Investigating the uses of mobile phone evidence in China criminal proceedings

Aolan Zhang, Ben Bradford, Ruth M. Morgan, Sherry Nakhaeizadeh

PII: S1355-0306(22)00047-8
DOI: https://doi.org/10.1016/j.scijus.2022.03.011
Reference: SCIJUS 1032

To appear in: *Science & Justice*

Received Date: 26 October 2021
Revised Date: 23 March 2022
Accepted Date: 28 March 2022

Investigating the uses of mobile phone evidence in China criminal proceedings

Aolan Zhang[a,b*]; Ben Bradford[a]; Ruth M. Morgan[b]; Sherry Nakhaeizadeh[b]

[a] Institute for Global City Policing, Department of Security and Crime Science, University College London, 35 Tavistock Square, London WC1H 9EZ, United Kingdom

[b] Centre for the Forensic Sciences, Department of Security and Crime Science, University College London, 35 Tavistock Square, London WC1H 9EZ, United Kingdom

* Corresponding author: aolan.zhang@ucl.ac.uk

Abstract

Data from mobile phones are regularly used in the investigation of crime and court proceedings. Previously published research has primarily addressed technical issues or provided operational manuals for using forensic science evidence, rather than analysing human factors and the implementation of forensic tools in investigation settings. Moreover, previous research has focused almost entirely on western countries, and there is a dearth of research into the uses of forensic evidence in China. In this study, a review was carried out of court sentencing documents referring to mobile phone evidence in China over the period 2013-2018. Automated content analysis was used to identify the specific evidence types utilised and the sentencing outcome for each case. Results show that mobile phone evidence was used in 3.3% of criminal proceedings. Among various data types mentioned in criminal proceedings, call records sustained as the most frequently used type of data. After which, instant messaging tools (e.g. WeChat) are an increasing proportion of all mobile phone evidence, from 1% in 2015 to 25% in 2018. For cases that utilised mobile phone data, the analysis of instant messaging and online transaction tools is routine, with little variation in the use of each application (WeChat, Alipay, QQ) for investigations of different types of crime. However, in the majority of criminal cases, mobile phone data function as subsidiary evidence and posed limited impacts on verdict reached. The current findings indicate that a large amount of mobile phone evidence is transformed into other evidence formats or filtered out directly before court proceedings.

Keywords: Mobile phone evidence; Digital forensics; Criminal proceedings; Automatic content analysis

1. Introduction

Information technologies have made many tasks more efficient and easier, but at the same time, they have introduced new opportunities for offending [1, 2, 3]. The proliferation of mobile phones and their increasingly advanced capabilities have embedded the use of mobile devices in a broad range of criminal activities [1, 2]. As a result, there has been an increase in the analysis of data from mobile phones and other digital devices in criminal investigations and the generation of evidence for court proceedings[4, 5].

Currently, multiple forensic tools allow police and others to extract data from mobile devices and produce evidence reports admissible for court. At the same time, growth in the number of cases, the number of related devices per case, and the amount of data stored in each device creates a ‘big forensic data’ challenge for legal professionals [6, 7]. Although the increasing value of mobile phone evidence has been recognized by police and academia, previously published research into digital forensic science mainly focuses on technical issues or tactics in forensic examinations, rather than the actual practice of using mobile phone data in investigations and prosecutions [4, 8, 9, 10]. However, considering the different features of crime in the physical and digital worlds, and rapid changes in technology, it is very challenging for investigators and forensic examiners to develop the breadth of specialist knowledge and skills needed to identify and interpret all these digital forms of evidence [11, 12]. Thus, understanding how mobile phone data have been used by law practitioners can offer insights for future policy [4, 13]

Using the information stored in a mobile phone is not an independent task; to understand how such data is used it is necessary to fit this task into the whole forensic science process [14]. The forensic process can be summarised into four stages: crime scene; analysis; interpretation; and production of intelligence or evidence [15]. From the crime scene to the court, each stage influences the others[16]. For example, information accessed in previous stages influences the knowledge generated in later stages [17, 18]. It is thus critical to locate uses of mobile phone evidence in the context of the whole forensic process.

