(1) The sanction against the infringement of any rule of criminal procedure shall be an absolute nullity when it is:
   (a) Prejudicial to the rights of the defence as defined by legal provisions in force;
   (b) Contrary to public policy.
(2) Nullity as referred to subsection (1) of this section shall not be overlook be raised at any stage of the criminal proceedings by any of the parties and shall be raised by the trial court of its own motion.

According to section 4:

(1) The case of infringement other than those provided for in section 3 shall result in relative nullity
(2) Cases of relative nullity shall be raised by the parties in limine litis before trial court. It shall not be considered after this stage of proceedings.

Section 5**:** states that any document rejected by a decision of the court shall be withdrawn from the case file and med in the registry.

It shall be forbidden to obtain information from the document withdrawn for use against the person concerned and under pain of civil action in damages.

Accordingly, in the Bamenda, case of chief Forbah Mac-Donald Sama,[xi] the accused was charged with five counts of:

(i) Causing a row in the Bamenda western court of appeal contrary to section 154(a) of the penal code,
(ii) Destroying physical evidence viz letter No. CC/71/A/148 of 30 December 1958 of senior divisional officer, Thompson addressed to the defendant by chewing the said letter already tendered in court as an exhibit. Contrary to section 164(1) (c) of the penal code,

ISSN 2581 3382

(iii) Destroyed a document, namely the exhibit and thereby offended section 168(1) of the penal code,

(iv) Assaulted Lucas Fondo, causing him inability to work lasting 15days contrary to section 281 of the penal code.

(v) Assaulted a public servant viz Clement Fru, the court Messenger attached to Bamenda Western Court of Appeal and thereby offended against 156(1) of the Penal Code.

As soon as the judgement had been delivered, the defendant walked to the court table, collected his file and the four documents tendered and began to chew them particularly Mr. Thompson's letter. As the police arrived, the defendant removed from his mouth the chewed documents and threw them over the window. He was then charged to court, but the magistrate convicted him of counts i, ii, iii and iv, and discharged and acquitted him of counts ii and v. on appeal, it was held that the destruction or concealment of exhibit must be during the pendency of a judicial proceeding, and that the court was not in session for count one to mature. He was only confirmed for the conviction in count a state affair to which self-defence was an absolute defence.

The facts of the Mac-Donald case had arisen in Nigeria[xii] and there the defendant was suspected of having swallowed a forged bank note. In order to recover the note the police took him to a doctor under whom he underwent extremely drastic treatment by means of emetics, purges and enemas. Commenting on this procedure the court said:

"In cases like this it would be wise as well as humane to get the patient's consent before treating him, and to get it in writing".

All searches, arrests, detentions and prosecutions are guaranteed in the constitution and under our existing Criminal Procedure Code.[xiii] ..

As per section 54, searches and seizures shall be carried out in accordance with the provisions of the Criminal Procedure Code, taking into account the loss of validity of evidence.

Accordingly, the Cyber Code is using the text of the conventional procedural laws to craft a comprehensive set of rules regulating law enforcement.[xiv] However, the conventional law on consent search may be inadequate in the digital environment .

ISSN 2581 3382

Accordingly, the abuse of technology such as the use of surreptitious electronic means with the intention of obtaining information without the knowledge or consent of the originator should constitute an offence irrespective of the ultimate goal or motive such as financial gain.[xv]

Thus the textual requirement that searches and seizures must above all else be "reasonable" has permitted the courts to craft a set of rules that balances law enforcement needs with individual interests in the deterrence of abusive law enforcement practices.[xvi] For example, it is a good practice for investigators to use written consent forms that state explicitly that the scope of consent includes consent to search computers and other electronic storage devices.[xvii] However, since the decisions evaluating the scope of consent to search computers have reached sometimes unpredictable results, investigators should indicate the scope of the search explicitly when obtaining a suspect's consent to search a computer.

Accordingly, section 42 of the Cyber Code

In computer crime cases, two consent issues often arise. First, when does a search exceed the scope of consent? For example, when a target consents to the search of a machine, to what extent does the consent authorise the retrieval of information stored in the machine? Second, who is the proper party to consent to a search? Courts have generally accepted that A police officer cannot force or threaten you into giving up your password or unlocking your electronic devices.

THE SCOPE OF THE ELECTRONIC CONSENT SEARCH IN CAMEROON

The scope of consent to search and seize in computer crimes is generally defined by its expressed object, and is limited by the breadth of the consent given.[xviii] This means that the standard for measuring the scope of consent under the law is objective reasonableness: What would the typical reasonable person have understood by the exchange between the agent and the person granting consent? This requires a fact-intensive inquiry into whether it was reasonable for the agent to believe that the scope of consent included the items searched of course, when the limits of the consent are clearly given, either before or during the search, agents must respect these bounds. The scope of consent surrounds the area that the person is allowing to be searched. The permitted scope of consent searches depends on the facts of each case. However, investigators should be especially careful about relying on consent as the basis for a search of a computer when they obtain consent for one reason when they wish to conduct a search for another reason. For instance, in the case of Go-Bart Importing Company v. united States,[xix] the Court of Appeal suppressed images of child pornography found on computers

