United States rules on electronic evidence collected from smartphones and their influence on China

Cao, Yiyang

Published in:
Journal of Forensic Science and Medicine

Published: 01/04/2019

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

Published version (DOI):
10.4103/jfsm.jfsm_51_18

Publication details:
Cao, Y. (2019). United States rules on electronic evidence collected from smartphones and their influence on China. *Journal of Forensic Science and Medicine*, *5*(2), 104-111. https://doi.org/10.4103/jfsm.jfsm_51_18

Original Article

United States Rules on Electronic Evidence Collected from Smartphones and their Influence on China

Yiyang Cao[1,2]

[1]Procedure Law Department, School of Law, Wuhan University, Wuhan, China, [2]Center for Chinese and Comparative Law, School of Law, City University of Hong Kong, Hong Kong, China

Abstract

The popularity and wide use of smartphones have led to an increase in the debate on the procedure relating to their investigation and search. We should not neglect the protection of citizens' privacy concerning the content of their smartphones since they contain so much personal information. In 2014, the United States (US) Supreme Court addressed two cases, *Riley v. California* and US *v. Wurie*, which dealt with smartphone searches and the search incident to arrest exception to the warrant requirement. Police must obtain a warrant when they want to search for evidence in the smartphone of a potential suspect. However, there are exceptions to this requirement: emergencies and exigent circumstances; the consent to search exception; and the "plain view" exception. The procedural law of China contains no legal regulations on smartphone searches. Therefore, we should establish the principles of smartphone searches to strike a balance between the protection of citizens' privacy and the punishment of crime. It is helpful for us to learn from the experience of the US and other countries and limit warrantless searches, improve the writ principles and clarify the scope and procedure of smartphone searches. It is also important to establish corresponding procedural sanctioning and supervisory mechanisms.

Keywords: Privacy, smartphone search, warrantless search, writ principle

Introduction

The remarkable growth in the number of people who own smartphones has created new challenges and opportunities in digital forensics. The smartphone can be presented as a goldmine for investigators as a source of digital evidence. Smartphones have become indispensable tools in modern society. They combine many functions containing copious amounts of personal information such as photographs, video recordings, internet history, Bluetooth, a calendar, an address book, and applications. Due to the ubiquity of smartphones and the nature of their use, the data collected from smartphones can be used in digital forensics. However, data collection from smartphones may invade privacy. If the police can go through some formal procedures before collecting data, citizens may have a reasonable expectation of privacy. Otherwise, legal issues pertaining to the secrecy of telecommunications and the privacy of the concerned persons may be triggered. Smartphone forensics are an emerging discipline that is still in its infancy. The criminal and civil procedure law of China currently includes no regulations on smartphone searches, so it is an opportune time for a principle to protect the rights of citizens in the use of data collected from smartphones to be established.

Access this article online

Quick Response Code:

Website: www.jfsmonline.com

DOI: 10.4103/jfsm.jfsm_51_18

Sources of Data from Smartphones

Compared with traditional evidence, digital evidence is more likely to be concealed and harder to preserve. However, electronic evidence obtained from smartphones can be easily collected and preserved through legal procedures and with the legislative methodology. The main methods of acquisition of data are as follows (1) data from a SIM (UIM) card; (2) data from smartphone memory; (3) external extended memory; and (4) cloud computing data from a mobile carrier.

SIM (UIM) card is an integrated circuit that is intended to securely store the international mobile subscriber

Address for correspondence: Dr. Yiyang Cao, School of Law, Wuhan University, No.299 Bayi Road Wuchang District, Wuhan City 430072, China.
E-mail: caoyiyang@whu.edu.cn

How to cite this article: Cao Y. United States rules on electronic evidence collected from smartphones and their influence on China. J Forensic Sci Med 2019;5:104-11.