Some empirical research has analysed the demand for mobile phone evidence in investigations, and reviewed court proceedings where this evidence has been admitted, in order to explore the extent to which mobile phone evidence has been used in criminal cases [4, 5, 7]. Turnbull et al. [4] and Quick and Choo [7] examined cases where requests for processing electronic evidence were made to the Electronic Crime Section (ECS) of South Australia Police between 2006-2009 and 2006-2015, respectively. The findings by Quick and Choo [7] indicated that from 2006 to 2015, the number of cases that requested analysis of electronic evidence increased from 268 to 1417, with the number of mobile phones examined increasing from 103 to 2846. The study also highlighted that about 60% of all devices storing electronic data that was analysed were mobile phones.

Exploring beyond the use of mobile phone data during investigations, McMillan et al. [5] demonstrated increasing use of mobile phone evidence in court proceedings. McMillan et al [5] focussed on appellate judgments in the court of appeal from 2006 to

2011 in England and Wales. During this period the number of cases that employed mobile phone evidence increased from 51 to 157. However, the total number of criminal cases or the proportion of cases that employed mobile phone evidence was not provided. It is thus difficult to identify the real growth in criminal cases that have used mobile phone evidence. Yet, the number of cases that have used mobile phone evidence in court proceedings is likely to be far lower than the number of investigations that produce and uses such evidence [4, 7].

Although it is difficult to estimate the contextual factors that may influence the uses of evidence [19], some common uses of mobile phone evidence have been identified. McMillan et al. [5] demonstrated that among 121 cases that used SMS evidence, 40 related to drug crime, and of the 86 that involved images and videos as evidence, 48 were sexual offence cases. Among 181 cases that employed call records in evidence, 163 used this type of data to identify co-conspirators. In addition, in 20 out of 33 cases that utilised cell-site analysis were used to prove or disprove an alibi. However, the inductively selected keywords guiding this study might have overlooked applications that were not popular throughout the research period. As a result, the number of incidents could be underestimated.

McMillan et al., [5] also evaluated the importance of mobile phone evidence in criminal cases by carrying out quantitative content analysis. The quantitative content analysis identified that mobile phone data were most often used with other forms of evidence to support a conviction, and they were not greatly relied upon the criminal proceeding. Therefore, although mobile phone evidence is increasingly being looked at in investigations and referred to in court proceedings, in some types of crime, this evidence has not had a significant influence on the final judgements handed down [5].

New technologies that can facilitate and enable crime are constantly developing and becoming available. It is thus necessary to revisit and consider the extent to which mobile phone evidence has been used, and explore the factors which may influence this use. By understanding how these data are used across the whole investigation process the challenges faced by legal professionals can be identified and corresponding technical or personnel support needed can be identified [5, 9, 10, 20, 21]. Such research can further provide empirical evidence which could support decision-making regarding allocations of experts, funding or facilities, and ways to deliver training[22, 23, 24].

Previously published studies have generally focussed on the uses of mobile phone evidence in so-called WEIRD (Western, Educated, Industrialised, Rich, Democratic) countries [25]. Therefore the findings from these studies may not generalise to other countries. This study was designed to address this by investigating the use of mobile phone evidence in China, as a very different context to previous studies and to pave the way for future efforts to compare the use of evidence from mobile phones in different countries.

China has a large population, intensive infrastructure development for mobile networks, and has witnessed a significant expansion of the population of ‘netizens’ who access the internet via mobile networks. Mobile phones have become an all-in-one solution for internet users [26] and in contrast to the strategies employed by western cybercriminals, the darknet is not a tool widely utilised in China [27, 28]. Instead, instant messaging tools, like QQ, are more commonly used [27].

Moreover, China shares a different internet community to other countries, owing to censorship and blocks that are put in place which limits access to some websites [29, 30, 31]. This has led to some users utilising Virtual Private Networks (VPNs) or a proxy to circumvent censorship [31]. However, there is still a large amount of the population that does not have access to information outside the firewall or use VPNs [32]. Limiting external access has led to the development and expansion of domestic social media tools, for example WeChat and QQ, which offer functions similar to WhatsApp. These tools provide multiple services that can offer users access to a range of capabilities spanning entertainment to social infrastructure tools such as governmental logistical services, which the public rely on in their day to day lives [33]. Given the specific context within China, legal professionals face challenging situations when seeking to utilise mobile phone evidence, whether in a collection of the vast quantities of data involved or in terms of presenting it to the court.