ISSN 2581 3382

after agents procured the defendant's consent to search his property for other evidence. In another case [xx] detectives searching for physical evidence of an attempted sexual assault obtained written consent from the victim's neighbour to search the neighbour's premises and personal property. Before the neighbour signed the consent form, the detectives discovered a large knife and blood stains in his apartment, and explained to him that they were looking for more evidence of the assault that the suspect might have left behind. While several agents searched for physical evidence, one detective searched the contents of the neighbour's personal computer and discovered stored images of child pornography. The neighbour was charged with possessing child pornography. On interlocutory appeal, the First Circuit held that the search of the computer exceeded the scope of consent and suppressed the evidence. According to the Court, the detectives' statements that they were looking for signs of the assault limited the scope of consent to the kind of physical evidence that an intruder might have left behind. By transforming the search for physical evidence into a search for computer files, the detective had exceeded the scope of consent. Where agents exceeds scope of consent by searching computer after defendant signed broadly-worded written consent form after the investigator told defendant that they were looking for drugs and drug-related items rather than computer files containing child pornography.

Because the decisions evaluating the scope of consent to search computers have reached sometimes unpredictable results, investigators should indicate the scope of the search explicitly when obtaining a suspect's consent to search a computer. Written consent forms can be beneficial in proving that consent was voluntarily given and can help demonstrate consent to search a premises, personal property, computer, or electronic devices. Consent may also be limited implicitly.

The scope of consent to search and seize in computer crimes is generally defined by its expressed object, and is limited by the breadth of the consent given.[xxi] This means that the standard for measuring the scope of consent under the law is objective reasonableness:[xxii] What would the typical reasonable person have understood by the exchange between the agent and the person granting consent? This requires a fact-intensive inquiry into whether it was reasonable for the agent to believe that the scope of consent included the items searched of course, when the limits of the consent are clearly given, either before or during the search, agents must respect these bounds. The permitted scope of consent searches depends on the facts of each case.[xxiii]

ISSN 2581 3382

ATHORITIES TO GIVE ELECTRONIC CONSENT

Third Party Consent

It is common for several people to use or own the same computer equipment. If any one of those people gives permission to search for data, agents may generally rely on that consent, so long as the person has authority over the computer. In such cases, all users have assumed the risk that a co-user might discover everything in the computer, and might also permit law enforcement to search this common area as well.

The watershed case in this area is United States v. Matlock,[xxiv] in which the Supreme Court stated that one who has "common authority" over premises or effects may consent to a search even if an absent co-user objects. According to the Court, the right of third-party consent requires mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognise that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched. Thus under the Matlock approach, a private third party may consent to a search of property under the third party's joint access or control. The third party consent rule often requires investigators to inquire into third party's rights of access before conducting a consent search, and to draw lines between those areas that fall within the third party's common authority and those areas outside of the third party's control .Co-users of a computer will generally have the ability to consent to a search of files. A woman can consent to a search of her boyfriend's computer located in their house, and noting that the boyfriend had not password-protected his files.[xxv] However, when an individual protects his files with passwords and has not shared the passwords with others who also use the computer, the authority of those other users to consent to search of the computer will not extend to the password-protected file.[xxvi] Conversely, if the co-user has been given the password by the suspect, then she probably has the requisite common authority to consent to a search of the files.

An employee can consent to a search of an employer's computer locked in a warehouse because the employee possesses the key, and finding "special significance" in the fact that the employer had himself delivered the key to the employee.[xxvii]

Evidence obtained during a consent search is not automatically suppressed when it is discovered that the third party who consented to the search lacked the authority to do so. Instead, agents can rely on a claim of authority to consent if based on the facts available to the

ISSN 2581 3382

officer at the moment, a man of reasonable caution would believe that the consenting party had authority to consent to a search of the premises. When agents reasonably rely on apparent authority to consent, the resulting search does not violate the law[xxviii].

The ability of minors to provide meaningful consent for the sharing of their personal information depends greatly on their cognitive and emotional development.[xxix] Given the difficulties that adults have in understanding what is happening with their personal information in a complex environment, it would be unrealistic to expect children to fully appreciate the complexities and potential risks of sharing their personal information. In recognition of this, private sector privacy legislation allows for consent through an authorized person, such as a parent or legal guardian.

Partner and Spouses

A woman can consent to a search of her boyfriend's computer located in their house, and noting that the boyfriend had not password-protected his files.[xxx] However, when an individual protects his files with passwords and has not shared the passwords with others who also use the computer, the authority of those other users to consent to search of the computer will not extend to the password-protected file.[xxxi] Conversely, if the co-user has been given the password by the suspect, then she probably has the requisite common authority to consent to a search of the files.