Table 1: Laws and regulations on electronic evidence in China

Enacting Institutions	Laws and regulations	Relevant concepts	Legal effect
Standing Committee of the National People's Congress	Law of the People's Republic of China on Electronic Signatures (2004 enacted, 2015 amended).	"Electronic signature" means the data in electronic form contained in and attached to a data message to be used to confirm the identity of the signatory and to show that the signatory recognizes what is in the message. (Chapter I, Article 2) "Data message" as mentioned in this law means the information generated, dispatched, received or stored by electronic, optical, magnetic or similar means. (Chapter I, Article 2)	Clarifies the legal effect of electronic signatures and data messages. A reliable electronic signature and traditional handwritten signature have the same legal effect
National People's Congress	Criminal Procedure Law (1979 enacted, 2012 amended)	All facts that prove the true circumstances of a case shall be construed as evidence. Evidence contains audiovisuals and electronic evidence. (Article 48)	Audio-visual materials and electronic evidence are classified as the eighth type of evidence. However, electronic evidence still does not have completely independent evidence status
National People's Congress	Civil Procedure Law (1991 enacted, 2012 amended)	Evidence shall be classified as follows: Electronic evidence. (Article 63)	Electronic evidence became the 5th type of evidence and has independent evidence status
National people's congress	Administrative Procedure Law (1989 enacted, 2014 amended)	Evidence includes: Electronic evidence. (Article 33)	Electronic data became the fourth type of evidence and has independent evidence status
Supreme People's Court	Provisions of Supreme People's Court on Evidence of Civil Procedures (2001 enacted)	——	It embodies the best evidence rule
Supreme People's Court	Provisions of Supreme People's Court on evidence of Civil Procedures (2002 enacted)	When confirmed by the other party or notarized in other effective ways, electronic evidence which is displayed in a fixed or physical carrier, e-mail, and other forms is equally as authentic as original materials. (Article 64)	It embodies the best evidence rule, and expands the scope of the "original materials" to make the electronic evidence more applicable to the best evidence rule
Supreme People's Court	Opinion of the Supreme People's Court on several issues concerning the application of the Civil Procedure Law of the People's Republic of China (2014 enacted)	Electronic evidence refers to the information that is formed or stored in electronic media through e-mail, electronic data exchange, online chat records, blogs, Weibo, short messages, electronic signatures, and the domain name. The recording data and video recording data stored in the electronic medium are applicable to the regulations of electronic data. (Article 116)	Clarifies the meaning of electronic evidence and points out forms of electronic evidence
Supreme People's Court, the Supreme People's Procuratorate, Ministry of Public Security	Provisions on the collection of criminal cases and the review of certain issues concerning electronic data (2016 enacted)	Electronic evidence is the data that is collected during the case and stored, processed and transmitted in digital form. It can prove the facts of the case Electronic evidence includes the following information and electronic documents: 1. Information published by Internet platforms such as web pages, blogs, Weibo, Wechat moments, posts, and other online platforms; 2. Communication information from mobile phone short messaging service, e-mail, instant messaging, communication groups and other network application services; 3. User registration information, identity authentication information, electronic transaction records, communication records, login logs and other information; 4. Documents, pictures, audio and video, digital certificates, computer programs and other electronic documents. (Article 1)	The concept of electronic evidence is defined, and the general form of electronic evidence is specified in a list which excludes special cases. It also regulates concrete procedure for the extraction and review of electronic evidence

identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also common to see that many SIM cards can store some information on them. For example, a SIM card contains its serial number, IMSI number, and two passwords: PIN and PUC.

Data from smartphone memory contains International Mobile Equipment Identity, an address book, memo, short messages, video recordings, sounds, images, and documents.

External extended memory is an electronic flash memory data storage device used for storing digital information. It can be used to expand the storage of smartphone memory. The

common forms of external extended memory are SD cards, Memory Stick cards, SDHC cards, and T-Flash cards.

Cloud computing data from a mobile carrier are a computing concept where software services, and the resources they use, operate as a virtualized platform across many different host machines, connected by the Internet or an organization's internal network. For example, the information about location, time, and contents on services such as WeChat, QQ, and Weibo.

It is essential that law enforcement agencies employ scientifically sound and reliable forensic tools and techniques to ensure that smartphone data recovered using new and evolving technologies will be admissible and useful in judicial proceedings. Can all the data collected from the aforementioned sources be regarded as electronic evidence? Can data from a damaged SIM card or deleted data from smartphone memory be used as electronic evidence? The newer smartphones, such as iPhones, can be remotely disabled or remotely data wiped. The remote-wiping capability is available on all major smartphone platforms. Apple iPhones are equipped with the "Find My iPhone" app, which allows a user to remotely lock or wipe the phone. Therefore, if the important information is wiped out through another iPad or iPhone, can the deleted or wiped out data which are recovered by the police be used as electronic evidence? This may be determined by whether the rules of admissibility of evidence are conditional on showing that the evidence is reliable.

Laws and Regulations on Electronic Evidence in China

Currently, there are already many laws and regulations that mention the relevant concepts of electronic evidence in China; these are presented in Table 1.

According to the aforementioned laws and regulations, electronic evidence is collected by parties and the People's Court in civil cases, and in criminal cases, it can be collected by the People's Court, a public procurator, public security investigators, and administrative bodies. However, there are no specific articles on the search of smartphones.

