Conflict with Privacy Protection in Criminal Electronic Evidence and Countermeasures

Yubao Wu

Department of Information Technology, Nanjing Forest Police College, Nanjing, Jiangsu, 210023, China

eice_wu@126.com

Keywords: Criminal Cases, Electronic Forensics, Privacy Protection

Abstract: Electronic evidence is one of the legal forms of evidence stipulated in the Criminal Procedure Law. Compared with traditional evidence, the way of obtaining electronic evidence is likely to violate the privacy rights of citizens. In the present case, it is difficult for relevant authorities to truly obtain complete electronic evidence without touching the privacy rights of suspects and other unrelated persons. Therefore, it is worth discussing how to control the boundary and scope of electronic forensics and citizen privacy protection.

1. Introduction

The so-called "right to privacy" means that citizens enjoy the right to refuse and reject any unauthorized surveillance, snoop and prevent the disclosure of personal information according to law. Privacy, as a basic personality right of citizens, occupies a very important position in the protection of citizens' rights. However, in the present case, when the State conducts electronic evidence collection in some criminal cases, it needs to use modern computer means to access the relevant information of the suspect and the criminal record. At this time, not only the privacy of the criminal suspect will be infringed, but also the privacy of the relevant personnel will be infringed to a certain extent, which is the conflict between the electronic evidence collection of criminal cases and the protection of privacy. How to solve these problems is the key to be discussed.

2. Overview of Electronic Evidence

2.1. Concept of Electronic Evidence

The broad range of electronic evidence is very broad, and all the evidence that can prove the facts of a case stored on a computer hard disk, mobile phone ROM, and other electronic storage media is electronic evidence. All evidence formed with the aid of modern information technology and electronic equipment, or shown electronically, that can prove the facts of a case[1]. Mainly include: electronic articles, e-mail, CD-ROM, web page, domain name, electronic contract, electronic bill of lading, electronic insurance policy, electronic invoice, etc.

2.2. Measures for Collection of Electronic Evidence

The so-called "mobile terminal forensics ", that is: the legal forensics subject through the legal way to find the extraction and inspection of mobile terminal equipment, in order to obtain the information contained in the mobile terminal, and then from the information to obtain evidence. Nowadays, many cybercrime activities are carried out through the way that mobile terminals connect to the network. Therefore, investigators according to the actual situation of mobile terminal evidence, is one of the electronic evidence collection measures.

  DOI: 10.25236/edssr.2020.111

Figure 1 Electronic evidence

With the advent of the big data era, citizens' electronic data began to migrate from mobile terminals to remote cloud. Therefore, when the relevant investigators can not extract the relevant criminal information from the mobile device, they can carry out remote extraction through the cloud, and then complete the relevant electronic forensics work.

Figure 2 Electronic evidence

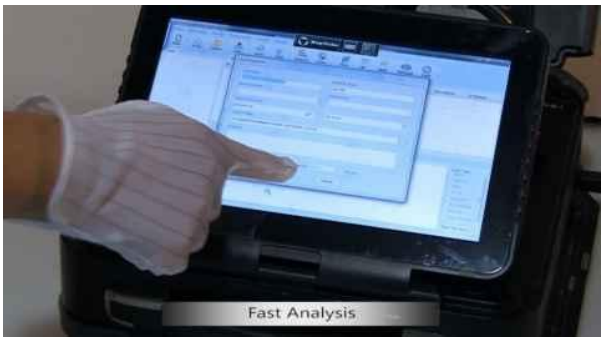

Figure 3 Electronic evidence

Some criminal gangs are more cunning, and it is difficult to obtain their criminal evidence by normal means. Therefore, the relevant departments will sometimes use electronic equipment to monitor, monitor and other activities, hoping to be able to obtain criminal evidence, and thus promote the progress of the case[2].

3. Threats to Personal Privacy in the Electronic Forensics Process

3.1. Conflict Between the Right of Electronic Evidence to Obtain Evidence and the Right to Privacy of Mobile Terminals

As mentioned above, many criminals commit criminal activities through mobile terminals and network connections. Therefore, in the process of collecting evidence, the relevant personnel will choose the form of connecting network to explore the mobile terminal of the criminal, so as to

obtain the relevant criminal evidence. However, we need to be clear: when the personal mobile terminal is connected to the network, it means that the virtual space with the mobile terminal as the main body is infinitely extended. In this virtual space, there is a lot of personal information, which is complex and diverse, and not all the information is related to the case. The personal information contained in the mobile phone is extremely complex and diverse, if carefully analyzed, can completely analyze the survival track of the mobile terminal owner. In this case, searching for a person's mobile phone is obviously more valuable than searching for a person's real estate. If the relevant search personnel after the successful arrest of the suspect, without any approval to directly search the suspect's mobile terminal equipment, then it is very easy to violate the suspect's privacy. This kind of harm is equivalent to the relevant investigators without the approval of the higher authorities, with only a key to open the door of the suspects to search the general, such violations of personal privacy is very easy to lead to the abuse and misuse of judicial power.