For this reason, this study seeks to address mobile phone evidence used in criminal proceedings in China between 2013-2018 in order to assess:

1) What proportion of all criminal cases employed mobile phone evidence in 2013-2018?
2) When mobile phone evidence is used, what crime types and mobile phone data types tend to be involved?
3) Are different types of evidence associated with specific types of criminal proceedings?
4) How important is mobile phone evidence to the inference of criminality in criminal proceedings?

2. Methods

In China, descriptions of crimes tried in court and the evidence used in court proceedings are recorded in judgement files and made publicly available. These documents can therefore provide information on the scenarios in which mobile phone evidence is used. In 2012, digital evidence, including mobile phone evidence, was included as a legal format of evidence in the Criminal Procedural Law (CPL). Due to the time required to upload from the database, a dataset was created of cases heard between 2013 and 2018 for this study. To provide a general understanding of the common uses of mobile phone evidence across various types of crime investigation, the quantitative associations between types of mobile phone data and types of criminal cases was tested.

In order to summarise the quantitative characteristics of mobile phone evidence used in the criminal judgement files, automated content analysis was used to identify the number of judgement files containing keywords relating to crime and evidence. Keywords were identified to aggregate similar incidents to develop a quantitative overview of the features of mobile phone evidence used in criminal proceedings. A computer-based content analysis was used due to the large sample size (N=1931). To ensure objects indicated by the presence of keywords could be accurately represented (e.g. that the keyword 'text message' actually represented the use of text messages as a part of evidence), the automatic analysis script was designed to search keywords in given certain sections of judgement files, according to the structure in which practitioners are accustomed to recording criminal proceedings.

2.1 Data collection

The case judgement files to be analysed were downloaded from China Judgement Online (http://wenshu.court.gov.cn/), an open online database operated by the Supreme Court of China. As it is required by law[1], all judgements rendered by people's courts are made available online, except where the cases involve state secrets or juvenile delinquency [2]. Therefore, this database offers a valuable dataset that reflects the general nature of detected crime among adults in China, which includes specific descriptions of the evidence presented by the prosecution.

Each judgement in the database is comprised of headings (title and case reference), facts (crime facts), reasons (evidence), judgement result (decisions from the procuratorate), and conclusion (sentences). In the 'reasons' section, each piece of evidence is numbered and described within a general evidence category specified in the CPL. Based on this rule, the advanced searching query tool embedded in the database was populated with the keywords in Table 1. All the cases identified with these keywords were downloaded and stored.

Items in the query	
Keywords	Mobile phone[3]

[1] Article 3 from Provisions of the Supreme People's Court on the Issuance of Judgments on the Internet by the People's Courts

[2] Article 3 from Provisions of the Supreme People's Court on the Issuance of Judgments on the Internet by the People's Courts

[3] In Chinese, the words "mobile phone" does not have many alternative forms as might be the case in English, and the judgement files that formed the data utilised in this study use "mobile phone" ("*shou ji*" in Chinese). With only "mobile phone" ("*shou ji*") in the searching query, all cases that mentioned mobile phone, smartphone or other paraphrases can be identified.

Section for searching keyword	Reasons
Types of cases	Criminal cases
Types of documents	Judgement file
Types trial	Criminal prosecution
Level of the court	Intermediate court
Procedure of trial	Trial of the first instance
Date of prosecution	2013.01.01-2018.12.31

Table 1 Keywords and settings populated in the searching query

As the criminal investigation was the focus of this study, the searching query specified the type of cases and trial (the crime was accused in a criminal or civil case) as “criminal cases” and “criminal prosecution” respectively. To exclude large volumes of low impact ‘petty crime’, this research limited its scope to the “Intermediate court”. In addition, to avoid redundant information, only first trial cases were kept. Judgements from higher people’s courts and the supreme court were also excluded, since these courts will only accept cases in the first trial that are regarded as significant in a province or nation-wide[4].

The search returned 2204 cases in the online database that met the search terms. Some cases failed to be downloaded from the dataset, since there were issues like ‘garbage display’ and blank content of the downloaded files. Therefore, a final dataset of 1931 criminal cases that employed mobile phone evidence was created for content analysis.