Procedure for Digital Forensic Evidence in Smartphones

Methodology for digital forensics

Digital forensics include short messages, video recordings, and services such as Wechat, QQ, and Weibo. Undoubtedly, short messages are the most common type of digital forensic evidence. Thus, I will use data collected from short messages as an example. There are two main ways for collecting data from short messages. One way is to read short messages directly from smartphone memory, and another is to obtain the information from the mobile carrier. The mobile carrier has specific information on data such as customers' recordings and user registration information, addresses, ID card numbers, and phone numbers.

Search and seizure of electronic evidence from smartphones

There is ongoing debate on the search and seizure of electronic evidence from smartphones. In China, is it necessary to establish regulations on obtaining a warrant before digital data on smartphones can be searched incident to arrest? By obtaining a warrant first, can we protect citizens' legislative expectation of privacy? More specifically, if the average person knows that some of their personal information could be shared with others or the public, will they not have expectations on their privacy? Many countries made laws and regulations on the protection of privacy and these countries also laid emphasis on the expectation of privacy. In European countries, the individual's "reasonable expectation of privacy" is the touchstone of article 8 (1) of the European Convention on Human Rights and without such an expectation article 8 is not applicable. Respect for privacy and data protection is also regulated in several specific Directives in Europe, namely the Data Protection Directive, E-Privacy Directive, and Data Retention Directive. The notion of "reasonable expectation of privacy" has had a significant impact on the evolution of the legal understanding of privacy. In the case of *Copland v. United Kingdom*,[1] the court ruled that monitoring or controlling personal calls, E-mails, and Internet use interfered with a European citizen's right to privacy. Europe protects informational privacy so thoroughly because it is a fundamental human right and it is essential to the development of self-identity and the freedom to be one's self.[2] In Japan, the secrecy of communication is guaranteed by the Constitution. The Telecommunications Business Act provides that the communications being handled by the telecommunications service provider shall not be censored, and the secrecy of such communications shall not be infringed.[3] South Korean Constitutional Law states, "the privacy of no citizen shall be infringed." The Communication Secrecy Protection Act of 1993, the Personal Information Protection Act, the Criminal Code, the Act on the Promotion of IT Network Use and Information Protection (Network Act), and the Use and Protection of Location Information Act have been enacted to protect the privacy of citizens in modern society. Article 201 of the Korean Criminal Procedure Act requires a judicial warrant for search, seizure, or inspection.[4] Some countries such as New Zealand and the United Arab Emirates, have the warrant requirement.[5] The Fourth Amendment to the United States (U. S.) Constitution provides that, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but on probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." It confirms that the expectation of privacy must be "legitimate," in the sense that it is backed by the extra-constitutional right to prohibit the invasion of privacy. Police officers are required to obtain a warrant before they can search digital data on smartphones incident to arrest. There are many U.S. cases that embody the warrant requirement.

The case of the US *v. Granville*[6] raised the issue of whether a person retains a legitimate expectation of privacy in the contents of their smartphone when that phone is being temporarily stored in a jail property room. In this case, a juvenile defendant was charged with improper photography or visual recording, based on a photograph taken with his smartphone. The district court granted the defendant's motion to suppress the photograph based on the unlawful warrantless search of his smartphone. The state appealed, and the court of appeal affirmed the decision of the district court, finding that a person "has a general, reasonable expectation of privacy in the data contained in or accessible by his cell, now "smart" phone, and a person continues to have a reasonable expectation of privacy in the contents of his cell phone even though it has been placed in a jail property room for safekeeping." Courts have held that a person has a subjective expectation of privacy in the contents of his/her smartphone and this expectation of privacy is one that society recognizes as reasonable and legitimate.

Another case is *U. S. v. Wurie*,[7] in 2007, police arrested Wurie for the suspected sale of drugs. After taking him to the police station, two cell phones and a set of keys were taken on his person. One of his cell phones was repeatedly receiving calls from a number identified as "my house" on the screen. The officers searched through the cell phone's call log and determine Wurie's home phone number. The officers used that number associated with the address and determined Wurie's address, which they then searched, finding 215 g of crack cocaine, a firearm, ammunition, four bags of marijuana, drug paraphernalia, and $250 in cash. Wurie was charged with possessing with intent to distribute and distributing cocaine base and with being a felon in possession of a firearm and ammunition. He filed a motion to suppress the evidence obtained as a result of the warrantless search of his cell phone. The U.S. District Court for the District of Massachusetts denied Wurie's motion to suppress. The court concluded that the search of the phone number associated with the "my house" contact was no different than the search of other personal containers found on the defendant's person.[8]

