LEGAL ISSUES AND CHALLENGES OF SEARCHING AND SEIZING HARDWARE AND SOFTWARE AS EVIDENCE FOR PROSECUTION IN GHANA

Augustine Amoako, University of South Africa

ABSTRACT

Many investigations seek to search computers for evidence of a crime only. The computer might contain business records relevant to a white-collar prosecution. In criminal case, for the law or legislation to be applicable to a particular fact or situation, there must be a seizure or a search and seizure accompanied by an attempt by the prosecution to introduce what was seized as evidence in court. Whether there was a search or seizure within the meaning of the law and if so, whether the search or seizure violated someone's constitutional rights depends on the nature of the interest that the law protects. When electronic storage media are to be searched because they store information that is evidence of crime, the items to be seized under the warrant should usually focus on the content of the relevant files rather than the physical storage media. The aim of this research is to give rudiments overview legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. Also, the study draws a legal survey on how law enforcement seeks authority to search and seize broad class of information as evidence. It is importance for law enforcement agencies, especially the computer crimes units or the cybercrime units to have an in-depth understanding to establish various methods and procedures that can be used to conduct search and seize of electronic evidence.

Keywords: Warrant, Contraband, Investigations, Computers, Search, Seizure, Law Enforcement.

INTRODUCTION

Computer hardware might itself be contraband, an instrumentality of a crime, or fruits of crime and therefore may be physically seized. For example; a computer that stores child pornography is itself contraband. In the united States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000), after Hay was indicted for possessing and distributing child pornography, he moved to suppress this evidence for lack of probable cause to search and on the ground of staleness, but the district court denied the motion. The district court also denied Hay's motion to reconsider and to hold an evidentiary hearing in order to challenge the veracity of Galante's affidavit under Franks v. Delaware, 438 U.S. 154 (1978). Hay never challenged the indictment or the instructions on this ground. Indeed, he stipulated that the computer graphics files recovered from his system involved children under the age of eighteen and the stipulation listed the age range of each child in each of the exhibits. Counsel conceded that the material was child pornography. A computer may also be used as an instrumentality of crime, as when it is used to commit a hacking offense or send threats or a computer used to operate bulletin board distributing obscene materials is instrumentality. In Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997), the court held that the officers' reliance on a valid warrant entitled them to qualified immunity on plaintiffs' Fourth Amendment claim, and established a good faith defense under the Electronic Communication Privacy Act.

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

RESEARCH APPROACH AND METHODOLOGY

This research seeks to explore the legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. To achieve this, the research questions to aid us in gathering baseline information on the subject matter are:

1. How is law enforcement and investigators addressing legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana

To begin with, it must be taken into account that the outermost in this study methodology is conceded as a scientific discipline and doctrinal legal discipline in implying mounting out and defining the most appropriate ways of having or showing good judgement in the subject of investigation of search and search of evidence in the study. The researcher followed a qualitative and doctrinal legal research approach and is of opinion that qualitative and doctrinal legal research approach provides answers to the research questions in this study. Zareen et al. (2013) analyse and clarify that, participant observation, in-depth interviews and artefact collection are the available strategies found in the qualitative approach. This research does not focus on data through questionnaires, systematic data analysis, observations and interview. The study relies mostly on library materials, which include reports, legislations, court cases, regulations, charters, and policies, amendments to legislation, academic journals, constitution, and textbooks. In this study, legal methodology (Yadav et al., 2013) is used to discern law and legal phenomena of cybercrime investigations through analysis of statutory provisions and cases by application of power of reasoning and gives emphasis on analysis of legal rules, principles and doctrines. Creswell & Poth (2016) states that research approach is the plan and procedure to conduct research and it involves the connection of philosophy, research designs, and specific methods. Creswell & Clark (2017) indicated that a problem statement is the heart, clear statement supporting evidence of the research project that leads to the need for an in-depth research study and analysis in the particular environment to be addressed. The statement of purpose of the research provides the major objective or intent or "*road map*" of a study. Likewise, Locke, Karie & Venter (2015) posit that research aims need to be clear, specific and concise. Denscombe (2017) indicates that the existing background knowledge and the interests, motives and preferences of the researcher are the sets of factors that co-determine the clarification of the research objective.