2.2 Coding of the analysis script

To analyse the situations and context in which mobile phone evidence is used in criminal proceedings, it was necessary to identify the specific types of mobile phone data employed, and the type of crime. Owing to the large sample size, this study employed Python scripts (3.8.5) to read those judgement files with PyCharm (Edition 2020.2.1). To replicate as closely as possible the mechanism of how humans read, to re-articulate the content in the script, and deal with the format in which judgement files are normally recorded, the script to identify certain sections of the files (including the introduction, evidence, sentencing) was written based on the common framework and expressions frequently used by and taught to practitioners [34]. Although the manual by Hu [34] suggested many formal phrases to introduce each section of a judgement file, there were many variations in the actual wording.

[4] CPL article 22 and 23

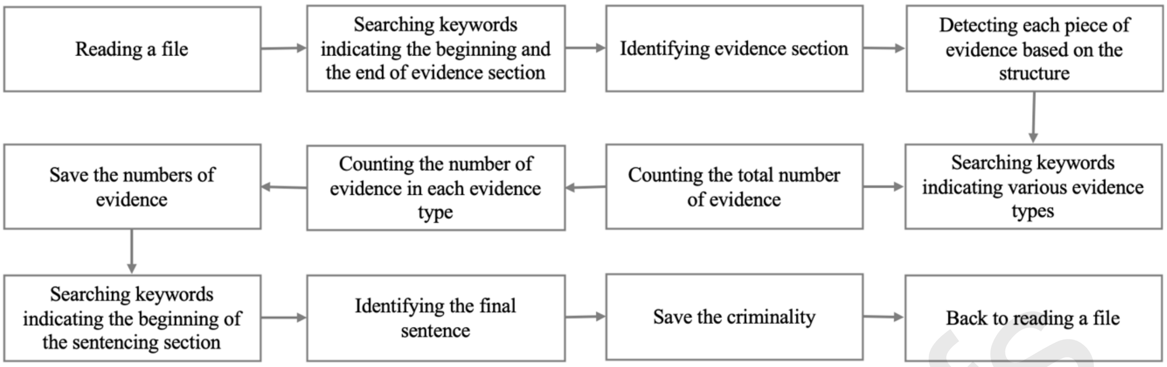
Reading a file
Searching keywords indicating the beginning and the end of evidence section
Identifying evidence section
Detecting each piece of evidence based on the structure
Searching keywords indicating various evidence types
Counting the total number of evidence
Counting the number of evidence in each evidence type
Save the numbers of evidence
Searching keywords indicating the beginning of the sentencing section
Identifying the final sentence
Save the criminality
Back to reading a file

Figure 1 The flow chart of python script to identify crime and evidence types

To enrich the keyword dictionary in the script and enable flexibility in information extraction, common patterns of expressions were identified by manually reading, and then used to set the rules in the automatic reading script. Specifically, 5% of sample cases were randomly selected and manually analysed to summarize the common patterns and keywords employed by judgement files. Given that a judgement file follows a certain structure, and each piece of evidence is recorded and listed in an individual paragraph of the evidence section, the basic mechanism of the Python script was designed as is shown in Figure 1. When the analysis was completed for all documents, the script saved all the results in a table for further analysis.

Evidence types (translated)	**Keywords**
1. Call records	1.1 Call records
	1.2 Lists of calls
	1.3 Lists of calling history
	1.4 History of calls
	1.5 Details of call records
2. Contact list	2.1 Contact list
3. Text message	3.1 Text message
4. Photographic evidence	4.1 Mobile phone photos
	4.2 Mobile phone album
	4.3 Album photo
	4.4 Mobile phone snapshot
	4.5 Album video
5. Audio-recordings	5.1 Audio- recordings
6. Cell-site analysis	6.1 Cell-site location
	6.2 Cell-site analysis
	6.3 Mobile phone location information
7. Notes	7.1 Notes
8. WeChat	8.1 WeChat
9. AliPay	9.1 AliPay

10. QQ	10.1 QQ
11. Facebook	11.1 Facebook
	11.2 facebook
	11.3 *Lian shu*[5]
12. WhatsApp	12.1 WhatsApp
	12.2 WhatsApp
13. Other foreign apps	13.1 Twitter
	13.2 Instagram
	13.3 VPN
	13.4 Gmail
	13.5 Telegram

Table 2 Keywords employed in the script

Keywords were selected and coded by manual reading, to avoid keywords that indicate multiple objects [35, 36, 37]. The keywords used to identify objects, and the corresponding ways to categorise evidence, were based on descriptions of evidence included in the CPL, and characteristics frequently used to describe each object in judgement files that had been identified within the sample cases. With this pre-processed result, this study focussed on the evidence types and crime types (outlined in Table 2) which had been identified as the most frequent types in the sample files. There are many additional types of data from different mobile phone applications, but these did not feature in the judgement files and therefore were beyond the remit of this study. However, to investigate whether there were any applications mentioned in evidence that, in theory, cannot be used with the network in mainland China, the script included keywords indicating non-mainstream applications, e.g., Facebook, WhatsApp (see Table 2, item 13).