From these two cases, we must first find out the scope of the search. Whether or not a smartphone can be searched without a warrant is a hotly debated topic. In the case of *U. S. Petitioner v. Willie Robinson*,[9] the officer searched the respondent's person and found, in a coat pocket, a cigarette package containing heroin. In the case of a lawful custodial arrest, a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment but is also a "reasonable" search under that Amendment.[9] What can be defined as a "reasonable" search? Can smartphones, pagers, and laptops be regarded in the same way as the cigarette package and justify the use of a warrantless search? Most courts have ultimately upheld warrantless smartphone data searches using a variety of approaches. Some have concluded that, under *Robinson*, a smartphone can be freely searched incident to a defendant's lawful arrest, with no justification beyond the fact of the arrest itself. For example, see the cases of US *v. Young*,[10] US *v. Finley*,[11] *People v. Diaz*.[12] Smartphones store more private information than beepers and traditional cell phones. Smartphones are both quantitatively and qualitatively different from other objects an arrestee might keep on their person based on their immense storage capacities. By compiling such specific information about all aspects of an arrestee's life, law enforcement can easily reconstruct their personal life dating back several years. This type of expansive search was completely distinguishable from the search of a cigarette pack's contents. Therefore, smartphones cannot be seen as an object that is under the control of the arrestee. Smartphones are more likely to be regarded as "computers" in evidence law. As the differences in the features of smartphones and personal computers continue to decrease, courts should recognize that smartphones entail the same expectations of privacy as computers and treat warrantless searches of smartphones in the same manner. Therefore, courts should require reasonable suspicion of the content of the parts of the phone being searched. If the police want to search the content in smartphones, they need to apply for another search warrant.

Exception of the Warrant Search for Smartphones

Although law enforcement must obtain a warrant before searching a smartphone's data, the Supreme Court has provided an exception to this general rule to better balance the government's needs against the arrestee's privacy interests. In some circumstances, there remains an exception which allows the government to search a smartphone without a warrant if there is a reasonable need.

Emergencies and exigent circumstances

Courts have often cited the exigency exception (i.e., the need to preserve evidence that could be lost or destroyed quickly) to validate a search of the contents of a smartphone without a warrant. The U.S. Court permits a search for evidence without an arrest but under circumstances where probable cause for an arrest existed, where the officers had reasonable cause to believe that the evidence was on respondent's person, and where that evidence was highly destructible. The Court, however, restricts the permissible quest to "the very limited search necessary to preserve the highly evanescent evidence." Another circumstance is described in *State v. Thomas*,[13] where officers who observed the subject of a felony arrest warrant flee from a public area into the defendant's house were justified in making a warrantless entry into the house under the exigent circumstance of hot pursuit and seizing evidence that was in plain view. The court analyzed whether a police pursuit that culminated in the entry of a house or other building to search for or arrest a suspect qualified as a "hot pursuit," that is, the police pursuit was sufficiently immediate, continuous, or vigorous to excuse noncompliance with the Fourth Amendment warrant requirement. Police can perform a warrantless search in emergencies and exigent circumstances where: (a) the evidence is highly evanescent; (b) the defendant is the subject

of a felony arrest warrant; and (c) it is necessary to reduce a threat to other police officers or citizens.

The U.S. case of *Riley v. California*,[14] asserts a Fourth Amendment right to be free from unreasonable searches and states that a defendant must demonstrate that he personally has an expectation of privacy in the place searched and that his expectation is reasonable. Riley was driving his car when he was stopped by police. A search of the car found a handgun. Riley was arrested as a result of this stop and police seized his smartphone. Smartphone records showed Riley's phone was used near the location of a shooting at around the time the shooting took place. The detective found photographs of Riley in front of a car that the police suspected had been involved in a shooting. The smartphone contained pictures of Riley making gang signs. At trial, Riley attempted to deny all the evidence collected from the warrantless search of his cell phone, contending that the searches of his phone violated the Fourth Amendment. The Fourth Amendment to the U.S. Constitution protects people from unreasonable government intrusions into their legitimate expectations of privacy and when a warrantless search is involved, the burden is on the prosecution to justify the search by proving the search fell within a recognized exception to the warrant requirement. Ultimately, the Court of Appeal affirmed, according to the decision in *People v. Diaz*,[12] which held that the Fourth Amendment permits a warrantless search of cell phone data incident to arrest if the cell phone was immediately associated with the defendant's person. The Supreme Court finally denied Riley's petition for review. Thus, the warrantless search of the cell phone was valid.