Most spousal consent searches are valid.[xxxii]In the absence of an affirmative showing that the consenting spouse has no access to the property searched, courts generally hold that either spouse may consent to search all of the couple's property. For example, in United States v. Smith[xxxiii], a man named Smith was living with a woman named Ushman and her two daughters. When allegations of child molestation were raised against Smith, Ushman consented to the search of his computer, which was located in the house in an alcove connected to the master bedroom. Although Ushman used Smith's computer only rarely, the district court held that she could consent to the search of Smith's computer. Because Ushman was not prohibited from entering the alcove and Smith had not password-protected the computer, the court reasoned she had authority to consent to the search. Even if she lacked actual authority to consent, the court added, she had apparent authority to consent.[xxxiv]

Parents

ISSN 2581 3382

Parents can consent to searches of their children's rooms when the children are minors.[xxxv] Therefore if the children attend maturity the parents may or may not be able to consent, depending on the facts. In some computer crime cases, the perpetrators are relatively young and reside with their parents. When the perpetrator is a minor, parental consent to search the perpetrator's property and living space will be valid.[xxxvi]

When the sons and daughters who reside with their parents are legal adults, however, the issue is more complicated. However, it is clear that parents may consent to a search of common areas in the family home regardless of the perpetrator's age.[xxxvii] Parents' authority to consent to search an adult's room can be rebutted as this is a base on the surrounding circumstances of each case. Although courts have offered divergent approaches, they have paid particular attention to three factors: the suspect's age; whether the suspect pays rent; and whether the suspect has taken affirmative steps to deny his or her parents access to the suspect's room or private area. When suspects are older, pay rent, and/or deny access to parents, courts have generally held that parents may not consent. In United States v. Durham,[xxxviii] a mother had neither apparent nor actual authority to consent to search of a 24-year-old son's room, because the son had changed the locks to the room without telling his mother, and the son also paid rent for the room. In contrast, parents usually may consent if their adult children do not pay rent, are fairly young, and have taken no steps to deny their parents access to the space to be searched.

Consent In Workplace Searches

Warrantless workplace searches occur often in computer cases and raise unusual complicated legal issues. Thus, every warrant less workplace search must be evaluated carefully on its facts. The legality of warrant less workplace searches depends on often-subtle factual distinctions such as whether the workplace is a public sector or private sector; whether employment policies exist that authorise a search, and whether the search is work-related.[xxxix] Furthermore, government, employers and supervisors can conduct reasonable work-related searches of employee workplaces without a warrant even if the searches do not violate employees' reasonable expectation of privacy.

Consent in Private Sector-Workplaces

Although most non-government workplaces will support a reasonable expectation of privacy from a law enforcement search, investigators can defeat this expectation by obtaining the consent of a party who exercises common authority over the area searched. In practice, this

ISSN 2581 3382

means that investigators can often overcome the warrant requirement by obtaining the consent of the target's employer or supervisor. Depending on these facts, a co-worker's consent may suffice as well.[xl]

Private-sector employers and supervisors generally enjoy a broad authority to consent to searches in the workplace. This implies that a general contractor's superintendent could consent to an inspection of the electronic data of an entire construction site, including subcontractor's work area.[xli]

Warrantless workplace searches by private employers rarely violate the privacy law. So long as the employer is not acting as an instrument or agent of the Government at the time of the search, the search is a private search and does not violate the law[xlii].

Public-Sector Workplace Searches

Although warrant less computer searches in private-sector workplaces follow familiar rules, public-sector workplace searches of computers presents a different matter. In public (that is, government) workplaces, officers cannot rely on an employer's consent, but can conduct searches if written employment policies or office practices establish that the government employees targeted by the search cannot reasonably expect privacy in their workplace. Accordingly, a government employee can enjoy a reasonable expectation of privacy in his workplace. However, an expectation of privacy becomes unreasonable if actual office practices and procedures, or legitimate regulation permit the employee's supervisor, co-workers, or the public to enter the employee's workspace.

Written employment policies and banners are particularly important in cases that consider whether government employees enjoy a reasonable expectation of privacy in government computers. Banners are written notices that greet users before they log on to a computer or computer network, and can inform users of the privacy rights that they do or do not retain in their use of the computer or network. In general, government employees who are notified that their employer has retained rights to access or inspect information stored on the employer's computers can have no reasonable expectation of privacy in the information stored there.[xliii]

REASONABLE WORKPLACE SEARCHES UNDER O'CONNOR V. ORTEGA[xliv]

ISSN 2581 3382

Government employers and their agents can conduct reasonable work-related searches even if those searches violate an employee's reasonable expectation of privacy. In most circumstances, a warrant must be obtained before a government actor can conduct a search that violates an individual's reasonable expectation of privacy. In the context of government employment, however, the government's role as an employer (as opposed to its role as a law-enforcer) presents a special case. In O'Connor, the Supreme Court held that a public employer or the employer's agent can conduct a workplace search that violates a public employee's reasonable expectation of privacy. So long as the search is reasonable its decision adds public workplace searches by employers to the list of special need exceptions to the warrant requirement. The special needs exceptions permit the government to dispense with the usual warrant requirement when its officials infringe upon protected privacy rights in the course of acting in a non-law enforcement capacity, The need for government officials to pursue legitimate non-law-enforcement aims justifies a relaxing of the warrant requirement because the burden of obtaining a warrant is likely to frustrate the non-law-enforcement governmental purpose behind the search.