Computer hardware and software as evidence

The computer is "*evidence*" only to the extent that some of the data it stores is evidence. In United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008), Giberson appeals from the district court's denial of his motion to suppress evidence of child pornography found on his personal computer, which led to his conviction for receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and possession of child pornography in violation of 18 U.S.C.§ 2252(a)(4)(B). He also appeals from his sentence, arguing that the district court erred in sentencing him for both possession and receipt of child pornography. But the court held that they have jurisdiction under 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a) (1) and therefore affirm his conviction, vacate his sentence, and remand. When probable cause to search relates in whole or in part to information stored on the computer, rather than to the computer itself, the warrant should identify that information with particularity, focusing on the content of the relevant files rather than on the storage devices which may happen to contain them. In United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) the court held that the district court agreed and suppressed the evidence.

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

The government filed this interlocutory appeal under 18 U.S.C. § 3731. While the judges agree with the district court that the warrant was invalid for lack of particularity, the judges hold that the good faith exception to the exclusionary rule should apply and, accordingly (563 F.3d 1127 (2009).

Seeking authority to search and seize broad class of information by law enforcement

Law enforcement should be particularly careful when seeking authority to seize a broad class of information. This sometimes occurs when agents plan to search computers at a business premises. In the case of United States v. Leary, 846 F.2d 592, 600-04 (10th Cir. 1988). It held that the government appeals from the district court's decision granting defendants' motion to suppress evidence seized under a search warrant. The judges affirm the district court, holding that the defendants' fourth amendment rights were infringed, that the search warrant was facially overbroad and invalid, and that the evidence seized should be suppressed. Agents cannot simply request permission to seize "*all records*" from an operating business unless agents have probable cause to believe that the criminal activity under investigation pervades the entire business (United States v. Ford, 184 F.3d 566, 576 (6th Cir. 1999). Instead, the description of the files to be seized should be limited. One successful technique has been to identify records that relate to a particular crime and to include specific categories of the types of records likely to be found. For example, the Ninth Circuit upheld such a warrant that limited the search for evidence of a specific (and specified) crime (United States v. Adjani, 452 F.3d 1140, 1148, 9th Cir. 2006). It is sometimes helpful to also specify the target of the investigation (if known) and the time frame of the records involved if known (United States v. Kow, 58 F.3d 423, 427 9th Cir. 1995).

Cyber search warrant execution

S.A Faqir (2013) asserts that the conventional search warrant execution refers to carrying out the search warrant by conducting the entry and search of the specified place. A search warrant is directed to a particular officer or class of officers. Only the named officer or a member of the named class of officers may execute or serve the warrant. If a warrant is directed to a sheriff, a deputy may execute the warrant and the sheriff need not be present. Officer may enlist private persons to help in the execution of a warrant, but an officer to whom the warrant is directed must be personally present at the search scene.

The process of executing data processing by conducting forensic analysis is what is termed as the virtual or cyber search warrant execution. Chernyshev et al. (2017) indicate that the first step is to begin to canvas the scene in an attempt to locate the digital media that you believe has the highest probability of containing the evidentiary information described in the warrant. The execution of cyber is conducted on – site, and therefore, mimics the stage of the traditional search procedures (crimes and criminal Procedures 18 USC § 3109, see also, Crimes Act 1914 Div. 5 s3ZS). The cyber search execution start with the traditional or conventional search procedures which begin with entry of dwelling to search as to the entry of dwelling to arrest. Law enforcement officers should knock and announce their authority and purpose before entering premises to execute a search warrant. In either way No-knock searches, searches without an announcement, may be authorized by state statute, particularly for drug cases. For example, In Wilson v. Arkansas (514 U.S. 927 [1995]), the Court ruled that the "*knock and announce common law principle is part of the Fourth Amendment's requirement that searches and seizures be reasonable*". It added, however, that this did not mean that every entry should be preceded by an announcement. The current rule is that, although knock and announce is part of the requirement of reasonableness in searches and

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

seizures, it is not a rigid rule and is subject to exceptions based on law enforcement interests. An announcement of identity as a law enforcement officer accompanied by a statement that the officer has a search warrant is usually sufficient. A person who refuses entry to an officer executing a warrant risks forcible entry. State v.Valentine, 504 P.2d 84 (Or.1972). But officers who have knocked and announced their authority and purpose may enter forcibly until it is reasonably apparent that they are being refused entry. Refusal does not have to be explicit, but most commonly, is implied by an occupant's failure to admit officers within a reasonable time after they knocked and announced. United States v. Banks, 124 S.Ct. 521. (2003), addressed the issue of what is a reasonable time for an occupant to respond. The law enforcement of the cyber search begins with notification and observes the physical location to be searched and then specify the search method to identify the digital or electronic devices stated in the warrant. Documentation, recording, and video shots should be done to avoid contamination of evidence. According to national institute of Justice (2001) documentation of the scene creates a permanent historical record of the scene. Documentation is an ongoing process throughout the searching and seizing of hardware and software evidence. It is important to accurately record the location and condition of computers, storage media, other electronic devices, and conventional evidence. Documentation of the scene should be created and maintained in compliance with departmental policy, national, State, and local laws. In addition, the National Institute of Justice Electronic Crime Scene Investigation guide for first responders (2008) state that the initial execution of cyber search should begin with documentation of the physical scene which include observing and documenting the physical scene, such as the position of the mouse and the location of components relative to each other (e.g., a mouse on the left side of the computer may indicate a left-handed user).