In China, we also have some regulations on evidence collection in emergencies and exigent circumstances. Article 136 of the Criminal Litigation Law of the People's Republic of China states that when an arrest or detention is carried out a warrantless search may be made in an emergency. Some people argue that the evidence from smartphones can be highly destructible and thus need to be preserved by a warrantless search. Newer smartphones and devices can be remotely disabled or remotely data wiped. The remote-wiping capability is available on all major smartphone platforms; and if the phone's manufacturer does not offer it, it can be bought from a mobile-security company. Apple's iPhone with the "Find My iPhone" app preinstalled. The app allows a user to remotely lock or wipe the phone. Expecting law enforcement officers to recognize in the field if the arrestee is carrying a phone capable of remote wiping is problematic because it requires officers to become smartphone experts. Some people maintain that requiring police officers to ascertain the storage capacity of a smartphone before conducting a search or seizure would be an unworkable and unreasonable rule.

Admittedly, if the evidence from smartphones is not properly preserved, it may be lost or destroyed, and it cannot be easily recovered. However, we still cannot use the exigency exception arbitrarily. Police may prevent a remote wipe from occurring by taking simple steps to protect the phone. Instead of using a warrantless search directly, one solution proffered is to require police to use a "Faraday bag" or a "Faraday cage" (essentially an aluminum foil wrap) or some equivalent, into which the device can be placed until a search warrant is obtained. This prevents smartphone signals from reaching a phone held inside, therefore eliminating the risk of losing evidence. Nowadays, it does not seem to be a tough thing to prevent overwriting of calls or remote wiping of information on a cell phone today. Instead, the evidence can be well protected by putting in a Faraday enclosure. Even if the data in the smartphone are lost or destroyed, the data itself may still be accessible later. Since the data may still be accessible, courts should find that searches performed because of the risks posed in waiting for a warrant incident to arrest are not required.

Accordingly, the exigency exception should be used in obtaining electronic evidence from smartphones. However, to safeguard against being used to violate the privacy of citizens, it is also of great importance to set a standard on exigency exception.

Consent to search exception

One exception to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent. Knowledge of the right to refuse consent to search is one factor to be taken into account, but the government need not establish such knowledge as the *sine qua non* of an effective, voluntary consent.[15] The Fourth Amendment recognizes a valid warrantless entry and search of premises when police obtain the voluntary consent of an occupant who shares, or is reasonably believed to share.[16]

If someone allows the police to search his smartphone, the police then have the right to search in the scope of consent. In the case of *Florida v. Jimeno*,[17] it was held that if police wish to search closed containers within a car, they need not request separate permission to search each container, although the suspect may place an explicit limitation on the scope of a search to which he consents. Because an individual's expectation of privacy with regard to the physical characteristic of smartphone itself is distinct from and far greater than, their expectation of privacy in the contents of their smartphone, it follows that an individual's consent to a search of their smartphone cannot necessarily be understood as extending to its private contents. Authority for third-party consent should be constrained to "shared rights," but it cannot transcend their scope of rights. For example, a mother may have authority to consent to a police search of a shared house, but she has no authority to consent to the search of items such as a briefcase and smartphones with private contents.

"Plain view" exception

One of the exceptions to the warrant requirement is "plain view." Items in plain view can be seized without a warrant. Not only must the police officer be lawfully located in a place from which the item can be plainly seen, but he/she must also have a lawful right of access to the item. The "plain view"

exception thus requires that: (1) the police have lawful access to the place from which the item can be plainly viewed; (2) that the items seized are in plain view at the time they are discovered; and (3) that it is "immediately apparent" to the police at the time of the discovery that the item constitutes evidence or fruit of a crime.

The "plain view" exception is mainly determined by the condition that the police finds the evidence without performing a search. This was affirmed in *Arizona v. Hicks*.[18] After the Arizona Supreme Court denied review, the State petitioned for *certiorari*. In the Supreme Court, Justice Scalia held that: (1) no "seizure" occurred for purposes of the Fourth Amendment, when the officer merely recorded the serial numbers of stereo equipment he observed in plain view; but (2) the officer's actions in moving equipment to locate serial numbers constituted a "search" which had to be supported by probable cause, notwithstanding that the officer was lawfully present in the apartment where the equipment was located.

In the electronic evidence of smartphones, the police need to search the entire contents of the smartphone for the specific evidence. Hence, in practical terms, there may be little difference between a specific warrant and a blank writ. For example, in the case of US *v. Carey*,[19] the Police seized images of child pornography from the defendant's computer hard drive, the search of which was not authorized by the warrant because the images were in closed files. They were not in plain view, but were instead seized pursuant to a general, warrantless search, where the warrant permitted only the search of the computer files for "names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." It was the contents of the files and not the files themselves which were seized, and it was evident from police officer's testimony that each time he opened a "JPG" file after the first, he expected to find child pornography and not materially related to drugs.[20] The evidence that was found in the computer was beyond the scope of the warrant. The aim of the search warrant may be taken into consideration in the application of the "plain view" exception. We can conclude that only by following the scope of the warrant can the police use the plain view exception to seize electronic evidence from smartphones.