Therefore a warrant less search satisfies two requirements to qualify as reasonable. First, the employer or his agents must participate in the search for a work-related reason, rather than merely to obtain evidence for use in criminal proceedings. Second, the search must be justified at its inception and permissible in its scope. The requirements under O'conner v. Ortega revisited.

The Search Must Be Work-Related

The first element of reasonableness test requires that the employer or his agents must participate in the search for a work-related reason, rather than merely to obtain evidence for use in criminal proceedings.[xlv] This element limits the exception to circumstances in which the government actors who conduct the search act in their capacity as employers, rather than law enforcers. The law provides for two such circumstances. First, that the public employers can conduct reasonable work-related but no investigatory intrusions, such as entering an employee's office to retrieve a file or report while the employee is out. Second, that the employers can conduct reasonable investigations into an employee's work-related misconduct, such as entering an employee's office to investigate employee misfeasance that threatens the efficient and proper operation of the office.

ISSN 2581 3382

Therefore the line between a legitimate work-related search and an illegitimate search for criminal evidence is clear in theory, but often blurry in fact. Public employers who learn of misconduct at work may investigate it with dual motives: they may seek evidence both to root out inefficiency, incompetence, mismanagement, or other work-related misfeasance, and also to collect evidence for a criminal prosecution. Indeed, the two categories may merge altogether. For example, government officials who have criminal investigators under their command may respond to allegations of work-related misconduct by directing the investigators to search employee offices for evidence of a crime.

The Search Must Be Justified at Its Inception and Permissible in Its Scope

To be reasonable a work-related employer search must also be both justified at its inception and permissible in its scope.[xlvi] A search will be justified at its inception when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a no investigatory work-related purpose. A search will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and are not excessively intrusive in light of the nature of the misconduct. If employers conduct a search that unreasonably exceeds the scope necessary to pursue the employer's legitimate work-related objectives, the search will be unreasonable and will violate the law.[xlvii]The bottom line of this is that a general and unbounded search of an employee's computer, desk, cabinets, and personal papers is impermissible.

Consent in Public-Sector Workplaces

Although public employers may search employee's workplaces without a warrant for work-related reasons, public workplaces offer a more restrictive milieu in one respect; in government workplaces, employers acting in their official capacity generally cannot consent to a law enforcement search of other employees' computer.[xlviii]The rationale for this result is that it is not permitted for one government official to consent to a search by another. Operation of a government agency and enforcement of criminal law do not amalgamate to give a right of search beyond the scope of either. Accordingly, law enforcement searches conducted pursuant to a public employer's consent must be evaluated. The question in such cases is not whether the public employer had common authority to consent to the search, but rather whether the combined law enforcement and employer computer search satisfied legal standards.[xlix]

ISSN 2581 3382

Evidence unlawfully obtain cannot be used against defendants in criminal court proceedings is the:

Of course, these search and seizure questions are not limited to computer networks in the workplace. Universities, libraries, and other organizations, both public and private, may operate computer networks on which users store data which they consider private--either partly or completely.

System Administrators' Consent

Case law demonstrates that the courts will examine the totality of the circumstances in determining whether an employee has a reasonable expectation of privacy or whether an employer shares authority over the employee's space and can consent to a search. But applying this employer-consent case law to computer searches can become especially troublesome when the employee's computer is not a stand-alone container, but an account on a large network server. The difficulty is a practical one. In the physical world, individuals often intuitively understand their rights to control physical space and to restrict access by others because they can observe how everyone uses the space. For example, with filing cabinets, employees can see whether they are located in private areas, whether others have access, whether the cabinets are locked, and who has the keys. While explicit company policies certainly help to clarify the situation, employees can physically observe company practices and will probably conclude from their observations that certain property is or is not private.

-By contrast, in an electronic environment, employees cannot "see" when a network administrator, supervisor, or anyone else accesses their data.

They cannot watch the way people behave with data, as they can with a file cabinet, and deduce from their observations the measure of privacy they ought to expect. As a practical matter, system administrators can, and sometimes do, look at data. But when they do, they leave no physical clues which would tell a user they have opened one of his files. Lacking these physical clues, some users who are unfamiliar with computer technology may falsely but honestly believe that their data is completely private. Will the courts hold this false belief to be one that society is prepared to recognize as reasonable? Will the courts still find it reasonable, even when a user knows that there are such people as system administrators who are responsible in some fashion for operating and securing the entire network? If so, do users who actually

ISSN 2581 3382

understand the technology and the scope of a system operator's access to data [page 23] have a lesser expectation of privacy and fewer Fourth Amendment protections than users who are not so well informed? And what happens in the years ahead as our population becomes increasingly computer literate?