Crime types (translated)	**Specific criminality in the sentence**
1. Drug-related crime	1.1 Smuggling, trafficking, transporting, manufacturing drugs
2. Sexual offences	2.1 Rape
	2.2 Molests
3. Fraud	3.1 Fraud
4. Violent crime	4.1 Intentionally killing
	4.2 Intentionally injuring
	4.3 Negligently causing death
	4.4 Negligently injuring
	4.5 Kidnapping,
	4.6 Human trafficking

[5] The Chinese words which directly translated from "face" and "book"

5. Property crime	5.1 Robbery[6]
	5.2 Theft
6. Corruption	6.1 Crime of graft
	6.2 Crime of bribery
7. National security-related crime (Terrorism)	7.1 Organising or leading a terrorist organization
	7.2 Advocating terrorism or extremism or instigating terrorist activities
8. Crimes of undermining the order of the socialist market economy (Market-related crime)	8.1 Crimes of smuggling
	8.2 Crimes of financial fraud
	8.3 Crimes of disturbing market order

Table 3 Categorisation of crime types[7]

Eight main crime types were identified in the judgement files; namely drug-related crime, sexual offences, fraud, violent crime, property crime, corruption, national security-related crime, and crimes of disrupting market order (Table 3). For the cases with more than one sentence, the script only kept the first result, i.e., the crime listed first in the result section was regarded as the index crime. For the majority of cases with more than one sentenced crime, the crime types were similar (for example, possession of drugs and drug trafficking). The number of cases that included more than one type of crime was limited[8].

This categorization of crime types aligns with the terms used in the original online database, which is also how Criminal Law in China categorises criminal crimes. However, as Criminal Law categorisation is relatively general, (for example, intentionally killing or injuring another and rape are categorized as “crimes of infringing upon the rights of persons and the democratic rights of citizens”), some of these general categories were refined into more specific ones. This process followed previous research which indicated an association between evidence types and crime types. For example, both studies by Turnbull et al. [4] and McMillan et al. [5] listed drug-related crime and sexual offences separately. Furthermore, in the research by Turnbull et al. [4], fraud was also analysed individually. Therefore, the script coded all crimes related to drugs, rape or sexual harassment, and fraud as drug-related crimes, sexual offences, and fraud respectively. In addition, violent crime in this study includes intentionally killing, intentionally injuring, negligently causing death, negligently injuring, kidnapping, and human trafficking, according to the original crime categories

[6] Robbery in this research refers to both robbing property using force, coercion or other methods (*qiang jie*) and seizing property without the owner’s awareness (*qiang duo*) which are mentioned respectively as two criminalities in the article 263 and 267 of the Criminal Law.

[7] This categorisation only included criminalities mentioned in judgement files collected. In other words, crimes not mentioned were not categorised in this table.

[8] There were 34 cases with different crime types in the sentence, 30 of these were for the primary crime of murder accompanied by theft.

provided by the database. As previous research [4] analysed fraud separately, this research also divided fraud from all other property crimes, like robbery and theft, and regarded these two types of crimes as property crimes for further analysis. This research also maintained the original categorisation of corruption, crimes of undermining the order of the socialist market economy, and crimes of endangering national security.