Privilege Against Self-incrimination and the Encryption Key of Smartphones

When the police have a warrant to search a smartphone, they may have difficulty in gaining the encryption key to access its contents. Hon. Brian M. Hoffstadt has published a paper entitled *Encryption Technology Meets Fifth Amendment*. Judge Hoffstadt points out that forcing an arrestee to reveal an encryption key may impinge on a defendant's right against self-incrimination. However, the privilege against self-incrimination could potentially put encrypted data forever beyond the reach of law enforcement.

Preventing the swift destruction of smartphone evidence, i.e., the exigency exception, is an interest that could conceivably render the search warrant rule useless. With the emergence of simpler techniques to secure and encrypt the data on one's electronic device, the issue of smartphone search warrants may be short-lived, regardless of how the Supreme Court rules. "Encryption is an altogether different beast. In most cases involving encryption, police already possess the device containing the encrypted data; the problem is that they cannot read the data." In contrast to the Fourth Amendment warrant exception, "the privilege against self-incrimination has no warrant exception." In other words, future smartphones may automatically encrypt user data. Once the police cannot decipher the contents of the phone, the only solution may be to gain the encryption key from the arrestee. To do that, prosecutors could be forced to grant the arrestee immunity.

Recently, in the US, police has tried to challenge the limits of privacy in technology and government access to data. There are two typical cases in practice. One example is *FBI v. Apple*[21] with the case regarding Syed Rizwan Farook's iPhone, and another one is *State v. Stahl*.[22] In 2015 and 2016, Apple Inc., received and objected to or challenged many orders issued by US district courts under the All Writs Act of 1789. In these two cases, the FBI was unable to unlock a smartphone because Apple passcodes have an auto-erase setting following ten incorrect access attempts. Hence, the FBI requested a court order to compel Apple to help the FBI gain access to the contents of the iPhone by altering Apple's software and disabling the auto-erase function. However, Apple held that creating a "backdoor" would destroy years of Apple's efforts in creating security features that secure customers' personal data ranging from photographs to financial information.

In December 2015, Syed Rizwan Farook and Tashfeen Malik killed fourteen people and injured 22 others in a shooting in San Bernardino. The two attackers later died in a shootout with police, having first destroyed their personal phones. The work phone was recovered intact but was locked with a four-digit password and was set to eliminate all its data after ten failed password attempts.[23] The US government attempted to gain access to the content of Farook's iPhone. However, the iPhone was locked with a numeric passcode set by Farook. FBI wanted Apple to enable the FBI to unlock a work-issued iPhone 5C, the "subject device" pursuant to a warrant of this Court by providing reasonable technical assistance to assist law enforcement agents in obtaining access to the data on the subject device.[24] The FBI cited the All Writs Act[25] in its argument and requested a court order to compel Apple to accomplish the following three important functions: (1) it will bypass or disable the auto-erase function whether or not it has been enabled; (2) it will enable the FBI to submit passcodes to the subject device for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol available on the subject device; and (3) it will ensure that when the FBI submits passcodes to the subject device, software running on

the device will not purposefully introduce any additional delay between passcode attempts beyond what is incurred by Apple hardware.[26] Apple believes that compliance with this Order would be unreasonably burdensome and this will infringe people's privacy.

In December 2016, in the Case *State v. Stahl*, the Second District Court of Appeals of Florida granted the State of Florida's motion to compel the defendant's passcode to his iPhone 5. Stahl was charged with video voyeurism. A woman shopped in the store, and she then observed the man with his arm extended, holding the cellphone under her skirt. He confirmed the phone number and provided the location of the phone. A search warrant was issued for the contents of the described Apple iPhone 5. However, the State was unable to execute the warrant and view the contents of the phone because Stahl's cellphone is passcoded and he refused to give law enforcement the passcode. The police could not unlock it without the defendant's passcode. The District Court of Appeal held that the state established with reasonable particularity that defendant possessed the passcode, and the self-authenticating nature of the passcode.[22] The Fifth Amendment of the U.S. Constitution provides that "no person shall be compelled in any criminal case to be a witness against himself." This privilege against self-incrimination "protects a person only against being incriminated by his own compelled testimonial communications." Accordingly, it is extremely important to strike a balance between individual privacy rights and the need for law enforcement, and to gain access to electronic devices it must be established with reasonable particularity that they contain relevant evidence. At present, this balance is more significant than ever, with an individual's ability to encrypt their personal devices constantly improving, and investigative technology and surveillance more omnipresent and advanced than ever before.