Seizing hardware components during search

Posit that the seizure of the hardware/physical containers involves labelling all wires connected to the computer or devices, and photographing the scene paying specific attention to the labelled connectors. The condition and location of the computer system including power status of the computer, on, off, or in sleep mode. Most computers have status lights that indicate the computer is on. Likewise, if fan noise is heard, the system is probably on. Furthermore, if the computer system is warm, that may also indicate that it is on or was recently turned off. The law enforcement should identify and document related electronic components that will not be collected and photograph the entire scene to create a visual record (National Institute of Justice Electronic Crime Scene Investigation guide for first responders 2008). The complete room should be recorded with 360 degrees of coverage, when possible and the front of the computer as well as the monitor screen and other components should be photographed (National Institute of Justice Electronic Crime Scene Investigation guide for first responders 2008). Also take written notes on what appears on the monitor screen. Active programs may require videotaping or more extensive documentation of monitor screen activity. The Movement of a computer system while the system is running may cause changes to system data. Therefore, the system should not be moved during search until it has been safely powered down. It is important to shut down the computer system in a manner that will not damage the integrity of any files. Different operating systems have different shutdown procedures. Some operating systems can be shut down by simply unplugging the power cord from the wall socket, while others have a more elaborate shutdown procedure. Anthony highlight that the most pressing issue relating to pull-the-plug is that some operating systems (OSes) really like to be shut down properly. Rapid power loss in some OSes can actually corrupt the operating system's kernel or the central module of the

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

system. UNIX, Linux, and Macintosh operating systems are the most vulnerable, but some Windows-based OSes, such as a Windows 2000 server, should be shut down properly. The EC-Council Investigation procedures and response (2016) outline the following procedures for shutting down or unplugging running computer systems:

1. MS –DOS/Windows 3.x/Windows 9x, Windows NT, Windows XP, Windows Vista, Windows, 7,8, and 10:

    (i) Take a photograph of the screen,
    (ii) Document any running programs
    (iii) Unplug the power cord from the wall socket.

2. UNIX/Linux

    (i) Right –click on Menu and click
    (ii) If root user is logged in, enter the password and type sync;sync;halt to shut down the system
    (iii) If the root user is not logged in and the password is available, type su to switch to the root user, enter the password, and type sync; sync; halt to shut down the system.
    (iv) If password is not available, unplug the power cord from the wall socket.

3. Macintosh Operating System:

    (i) Record the time from the menu bar
    (ii) Click special and then Shut Down
    (iii) Unplug the power cord from the wall socket

Robinson (2016) assert that the chain of custody should be done at this stage to track the evidence collection from its original source to the courtroom presentation. The execution of cyber search for and collection of evidence at an electronic crime scene is relevant. Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value (NIJ Electronic Crime Scene Investigation Guide for first responders 2008). This relates not just to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of computer evidence, therefore, require special collection, packaging, and transportation. The digital or recovery of non-electronic evidence can be crucial in the execution of cyber search and seize. Proper care should be taken to ensure that such evidence is recovered and preserved. Law enforcement should collect evidence through the order of volatility. The other of collection should proceed from the most volatile to the least volatile. Beginning with the most volatile such as registers and caches, to routing table, process table, kernel statistics, and memory, to temporary files systems, then disk or storage media, remote logging and monitoring data that is related or significant to the system in question then physical configuration and network topology and lastly archival media. Items relevant to subsequent examination of electronic evidence may exist in other forms such as written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs and should be secured and preserved for future.

Who May accompany the officers executing the Search?

Ferdico, et al. (2005) posits that a search warrant is directed to a particular officer or class of officers. Only the named officer or a member of the named class of officers may execute or serve the warrant. If a warrant is directed to a sheriff, a deputy may execute the warrant and the sheriff need not be present. Officers may enlist private person to help in the

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

execution in the execution of a warrant, but an officer to whom the warrant is directed must be personally present at the search scene. For example, in United States, it is a violation of the fourth Amendment for police to bring members of the media or other third parties into a home during the execution of a warrant when the presence of the third parties in the home was not in aid of the execution of the warrant.