2.3 Coding scheme of evidence weight

To investigate the degree to which mobile phone evidence may influence court decisions, this study employed the indicator *evidence weight* to categorise each case based on the importance of the mobile phone evidence (as originally presented by McMillan et al. [5] and Berman et al. [38]). For this analysis by manual reading, 20% of cases in each year were chosen at random, which resulted in 390 cases being analysed. The criteria for evidence weight at each level were:

- High: Cases graded with high evidence weight indicate that mobile phone evidence employed in the case was vital to the outcome. For example, cases that record thorough analysis of mobile phones, with outcomes of that analysis making a direct contribution to the reconstruction of events, demonstrate intention or to disprove crime facts, would be coded as high evidence weight.
- Medium: Cases graded with medium evidence weight indicate that mobile phone evidence was used to strengthen or support other evidence or facts not directly related to sentencing. For example, cases would be categorised as medium weight if mobile phone data was only a subsidiary part of the prosecution, or related to factors (like relationships between individuals) that evidence could prove or disprove but which were not related to the final sentencing or conviction.
- Low: Cases graded with low evidence weight indicate that mobile phone evidence was only mentioned in the judgement file but not discussed further. For example, some cases only include a mobile phone as physical evidence without using data stored in it, and also some cases only mentioned a mobile phone in the confession of suspects or testimony of a witness.

There are no specific coding procedures in previously published research. Therefore, the code framework for this study was built, reflecting the criteria above, to specify the decision procedures of coding each case. The refined coding scheme with specific criteria is shown in Figure 2.

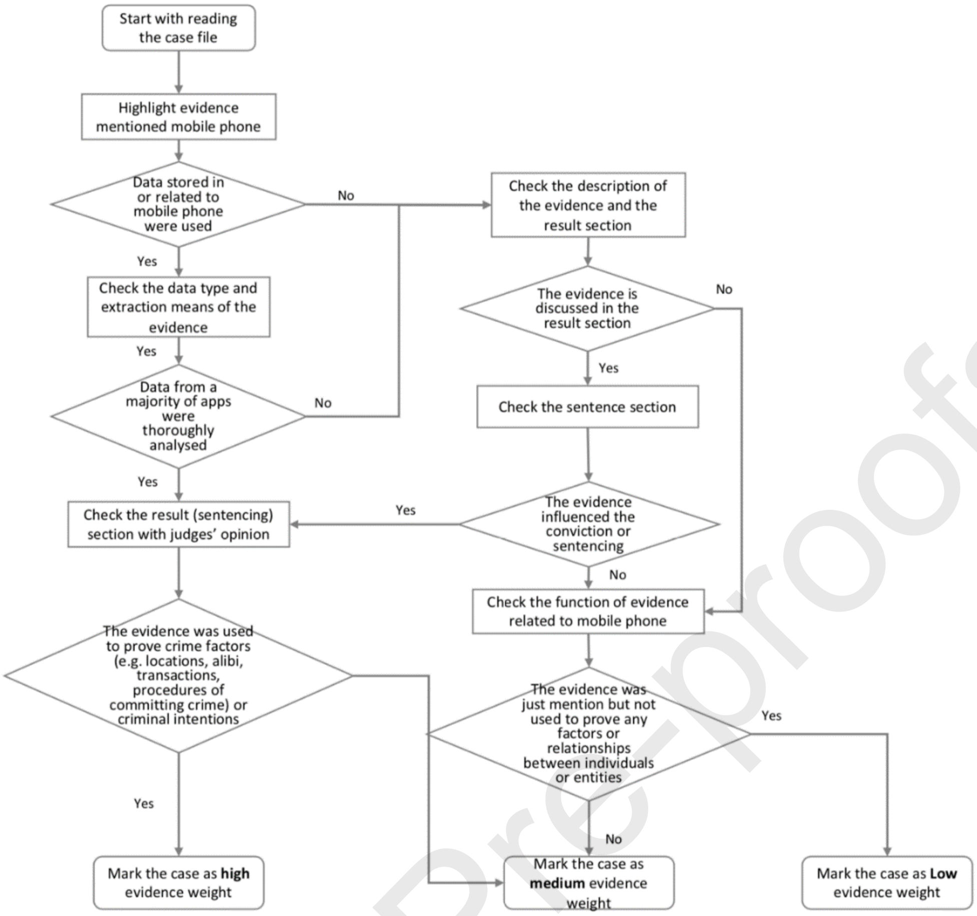
Start with reading the case file
Highlight evidence mentioned mobile phone
Data stored in or related to mobile phone were used
No
Yes
Check the data type and extraction means of the evidence
Yes
Data from a majority of apps were thoroughly analysed
No
Yes
Check the result (sentencing) section with judges' opinion
The evidence was used to prove crime factors (e.g. locations, alibi, transactions, procedures of committing crime) or criminal intentions
Yes
Mark the case as high evidence weight
Check the description of the evidence and the result section
The evidence is discussed in the result section
No
Yes
Check the sentence section
The evidence influenced the conviction or sentencing
Yes
No
Check the function of evidence related to mobile phone
The evidence was just mention but not used to prove any factors or relationships between individuals or entities
Yes
No
Mark the case as medium evidence weight
Mark the case as Low evidence weight