Prosecutors who face these issues at trial should be ready to argue that reasonable network users do, indeed, understand the role and power of system operators well enough to expect them to be able to protect and even restore their files. Therefore, absent some guarantees to the contrary, reasonable users will also expect system administrators to be able to access all data on the system. Certainly, if the system has published clear policies about privacy on the network or has even explained to users that its network administrators have oversight responsibility and control, this will support the position that a system operator's consent to a search was valid. But if the network and its users have not addressed these issues and the situation is ambiguous, the safest course will be to get a warrant. (Of course, if the system administrator does have authority to access and produce a user's files and simply will not do it on request, agents should use a subpoena.)

If agents choose to apply for a warrant and are concerned that a target/user will delete his data before they can execute the search, the agents should consider asking a cooperating system operator to make and keep a backup of the target's data, which they can later procure under the warrant or subpoena. The circumstances of each case will dictate the wisest approach, but agents and prosecutors should explore all these questions before they just ask a system administrator to produce a user's files.

-Every computer network is managed by a system administrator or system operator whose job is to keep the network running smoothly, monitor security, and repair the network when problems arise. System operators have access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems. When investigators suspect that a network account contains relevant evidence, they may feel inclined to seek the system administrator’s consent to search the contents of that account.

As a practical matter, the primary barrier to searching a network account pursuant to a system administrator’s consent is statutory, not constitutional. System administrators typically serve as agents of providers of electronic communication service. Accordingly administrator’s consent to search an account must comply with the law in force. To the extent that the law

ISSN 2581 3382

authorises system administrators to consent to searches, the resulting consent searches will in most cases comply with the law.

IMPORTANCE OF CONSENT ELECTRONIC SEARCH ES AND SEIZURES

A search conducted with the consent of the person concerned places a police official in a much better position than a search without consent. It eliminates the procedural burden of proving the existence of reasonable grounds to the search. Working out the appropriate balancing of interests in warrantless search and seizure cases is not always easy, especially since the stakes for both individuals and the state tend to be high.

The first is that the urgency of the situation necessitates an immediate search, despite the absence of judicial authorisation; The second is that there is a minimal level of intrusion caused by the search and therefore minimal violation of privacy. This argument may be linked to the third justification, which is that there is no reasonable expectation of privacy in the circumstances existing at the time.

AN ASSESSMENT OF ELECTRONIC SEARCH CONSENT UNDER CAMEROON LAWS AND THE IMPLICATIONS FOR VOILATING THE RULES OF VOLUNTARINESS

Consent renders a search reasonable whenever it is both voluntary and authoritative. Having a legitimate expectation of privacy in a place and/or thing is a necessary predicate for authority to consent, but it does not always give rise to that level of shared access and control that is essential to a finding of authority to consent to search or seizure. Thus, expectation of privacy is a necessary component in determining the validity of a consent. Mere Acquiescence to a Claim of Lawful Authority Is Not

However, consent is to be determined by considering the 'totality of the circumstances' surrounding the consent and search:[Under the 'totality of circumstances' test, the court must determine what actually occurred between the subject and law enforcement.:

- What was said and done by both the subject and law enforcement officer(s) prior to and during the search.

ISSN 2581 3382

- The personal characteristics of the subject, i.e. age, state of intoxication, education, physical condition, experience with law enforcement, any special vulnerability, any impediment to communication.
- -The degree of force/control demonstrated by law enforcement, i.e. the number of officers, display of weapons, direct or implied threats.

The person has the right to refuse to give consent, and except in limited cases may revoke consent at any point during the search. In addition, the prosecution in any trial using the search results as evidence is required to prove that the consent was voluntary and not a result of coercion.[1]

- (b) The consent must be given voluntarily Where a person consents to the invasion of his or her privacy, the requirements of "reasonable grounds and prior authorisation" do not apply. Waiver of rights is however never lightly inferred. The question of paramount importance then, is whether the consent was validly, that is voluntarily given. The voluntariness of the consent is to be determined from the totality of the circumstances.
- Other indicators of the absence of voluntariness are explicit or implicit threats or shows of force. For a successful reliance on consent the courts have indicated that the following criminal law standards are relevant: the consent must have been given voluntarily; expressly or tacitly; before the otherwise unlawful act is committed; by a person capable of forming a will; while aware of the true and material facts regarding the act consented to; by the person who is going to be harmed. Consent cannot validate an irregular search warrant Section 94 of the Criminal Procedure Code stipulates that consent by the subject of a search and seizure operation can serve to validate such an operation where it is conducted without a search warrant. However, what of those situations where police officials are purportedly acting in terms of an invalid warrant? Can it be argued that the consent of the person concerned would have the effect of validating the warrant or validating a warrantless search?
- it is "trite" law that, if the relevant search warrants were invalid because they had been invalidly issued, no amount of consent or agreement by the subjects of the search could have the effect of rendering them valid or lawful. [li]

ISSN 2581 3382

Voluntariness is a question of fact to be determined from all of the circumstances, mere acquiescence is not consent. The violation of the rules relating electronic consent has implications as indicated below

A Constitutional Implication

The basic human right to privacy is entrenched in section the preamble of the Constitution In concept and principle, the constitutional questions raised by contemporary surveillance technologies have much in common with challenges confronted by our forebears in the late eighteenth century, when the security of the people was threatened by general warrants, and the early twentieth century, when the security of the people was threatened by the growth and expansion of law enforcement agencies.