Zeid Raad Al Hussein, the UN High Commissioner for Human Rights, held that if the Court enables the FBI to use software to access passcodes to subject devices for electronic testing, a Pandora's box could be opened. Some people also fear that the government and law enforcement agencies around the country would use this "backdoor" to gain access to data information in other devices. Even worse is the high risk that "hackers and cybercriminals" may obtain access to personal electronic information using the software. Ultimately, it will put personal electronic information at a high risk. If police can gain access to almost every aspect of a person's life by obtaining a warrant or exception of warrant search, it may easily infringe the privacy rights of citizens.

Conclusion

China, indeed, has not established rules about warrant search for smartphones. In the US, if the police wants to obtain information from smartphones, except in emergencies and exigent circumstances, they must have a search warrant from the court. Otherwise, the evidence would be excluded as illegal. Due to legislative omissions, it is difficult for investigators to search for electronic evidence from smartphones. With the use of electronic evidence, it is easy to infringe on other people's property, privacy, and other legal rights and it is more likely that the objectivity and authenticity of the evidence will be damaged. Hence, it is imperative that the legislation relating to the search of smartphones is improved. Our country should punish crime and protect human rights. The procedural rules of smartphone searches can be improved in practice by setting the authentication of the electronic evidence as the object of the search. The mechanism of judicial review and the writ principles can prevent investigators from abusing police power during a search, narrow the scope of the smartphone search, and protect the privacy of citizens. It is necessary to draw lessons from successful practices in the US and other countries to establish a perfectly legal mechanism of smartphone search to realize justice in the future China.

First, the procedure for search and seizure should follow the principle of proportionality. To protect the rights of citizens, the use of coercive measures and search should be limited. The principle of proportionality is made up of three parts: the principle of appropriateness, the principle of necessity, and the principle of equilibrium. The public interests which are enhanced by the means of exercising police power are proportionate to the harm and restriction of citizens. It is helpful to use the principle of proportionality to restrict the power of government. The examination and approval procedures shall be strictly followed, and strict restrictions shall be imposed on the scope of smartphone search cases, collection subjects, duration, process and times, thus ensuring that the collection procedures are legal. Obeying the principle of proportionality is a good way to strike a balance between the power of a search and the protection of human rights.

Furthermore, we must clarify the definition of a smartphone search and follow the writ principles and regulations. If the police want to initiate a smartphone search, they need to have a warrant issued by the judicial body first. Otherwise, unless in conformity with an exception to the legislative conditions, the evidence obtained will not be admissible and should be ruled out in accordance with the law. In terms of the subject of judicial review, according to the experience of the rule of law abroad, especially in the cases of *Riley* and *Wurie*, the court should be independent and neutral. As the court is a neutral judgment body, it does not assume the responsibility of either prosecution or defense in criminal procedure law. If a neutral court acts as a review body, it will be most conducive to preventing the abuse of police power in searches, thus effectively protecting the privacy of citizens.

Moreover, in terms of the scope of smartphone searches, clear limits are required for both the investigative body carrying out the search and the judicial body issuing the search warrant. These limits are necessary for the collection of criminal evidence and the arrest of the criminal, and should clearly include the objective evidence requirements. The legislation should clearly stipulate

that only if the application of the investigative body meets the following conditions can the judicial body issue a smartphone search warrant: (1) there is evidence of the occurrence of the crime; (2) the electronic evidence in the smartphone which is to be searched can help to prove the facts of the crime; and (3) smartphones may store documents, pictures, video, or other electronic evidence, and this evidence should be an objective form of evidence, not a subjective one.

In addition, it is necessary to establish a sound monitoring mechanism. Without judicial authorization, the search will illegally violate the person's right to privacy. To prevent investigators from abusing their power to search electronic evidence and to reduce the violation of citizens' privacy rights, in China, it is of great necessity to make laws and regulations to specify that the search of electronic data stored in smartphones should be carried out by at least two investigators. This shall be an effective approach to monitor the behavior of investigators and prevent illegal, improper searches for random purposes. There should also be a witness to the search. Because data held on smartphones tend to be very small and inconspicuous, video recording usually only captures the general process of a search, and it is difficult to record details and contents displayed on the screen of a smartphone. When a witness is present, the whole process of the smartphone search can be supervised to restrain any illegal or improper behavior of investigators.