Figure 2 The coding scheme employed to assess evidence weight

2.4 Analysis

To test the associations between each type of mobile phone evidence and crime type, binary logistic regression models were estimated using Stata 11. To provide further insights from the binary logistic regression models, this study also applied the margins command to calculate the predicted probabilities for hypothetical cases (i.e. combinations of crime type and evidence type) [39].

3. Results

With the script automatically identifying keywords and aggregating incidents according to the coding scheme, the final output of the automatic analysis provided year, number of evidence used in total, number of evidence related to mobile phones, number of evidence used for each evidence type, and crime type.

3.1 Proportion of criminal cases employed mobile phone evidence

To provide a baseline to measure the extent to which mobile phone evidence was used in criminal proceedings, the searching query (in Table 1) was run again but without the keyword “mobile phone” to check the total amount of incidents in the research period. This process identified a total of 66,552 cases. Comparing the number of criminal cases with and without mobile phone evidence for each year (Table 4), the proportion of cases that employed mobile phones is shown in Figure 3. The numbers are all raw numbers provided by the online database in which cases that failed to be downloaded and were not applicable for further content analysis are included. As these cases still included mobile phone evidence, they were included in the total number but not used for further analysis. As Figure 3 shows, there was a slight growth, from 2015, in the proportion of criminal cases in which mobile phone evidence was used. However, mobile phone evidence was not particularly prevalent in criminal court proceedings, with less than 4% of cases throughout the research period using this type of evidence.

Year	*All Incidents*	*Incidents with mobile phone (%)*
2018	17402	665(3.82)
2017	17427	626(3.59)
2016	13483	425(3.15)
2015	8166	240(2.94)
2014	8050	198(2.46)
2013	2024	50(2.47)
Total	**66552**	**2204(3.31)**

Table 4 Incidents in each year

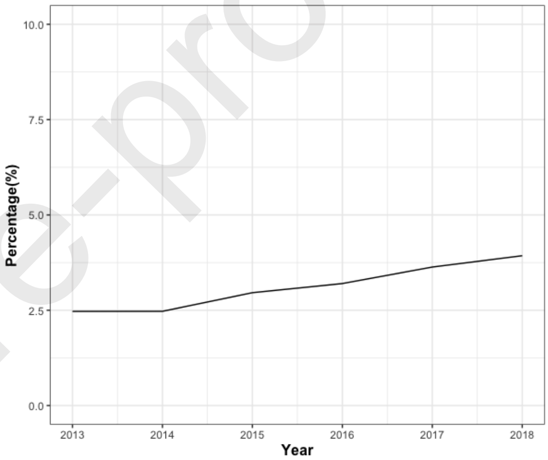

Figure 3 Proportion of cases that employed mobile phone evidence

3.2 Crime types involved in cases employing mobile phone evidence

After the cases that failed to be downloaded and cases whose evidence section cannot be analysed were excluded, the dataset comprised 1931 cases. As a result, the total number of cases employing a mobile phone is different from the original case number provided in the database (Table 4). Based on the categorisation of crime (see Table 3), the total number of cases in each category in the original online database is presented in Table 5, with the proportion of cases that used mobile phone evidence in each crime type. Figure 4 provides a visualised comparison of these percentages.