Cameroon Constitution in its preamble provides for the requirement that individuals should have control over information about themselves is an important aspect of privacy. The deprivation of control over what individuals do and who they are is considered as the "ultimate assault on liberty, personality, and the self." Indeed, self-disclosure is one of the major mechanisms individuals use to regulate their privacy. This notion of privacy reveals its connection to human dignity, to the extent that dignity requires non-exposure.[lii]The disclosure of this information may trigger emotions such as anxiety, fear, and humiliation. Here, the understanding of privacy is based in the intimate sphere, where invaded privacy can lead to dignitary harms such as exposure and shame. Constitutional rights, may be waived, and one may consent to a search of his person or premises by officers who have not complied with the Constitution.

The Constitutional concern with protection of individual privacy can be best satisfied through a careful consideration of the scope, voluntariness and authority of consent, once the purely objective threshold of "standing"(impact on one's protected interests) is crossed. In this regard section 41 of the Cyber Code states that "every individual shall have the right to the protection of their privacy." This section also gives the judges the right to take any protective measures notably, sequestration or seizure to avoid or end the invasion of privacy.[liii] Accordingly, the law provides for the responsibility of content provider for data transmission[liv], forbidding a natural person or corporate body to listen, intercept and store communications and the traffic data related thereto, or to subject them to any other means of interception or monitoring without the consent of the users concerned, save where such person is so authorised legally.[lv]

ISSN 2581 3382

B Judicial Implications

Court required consideration of the totality of the circumstances when evaluating the voluntariness of a consent to search. Because this consideration will assess all facts pointing to genuine, subjective abandonment of protected privacy interests, it is unnecessary to assess expectations of privacy in determining what constitutes a search.

Evidence obtained in conflict with the provisions of section 94 of the Criminal Procedure Code, or in conflict with the Constitution, may still be allowed to be produced in evidence, provided that the trial is not rendered unfair as a result thereof and the admission of such evidence does not cause the administration of justice to come into disrepute.

Thus, as to either of them, the police entry is a "search." Whether the search is lawful, then, depends on whether she has authority to consent.

If apparent authority would render the consent valid, however, as most courts have contended, then the search was lawful. [lvi], quite persuasively, that whether apparent authority may validate consent depends upon one's attitude toward consent searches.

The prosecution is in the best position to say what justified the police conduct For these reasons, it is not only appropriate that the burden first be on the defendant to show that a search occurred, but also that it then shift to the prosecution to show that the search was consented to. [lvii]Although the burden of showing a search remains with the defendant, and the burden of showing consent remains with the government, the outcomes of some cases would change simply because factual issues formerly subsumed in the definition of search would be come factual questions of consent.

Evidence obtained in violation of the Constitution may be inadmissible in court because of the exclusionary rule. Evidence illegally obtained is inadmissible in court. An extension of the exclusionary rule is the fruit of the poisonous tree doctrine. This doctrine states that illegally obtained evidence used to secure further evidence must also be excluded. The burden then shifts to the government to justify the search on the basis of consent. The prosecution is in the best position to say what justified the police conduct. Indeed, in the case of third-party consent, the defendant may not even have been present. Moreover, this allocation with respect to each issue avoids placing the burden of proof on a party to establish the nonexistence of an event. From a policy perspective, the defendant moving to suppress evidence is seeking exclusion of

ISSN 2581 3382

relevant and probative facts and should bear some burden in showing the need for such exclusion. At the same time, the prosecution, in opposing the motion on the basis of consent, is seeking to support a warrantless search[lviii] For these reasons, it is not only appropriate that the burden first be on the defendant to show that a search occurred, but also that it then shift to the prosecution to show that the search was consented to. It is important that distinctions between these issues be carefully drawn and maintained. The Court, however, has insisted that the burden is on the prosecution to prove the voluntariness of the consent[3lix17] and awareness of the right of choice.[318] Reviewing courts must determine on the basis of the totality of the circumstances whether consent has been freely given or has been coerced.

In computer crime cases, several consent issues are likely to arise. Whether consent was voluntarily given is a question of fact which the court will decide

the interest of the citizen to be protected from illegal or irregular invasions of his liberties by the authorities, and the interest of the State to secure that evidence being upon the commission of a crime and necessary to enable justice to be done shall not be withheld from Courts of law on a merely formal or technical ground.'

It also is desirable that the Government should not itself foster and pay for other crimes, when they are the means by which the evidence is to be obtained

Accordingly, three approaches are possible to the problem:

- if evidence is relevant, it cannot be excluded on the ground that it was obtained by illegal action;
- if evidence is obtained by illegal action, it is never admissible;
- where evidence is procured by illegal action, it is a matter for the trial judge to decide, in his discretion, whether to admit it or not, subject, in cases where the evidence is admitted, to review by an appellate court.