Finally, we need to establish a procedural sanction mechanism. The electronic evidence from a smartphone which is collected by illegal ways should be excluded. To prevent investigators from obtaining electronic evidence illegally and to protect citizens' privacy, it is necessary to establish and improve rules exclusive to illegal evidence. Because of the different degrees of infringement of citizens' right to privacy, the exclusion of illegal electronic evidence from smartphones can be divided into two parts: absolute exclusion and relative exclusion. Absolute exclusion means that the electronic evidence obtained from a smartphone has fundamentally violated the search rules and should be ruled out. This kind of evidence cannot be corrected or reasonably explained; therefore, it must be excluded. Relative exclusion means that the violation of the search rules is not fundamental and urgent. The investigator can make some corrections or make a reasonable explanation to prove that the electronic evidence is true to prevent it from being excluded. In other words, searching the data from a smartphone which is not in conformity with search procedure may seriously affect the justice of the case if corrections or a reasonable explanation are not provided and the evidence is excluded. To protect the human rights and privacy of individuals, it is of great importance to establish a procedural sanction system to exclude any illegal evidence which is collected during an investigation.

By following the example set by other countries China could gain a new perspective on the use of electronic evidence. Exploring the legal way to search electronic evidence from smartphones might be a good start to an improvement in the administration of justice in China.

Financial support and sponsorship

Nil.

Conflicts of interest

There are no conflicts of interest.

References

1. Copland v. United Kingdom, 45 Eur. Ct. H.R. 253, § 43 (2007).
2. Lemmens K. The protection of privacy between a rights-based and a freedom-based approach: What the Swiss example can teach us. Maastricht J Eur Comp 2003;10:381-4.
3. GPS Investigations in Japan, and Privacy Concerns. Available from: https://www.insidegnss.com/gps-investigations-in-japan-and-privacy-concerns/. [Last accessed on 2019 Feb 19].
4. Westmoreland C. Police and Privacy: A Comparison of Search and Seizure Protection in the United States and Korea, Available from: https://www.ftc.gov/system/files/documents/public_comments/2017/12/00005-142667.pdf. [Last accessed on 2019 Feb 19].
5. Aljneibi K. Search and seizure for electronic evidence: Procedural aspects of UAE's legal system. Digit Evid Electron Signature Law Rev 2013;10:115.
6. State v. Granville, 423 S.W.3d 399, 408 (Tex. Crim. App. 2014).
7. United States v. Wurie, 728 F.3d 1 (1st Cir. 2013).
8. O'Connor, E. The search for a limited search: The first circuit denies the search of cell phones incident to arrest in United States v. Wurie. Boston Coll Law Rev 2014;59:63.
9. United States v. Robinson, 414 U.S. 218 (1973).
10. United States v. Young, 278 Fed. Appx. 242, 245 (4th Cir. 2008).
11. United States v. Finley, 477 F.3d 250 (5th Cir.2007).
12. People v. Diaz, 51 Cal. 4th 84 (2011).
13. State v. Thomas, 280 Kan. 526, 124 P.3d 48 (2005).
14. Riley v. California, 132 S.Ct. 94, 181 LEd.2d (2014).
15. United States v. Drayton, 536 U.S. 194 (2002).
16. Georgia v. Randolph ,547 U.S. 103 (2006).
17. Florida v. Jimeno, 500 U.S. 248 (1991).
18. State v. Hicks, 146 Ariz. 533, 707 P.2d 331 (App. 1985).
19. United States v. Carey, 172 F.3d 1268 (1999).
20. Curtis G. The Law of Cybercrimes and Their Investigations. London and New York: CRC Press; 2011.
21. In re order requiring Apple, Inc. to assist in the execution of a search warrant issued by this Court,149 F.Supp.3d 341 (2016).
22. State v. Stahl, 206 So. 3d 124 (2016).
23. What You Need to Know about the FBI v. Apple iPhone Case. Available from: https://www.hulseyiplaw.com/n-know-fbi-v-apple-phone-case/. [Last accessed on 2019 Feb 19].
24. Tanfani J. Race to unlock San Bernardino shooter's iPhone was delayed by poor FBI communication, report finds. The Los Angeles Times; 18 August, 2018.
25. Apple v the FBI: Why the 1789 All Writs Act is the wrong tool. Available from:https://www.theguardian.com/technology/2016/feb/24/apple-v-the-fbi-why-1789-all-writs-act-is-the-wrong-tool. [Last accessed on 2019 Feb 19].
26. Kerrigan H. Historic Documents of 2016. U.S.: CQ Press; 2017.