In Wilson v**.** Layne**,** 526 U**.**S**.** 603 **(**1999**),** the Supreme Court decision held that the Fourth Amendment protection against unlawful search and seizures prohibited the police from bringing members of the news media into private homes while executing search warrants. Virtual crime or digital crimes have extra-ordinary phases in its search execution and require digital tools and conventional searches to accomplish the desire results together with team of investigators such as technician, evidence custodians, forensic examiners, and forensic analyst and electronic discovery experts. Usually, they have the first responders who create a toolkit before a cybercrime event happens and prior to any potential evidence collection. Once a crime is reported, someone should immediately report the site and should not have to waste any time gathering materials. The first responder toolkit is a set of tested tools designed to help in collecting genuine presentable evidence. The first responder has to select trusted computer forensic tools that provide output-specific information and determine system dependencies. Since there are complex and difficulties in digital investigations, there is always a professional investigator who is trained to conduct all complex cybercrimes and conduct the traditional searches and deal with real suspects.

The Time Allowed for a Search

The search cannot last indefinitely, with or without a warrant. Once the item mentioned in the warrant is recovered, the search must cease Etges & Sutcliffe (2010) Three different aspect of time affect law enforcement and investigators in the execution of search warrant (Ferdico et al., 2005), first is the allowable delay between the warrant's issuance and its execution, secondly the time day during which the warrant may be executed, and the amount of time allowed for the law enforcement officer to perform the search once it is initiated. In jurisdictions with no time limit fixed by statute, court rule, or judicial decision, a warrant must be executed within a reasonable time after issuance. Some jurisdictions require that a search warrant to executed and returned within ten days after its date of issuance. Theses jurisdictions may also require that the warrant be executed forthwith. To resolve this apparent ambiguity, courts require that the warrant be executed within a reasonable time after issuance. Casey (2011) adds that the US State of Texas allows three days, excluding the date of issuance and the date of execution, Veron's Ann. Texas C.C.P. Art. 18.07, wherea's California allows ten days, West's Ann. Cal. Penal Code § 1534. Likewise, state laws vary on the hours during which a search warrant may be executed. California law provides that upon a showing of good cause, the magistrate may, in his or her discretion, insert a direction in a search warrant that it may be served at any time of the day or night. In the absence of such a direction, the warrant shall be served only between the hours of 7 a.m. and 10 p.m. West's Ann. Cal. Penal Code § 1533. Some states in United States, including Texas, do not impose restrictions on the hours when a warrant may be executed; others allow nighttime searches under special circumstances. Carmen (2007) state that continued search without justification becomes a fishing expedition for evidence and is illegal. An illegal search is never made legal by what is subsequently found. For example, suppose the police go to an apartment to execute a search for a shotgun allegedly used in a murder. After the shotgun is recovered, the police continue to search for other evidence in connection with the murder. They open a bedroom closet and find a pair of bloodied jeans worn by the suspect during the murder. The

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

bloodied jeans, if seized and used in evidence, will not be admissible, because they were illegally obtained.

Ghana Legal response to searching and seizing digital evidence

Probable or reasonable cause has been clearly specify or formed into a corporation in the Ghanaian legislation for conventional searches. The Criminal Procedure Law 1960 (30) provides extreme magnitude for issuing a search warrant. Section 88 (1a, b, c) states that, a District Magistrate who is satisfied, by evidence upon oath, that there is reasonable ground for believing that there is in any building, vessel, carriage, box, receptacle, or place or :

1. Anything upon or in respect of which any offence has been or is suspected to have been committed, for which according to any law for the time being in force, the offender may be arrested without warrant; or
2. Anything which there is reasonable ground for believing will afford evidence as to the commission of any such offence; or
3. Anything which there is reasonable ground for believing is intended to be used for the purpose of committing an offence against the person for which, according to any law for the time being in force, the offender may be arrested without warrant, may at any time issue a warrant under his hand authorising any constable to search any such building, vessel, carriage, box, receptacle, or place for any such thing, and to seize and carry it before the Magistrate issuing the warrant or some other Magistrate to be by him dealt with according to law.