The laws usually make an exception for Consent in cases where evidence is seized in a search, that evidence might be rejected by court procedures, such as with a motion to suppress the evidence under the exclusionary rule. The court has complete discretion as to what evidence it will allow to be used in a case. However, when considering whether to allow illegally obtained evidence, the court will balance the need to deter/discourage law breaking against the desire to have all material facts before the court.

ISSN 2581 3382

Covertly obtained evidence (secretly recorded meetings with the defendant) as it demonstrated that the defendant's evidence was false, however to treat such evidence with caution since the party making the recording may seek to manipulate the conversation, leading to statements which could be taken out of context.

Before obtaining / putting forward such evidence the following factors should be considered;

Evidence will not be admissible if it was obtained through torture or inhuman or degrading treatment[lx]

Privileged material will not be admissible in court unless it was created in the course of a criminal act or to further a criminal enterprise.[lxi]

It is a criminal offence to intercept communication between individuals, such as emails and telephone calls, unless you have their permission [lxii].

It is a civil wrong and a criminal offence to persuade someone to disclose personal data (for example a person's name and address) without the "data controller's" consent A security principle states that files should be protected against "human dangers" such as unauthorised access, fraudulent misuse of data or contamination by computer viruses.. A security principle states that files should be protected against "human dangers" such as unauthorised access, fraudulent misuse of data or contamination by computer viruses.[lxiii]

As shown by the above, the risks of using covertly gathered evidence has the potential consequences including harm to the claim and sanctions for the investigating agent themselves. Agents should therefore consider carefully whether the benefits of using such evidence outweigh the risks.[lxiv]

WHERE DO GO FROM HERE?

Since judicial guidance in this area is still limited in Cameroon, investigators seeking and executing search warrant authorising the seizure of computers and computerised information are on untested ground.[lxv] Careful adherence to established constitutional and legal principles, coupled with the use of expert assistance when needed, will enhance the likelihood of obtaining computerised evidence that is judicially admissible. [lxvi] The guiding factors in electronic search and seizures must conform to standard factors like :

ISSN 2581 3382

(1) the duration of the surveillance;
(2) the lowering of structural barriers to pervasive surveillance, reflected in the greatly reduced cost of tracking;
(3) the recording of an individual's or group's movements;
(4) the elicitation of information from within a protected space such as a home; and, as appropriate,
(5) whether the technology undermines core constitutional rights and
(6) whether surveillance technologies are piggy-backed on each other.

Enumerating these factors creates a framework that adds rigor to the constitutional and *judicial inquiry*. Because these factors are technology-neutral, *they* can stand the test of time, rather than being left behind at the next set of innovations." [210]

Another disadvantage of "reasonableness" assessments generally is their inherently inexact nature. In many contexts, the Court has opted for bright-line criminal procedural rules because of their clarity and *predictability.* [lxvii]*Therefore,* for computer-related criminal laws to be truly effective, they must be standard, interoperable and robust Policy.

Further, a sound policy can make the difference between a legal or illegal search.

The policies should explain what happens to seized possessions; define consent searches and note how consent may be obtained and the consequences for failing to *provide specific* rules for *consent.*

Individuals should be made aware of all purposes for which information is collected, used or disclosed. At a minimum, they must be informed of purposes in sufficient detail such as to ensure they meaningfully understand what they are invited to consent to.

These purposes must be described in meaningful language, avoiding vagueness like 'service improvement'.

Also, because of the disconnect many perceive between the standard of "voluntary consent," and the Court's application of it, many scholars this research recommends a robust definition of "voluntariness." For example, numerous scholars have called for a requirement that police notify suspects of their right to decline a request to search and for recognition that coercion is inherent in any police interaction,

ISSN 2581 3382

REFERENCES

[i] *Easttom C.* Computer Crime Investigation and the Law. Oxford University Press *(2010)* .225-230.

[ii] *Walden, I.)* Computer Crimes and Digital Investigations, *Oxford: Oxford University Press (2007) at .112*

[iii] Note section 94 of the Criminal Procedure Code .

[iv] Pollitt, M ''*Digital Evidence in Internet Time'',* in R. Broadhurst (Ed.) Bridging the Gap: A Global Alliance on Transnational Organised Crime, Hong Kong Police: Printing Department HKSAR 32. (2003) at1332-325

[v] *ibid*

[vi] Patricia Asongwe "Cyber security and Challenges of Cyber criminality: Response, Strengths and Weaknesses of Cameroonian Law" Ph .D Dissertation, University of Yaounde II, (Yaounde, 2017) at 421

[vii] The Constitution of 1996 as amended and supplemented by Law No2008/001 of 14 April 2008

[viii]Dibussi Tande 4"Can Cameroon's New Criminal Procedure Code Deliver"Justice with a Human face"? Africa, Cameroon, Justice, (**2007**)

[ix] *Law No 2005/007 of 27 July 2005 on the Criminal Procedure Code of 2005*

[x] *Section 2*

[xi] *BCA/36/78, chief Forbah Mac-Donnal Sama v; The People. Unreported decision of the court of Bqmenda Court of Appeql on the 4th of January 1979*