3.2. Conflict Between the Right to Obtain Evidence by Remote Electronic Evidence and the Right to Privacy

In view of the fact that many suspects now choose to store their own electronic data related to crime in the cloud, the searchers will choose the method of remote extraction when conducting electronic evidence collection. For example: search network server, enter network background through third party enterprise and so on. Such a remote way of extracting evidence involves a wide range of electronic data information, including not only the relevant information of the suspect, but also the personal information of other citizens who are not related to the case. Therefore, once the right of remote evidence of electronic evidence is abused, it is very easy to cause a large area of information disclosure, not only to the personal information of the criminal suspect will cause infringement, but also to the personal information of the citizens who have nothing to do with the case, the impact is extremely bad.

3.3. Conflict Between Evidence-Taking Measures Such as Electronic Surveillance and Privacy Rights

In the present situation, many investigators will choose to use electronic equipment for electronic surveillance, monitoring and other forms of criminal evidence. This way will not only infringe on the personal life of the criminal suspect, but also make the personal information of the citizen who is related to the criminal suspect, but not related to the case, which is a conflict for the privacy of the citizen, and also a dangerous behavior to the privacy of the citizen.

4. Strategies for Protecting the Privacy of Citizens in the Process of Electronic Evidence

We need to be clear: for the criminal, they will allow the criminal evidence to be hidden by changing the name of the document, changing the attributes of the document, changing the form of the document, etc. In this context, investigators can do their best to find the criminal evidence and bring the criminal to justice only through a large number of search and careful exclusion of information. It is unlikely that investigators will find evidence of the crime on the premise of fully protecting the personal privacy of suspects and other citizens. Therefore, the relevant departments should give a proper balance between electronic evidence collection and citizen privacy protection according to the actual situation, so as to promote the process of solving cases while protecting the legitimate rights and interests of citizens.

4.1. Determining the Rules for the Collection and Approval of Electronic Evidence

According to the existing law, the relevant search personnel can search and obtain evidence of electronic evidence only with the consent of the public security organs at or above the county level. This situation leads to the absence of the search rights of search agents from the checks and balances of the third-party judiciary, which can easily lead to the abuse and misuse of search rights[3]. Therefore, the relevant departments should determine the rules for the collection and approval of electronic evidence according to the actual situation, so as to further protect the privacy

of citizens.

The relevant departments shall promulgate the following provisions: in case of non-emergency, the search personnel performing the electronic forensics task shall apply for a search warrant issued by the third party judicial department, hold a search warrant to search the relevant mobile equipment, and can not search without a search warrant. The so-called third-party judicial department must be related to the case, but not to the public security department, and is an independent and neutral judicial organ, such as: court, procuratorate, etc. This can further protect the privacy of citizens and promote the process of obtaining evidence of electronic evidence, which is very helpful to solve related criminal cases.

4.2. Principles for the Unlawful Exclusion of Electronic Evidence

According to the law of our country, our country regards electronic evidence as physical evidence. Such evidence would therefore be excluded only if the procedure for obtaining evidence was illegal and could not reasonably be explained. Conversely, it is difficult to actually exclude evidence of this kind if the procedure for obtaining it is improper. Although this way is helpful to speed up the detection of cases, it is very easy to cause investigators to abuse their own investigative rights, and then lead to the violation of citizens' privacy rights. Therefore, the relevant departments should regulate the procedure of obtaining electronic program according to the actual situation, so as to ensure the investigators to exercise the right of investigation legally and to protect the privacy of citizens from the infringement of public power.

The relevant departments may promulgate the following provisions: evidence obtained from private searches without judicial authorization shall be classified as illegal evidence and shall be excluded according to the actual circumstances of the case. Evidence of significant progress and proven truth in the resolution of the case may be accepted as appropriate, but the conduct of its unlawful search shall be punished accordingly. In addition, the relevant departments should establish the corresponding investigation penalty system for investigators, so as to regulate the investigation behavior of investigators, so that the public power can be exercised within the scope of the law, so as to better protect the privacy of citizens, so that the contradiction between electronic evidence and privacy in criminal cases can be further resolved.

5. Conclusion

To sum up, in the process of criminal electronic evidence collection and approval rules, determine the principle of illegal exclusion of electronic evidence and regulate the scope of collection of electronic evidence, we can solve the conflict between the process of electronic evidence and the protection of citizens' right to privacy, so that the collection of electronic evidence in our country becomes more legalized, and the privacy of our citizens is more legitimately protected.

Acknowledgements

The 2019 major special support from Jiangsu Provincial Department of science and technology, Research and demonstration of key technologies for security protection of Jiangsu Police cloud (BE2019762)

References

[1] Tian, Zhen. Legal regulation of the conflict between the application of electronic evidence and the protection of citizens' right to privacy. Youth Science (Teacher Edition), vol. 34, no. 9, pp. 1-2, 2013.

[2] Li, Shuang. A study of electronic evidence collection in criminal proceedings. Hebei: Yanshan University, 2017.

[3] Li, Hongdan., Li, Mengyue. On the Protection of Citizen's Privacy in Electronic Data Collection. Business Bulletin, no. 11, pp. 153, 2013.