In addition, section 89 specify the time when search warrant may be executed and it state that every search warrant may be issued and executed on a Sunday and shall be executed between the hours of 6.30 a.m. and 6.30 pm., but the Court may, by the warrant, in its discretion, authorize the police officer or other person to whom it is addressed to execute it at any hour. However, at the time of writing the researcher found out that there is no documented court cases that addressed the issue of Internet Protocol (IP) address and probable cause. All addressed made on probable cause by scholars and expert concerns conventional searches. No provisions in the legislations specifically deal with cyber searches mirror copy and there is no scholarly work identify and analysis the issue. In addition, there are no court decisions on cyber searches and mirror copy. With this in place, it is highly that conventional search warrant procedures would be applied to cyber searches. The Criminal Procedure Law 1960 (30) provides threshold for issuing a search warrant, and executing officers to search and seize any material items that are tangible and might relate to any offense. Currently, the laws of Ghana authorize search of and seizure of things that are tangible.

However, the virtual or digital contents were not addressed by the law and not identify as an article or item on their own right. On the other hand, the Criminal Procedure Code 1960 (Act 30) identifies that the subject of the search warrant is either physical place, building in which a person lives and maintain privacy, or vessel, carriage, box, receptacle that items are kept. In addition the Section 88 (A and B) of the criminal Procedure Code 1960 (Act 30) authorize the police to seize anything which there is reasonable ground for believing will afford evidence as to the commission of any such offence or anything which there is reasonable ground for believing is intended to be used for the purpose of committing an offence against the person for which, according to any law for the time being in force, the offender may be arrested without warrant.

In Ghana, the judge or magistrate is the only authority entitled to prepare and issue search warrants. The judge or magistrate issue search warrant to the police officers to execute it. However, the officer designated to execute search warrant must all time obey and adhere

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

to the judge or magistrate instructions about the warrant execution procedures, its scope, location or area to be searched, its time or day the search should be executed. The warrant must be performed according to the rules of laws governing the search and seize. In regard to the pre-digital search phase, the Criminal Procedure Code 1960 (Act 30) gives powers to the judge or magistrate to issue search warrant to the police or law enforcement to search without notifying in advance the defendant or the suspect of the search. The defendant or his representative can be present during the time of search warrant execution. The Act also gives powers to judge or magistrate to issue broad discretion which concerns the appropriate procedures and measures that the law enforcement or the investigators follow to ensure proper search and seizure operation. However, the digital phase has no legal provisions that address the particular procedures or methods for searching and seizing computer artefacts. Even though there are no provisions concerning cyber searches, conventional search execution requirements must be observed when executing cyber search. The Judge can nominate an expert such as digital forensic investigators, to provide assistance and the expert must declare under oath that they will carry out their task in trustful manner and impartially.

Allow a neutral judicial officer to assess whether the police have probable cause to make an arrest or conduct a search (Mollet v State 939 P.2d 1 (Okla.1997) 743).

Marghaireh (2009) assert that applying the traditional procedures of knocking and notifying to the place the search may jeopardise the integrity of the evidence that is going to be discovered because digital evidence can be quickly and easily destroyed even by something as simple as pressing a hotkey Law enforcement can always be successful in searching and seizing evidence when they used sneak tactics or take the suspect by surprise to avoid destruction of evidence. Therefore using sneak and peck search warrant, instead of a traditional or classical search warrant that involve knocking and notifying is welcome and self-evident in digital search and seizure and digital investigation than any other investigation.

Legal issues and challenges in searching and seizing digital Evidence

Ferdico et al. (2005) assert that under the common law, it was clear that the security of one's property was a sacred right and that protection of that right was a primary purpose of government. In Ghana, article 18 of the Ghanaian Constitution deal with individual protection of privacy of homes and other properties. Section 2 of Article 18 of the Ghana Constitution state that: No person shall be subjected to interference with the privacy of his home, property, correspondence or communication. In addition, the constitution protect unreasonable or illegitimate search of physical places used for residential purposes, such as hotels, guest houses, private apartments In the United States, the protection of property interests as the basis of the fourth Amendment was adopted by the U.S. Supreme Court, and until relatively recently, analysis of Fourth Amendment issues centered on whether an intrusion into a constitutionally protected area had occurred. In Olmestead v. United States, 277 U.S. 438 (1928), one reason for the Court's holding that wiretapping was not covered by the Fourth Amendment was that there had been no physical invasion of the defendant's premises. The Court said: the evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched. Furthermore, In silverman v. United States, 365 U.S. 505 (1961), however, a spike mike was pushed through a common wall until it hit a heating duct, and the Court held that the electronic surveillance was an illegal search and seizure. And in Clinton v. Virginia, 377 U.S. 158 (1964), the Court ruled inadmissible evidence obtained by means of mechanical listening