[xii] Chimicokpu V. Commissioner of Police 1959 N.R.I.L.R. 1 at page 6

[xiii] Asongwe P; supra note 6 at 456

[xiv] *ibid*

[xv] *This is the approach taken in computer crime legislation. See for example, t*

[xvi] *ibid*

[xvii] *Secton 94 of the Criminal Procedure Code*

[xviii] *Michael Yanou; " Criminal Law and Procedure in Cameroon.' Yanou LAW Series 2012 at .225*

[xix]*75 L.Ed. 374 (1931)*

[xx] *United States V. Office Known as 50 State Distrib., 708 F.2d 1371 (9th Cir.1983), Cert. denied, 79Led 2d677 (1984).*

[xxi] *Yanou M; supra note 18 at .229*

[xxii]*Kings v. State ex rel Murdock Acceptance Corporation*, 222 So . 2d 395, 398 (1969)

ISSN 2581 3382

[xxiii] *Yanou M.note 18 at 228*

[xxiv]708 F.2d 1371 (9th Cir.1983), Cert. denied, 79Led 2d677 (1984).

[xxv] Dibssi Tande *supra note 8*

[xxvi]Ibid

[xxvii] See the principle of vicarious liability. However, this principle will hold only when the investigator is acting within authority and in course of his duty.

[xxviii] *Conly C; "Organising For Computer Crimes Investigation and Prosecution" .Washington D.C. U.S Department of Justice. National institute of Justice (1989) at 166-176*

[xxix] Asongwe p; supra note 6 at 465

[xxx] *ibid* .

[xxxi] Ibid at 483

[xxxii] *ibid*

[xxxiii]731 F.2d 1125 (4th Cir. 1994), cert. denied, 86 L Ed2d 130 (1994).

[xxxiv] *Ker v. C*. 831 F.2d 1125 (1997) This rule also applies where the marriage is polygamous

[xxxv]The provision of maturity varies from one country to another.

[xxxvi] Arkin S Prevention and Prosecution of computer and Highway technology crimes New York NY Mathew Bender Books 77, 1(1989). At 120-124

[xxxvii] *Ibid at 125*

[xxxviii]452 U.S.692, 703 (1981)

[xxxix]Jackson, M. Keeping Secret: International Developments to Protect Undisclosed Business Information and Trade Secretes. In Thomas D and Loader B (Eds.), Cyber Crime: Law Enforcement, Security and Surveillance in The Information Age New York: Routledge (2000). at 153-173

[xl] *Ibid at 190*

[xli] *ibid*

[xlii] Coleman C. Supra note 28 al..155

[xliii] *ibid*

[xliv]*774F.2d 402, 407 (1985)*

[xlv] *O'Hara. C et al ;* Fundamentals of Criminal Investigation *6th ed. ISBN 0-398-05889- (1994) at.345*

[xlvi] . Grabosky, P. *Electronic Crime*, New Jersey: Prentice Hall (2006) at 235-236

[xlvii] Marc D "Why The Police Don't Care About Computer Crime"Harvard Journal of Law and Technology .(1997)at 465.

[xlviii] *ibid*

[xlix]*Katayer K;* ''Digital architecture as crime control''.*Yale Law Journal, .(2003*).at *112- 116*

ISSN 2581 3382

[l] *Casey, G* Digital Evidence and Computer Crime . *St. Louis, MO: Elsevier Press.Georgia E (2004) at 187-185.*

[li] *Note section 4 of the Criminal Procedure Code*

[lii] *Kerr O "Searches And Seizures In A Digital World" George Washington University Law School Journal (2006) at 300-302*

[liii] *See section 42 of the Cyber Code*

[liv] *ibid Section 43*

[lv] *Ibid Section 44. (1)*

[lvi] Sarkar, M. C. (2001) Sarkar on Evidence, 15th Ed, Nagpur, Wadhwa & Company,. Vol.I and Vol.II .Sweet & Maxwell at . 337

[lvi] *Walden, I. (2007)* Computer Crimes and Digital Investigations, *Oxford: Oxford University Press.PP.233-236*

[lvii] Yanou M. supra note 18 at 230

[lviii] *ibid*

[lix] *ibid*

[lx] Article 3 of the European Convention on Human Rights

[lxi] *Asongwe P supra note 6 at 480*

[lxii] *Section 65 of the Cyber Code outlaws unauthorized and intentional interception computer data, including electromagnetic emissions, to, from or within a computer system, by technical means.*

[lxiii] See sections 34 and 40 of the Cyber Code

[lxiv] *Kerr O:"Computer Records and the Federal Rules of Evidence" USA Bulletin.*

[lxv] *Asongwe P .supra note 6 at 405-407*

[lxvi] *Yanou M ; supra note 18 at 270*

[lxvii] Blume P "Data Protection" International Review of Computer Law Computers & Technology 2nd ed (1997) at .98

[lxvii] *Ibid See also Ndifiembeu B. A Handboook On The Criminal Procedure Code of the Republic Of Cameroon unpublished (2006)*

ISSN 2581 3382