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

device stuck into the wall of an apartment adjoining the defendant's. In Katz v. United States, 389 U.S. 347 (1967), another electronic surveillance case, dispensed with the requirement of an actual physical trespass in applying privacy the United States Fourth Amendment. The court held that the government's electronically listening to and recording the defendant's words violated the privacy on which the defendant justifiably relied when using the telephone booth and thus constituted a search and seizure within the meaning of the Fourth Amendment. The added, "*The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance*". The katz case signaled a major shift in the interpretation of the Fourth Amendment away from a property approach toward a privacy approach.

CONCLUSION

Successful investigations search and seizure of hardware and software to as serve as evidence in a crime depends heavily on technological infrastructure. The primary frontier for defence against cyber threat is technology (International Telecommunication Union (ITU), 2018). In order for law enforcement to properly search for and seize of hardware and software, there should be in a properly constituted computer emergency or incident response teams, technical apparatus, tools and capabilities for the search and seizure of hardware and software. It is also require putting in place a framework that is conscientious for the effective coordination among the cyber search team. A country without a meticulous cyber search team will continue to lack digital evidence handling through the chain of custody. At present, Ghana has no national cyber search and seizure team to deal with cyber search and seizure of computer to deal with the technical search and seizure of digital evidence and there are no national framework on cyber search and seizure of digital evidence. This has resulted in many virtual crimes left behind because there are no skilled cyber search team in place to conduct the digital search and seizure and hence result in difficulties for prosecutors and juris to authenticate digital evidence in the courtroom. Unlike the United Kingdom and United States where a comprehensive guidelines has been developed for virtual criminal investigators for search and seizure of hardware and software as evidence respectively by their reputable bodies such as the Association of chief of Police (ACPO) and National Institute of Standard and Technology (NIST), Ghana lack such guidelines. The standard guidelines on digital search and seizure by NIST and ACPO could be adopted and modified to suit Ghana's digital search and seizure legal enclave in order to serve as guideline on cyber search and seizure for both public and private digital investigators.

REFERENCES

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. *Academic press*.

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile forensics: advances, challenges, and research opportunities. *IEEE Security & Privacy*, *15*(6), 42-51.

Creswell, J.W., & Clark, V.L.P. (2017). Designing and conducting mixed methods research. *Sage publications*.

Creswell, J.W., & Poth, C.N. (2016). Qualitative inquiry and research design: Choosing among five approaches. *Sage publications*.

Denscombe, M. (2017). EBOOK: The good research guide: For small-scale social research projects. McGraw-Hill Education (UK).

Etges, R., & Sutcliffe, E. (2010). An overview of transnational organized cyber crime. *Journal of Digital Forensic Practice*, *3*(2-4), 106-114.

Ferdico, J.N., Fradella, H.F., & Totten, C.D. (2005). Criminal procedure for the criminal justice professional. *Thomson/Wadsworth*, 672.

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.

Karie, N.M., & Venter, H.S. (2015). Taxonomy of challenges for digital forensics. *Journal of forensic sciences*, *60*(4), 885-893.

Robinson, E.M. (2016). Crime scene photography. *Academic Press*.

S.A Faqir, R. (2013). The use of technology of global positioning system (GPS) in Criminal investigation & right to privacy under the constitution and criminal legislations in Jordan: legal analysis study. *Revue internationale de droit pénal*, (3), 433-462.

Yadav, D., Mishra, M., & Prakash, S. (2013). Mobile Forensics challenges and admissibility of electronic evidences in India. In *2013 5th International Conference and Computational Intelligence and Communication Networks*, 237-242.

Zareen, M.S., Waqar, A., & Aslam, B. (2013). Digital forensics: Latest challenges and response. In *2013 2nd National Conference on Information Assurance (NCIA)*, 21-29.

Received: 11-Aug-2023, Manuscript No. JLERI-23-13897; **Editor assigned:** 14-Aug-2023, Pre QC No. JLERI-23-13897(PQ); **Reviewed:** 01-Sep-2023, QC No. JLERI-23-13897; **Revised:** 05-Sep-2023, Manuscript No. JLERI-23-13897(R); **Published:** 16-Sep-2023

Citation Information: Amoako, A. (2023). Legal issues and challenges of searching and seizing hardware and software as evidence for prosecution in Ghana. *Journal of Legal, Ethical and Regulatory Issues, 26*(6), 1-10.