Crime type	*Total cases*	*Used mobile phone evidence (% of total)*
Drug-related	19029	1275 (6.70)
Violent crime	17680	336 (1.90)
Market	3066	165 (5.38)
Property	3066	66 (2.15)
Fraud	2114	64 (3.03)
Sexual offences	355	10 (2.82)
Terrorism	30	8 (26.67)
Corruption	2244	7 (0.31)
Total	**47584**[9]	**1931**

[9] The number of cases under each crime type was calculated based on the crime types identified by the original online database. Since some cases did not identify the crime types this research focuses on, or

Table 5 Numbers and proportions of cases that used mobile phone evidence in different types of crime

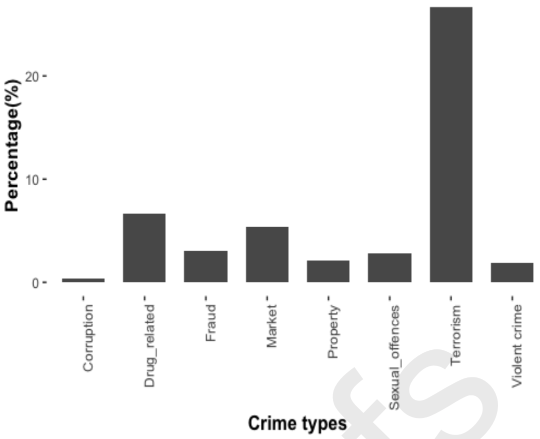

Figure 4 Proportion of cases that used mobile phone evidence in each crime type

Among cases that employed mobile phone evidence, drug-related crime comprises the largest number of incidents. Among all drug-related crimes in the research period, 6.7% employed mobile phone evidence. Although 26.7% of terrorism cases involved mobile phone evidence, there were only 30 terrorism cases in the entire database. In contrast, even though the database included 2,244 corruption cases, just 0.3% of them employed mobile phone evidence.

3.3 Types of data included in mobile phone evidence

Based on the descriptions of evidence in the judgment files, this study identified the exact information mentioned in each piece of evidence. For each case, the script counted the total number of pieces of evidence mentioned in court proceedings and the number of evidence in each type of mobile phone data.

Figure 5 presents the 11 formats of mobile phone data used as evidence. Among all types of data included in this study, call records were referenced most extensively. Among cases that recruited mobile phone evidence, there are 4,000 pieces of evidence relating to call records (i.e., more than two per case). Following call records, evidence related to WeChat and text message was also relatively frequent, with 1,239 and 865 pieces respectively. In comparison to these two methods by which mobile phone users send messages, QQ, another instant messaging application prevalent in China, was not as commonly mentioned in evidence. The only category related to payment is AliPay, an online payment application. Data or information related to AliPay were found in 405 pieces of evidence.

Audio recordings, notes on mobile phones, and cell-site analysis were seemingly rarely used in criminal cases. These three types of evidence were used less than fifteen times in the six years of cases in the dataset. Even when keywords indicating foreign applications that are blocked by the Great Firewall Project were added, there was only one piece of evidence related to Facebook. Apart from this, no other keywords relating to banned applications or VPNs were identified.

no mobile phone evidence is used in these cases, the total number of cases here is different from the total criminal case number in Table 4.

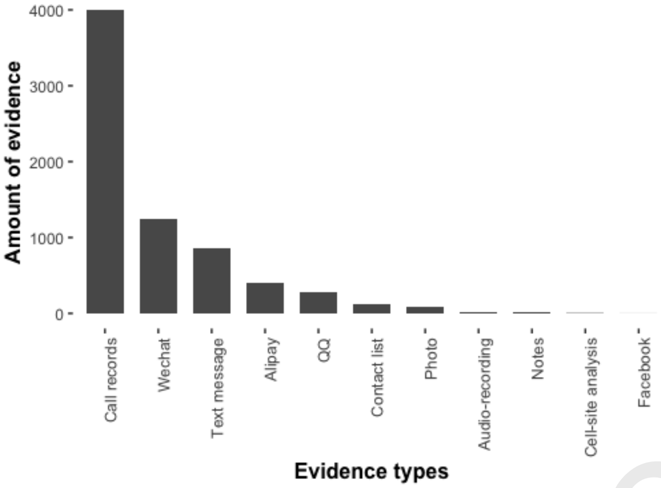

Figure 5 Amount of evidence for each category

To specify changes in the use of each type of mobile phone evidence across the research period, Figure 6 provides a comparison of the proportion of each data category in all mobile phone evidence for each year. Call records remained the predominant type of evidence, accounting for 40%-50% of all mobile phone evidence recruited in criminal cases in each year between 2013 and 2018. The proportion of WeChat evidence grew significantly after 2015, from 1% to 25%. At the same time, evidence relating to Alipay accounts for an expanding proportion of all mobile phone evidence after 2015, reaching 6% in 2018.

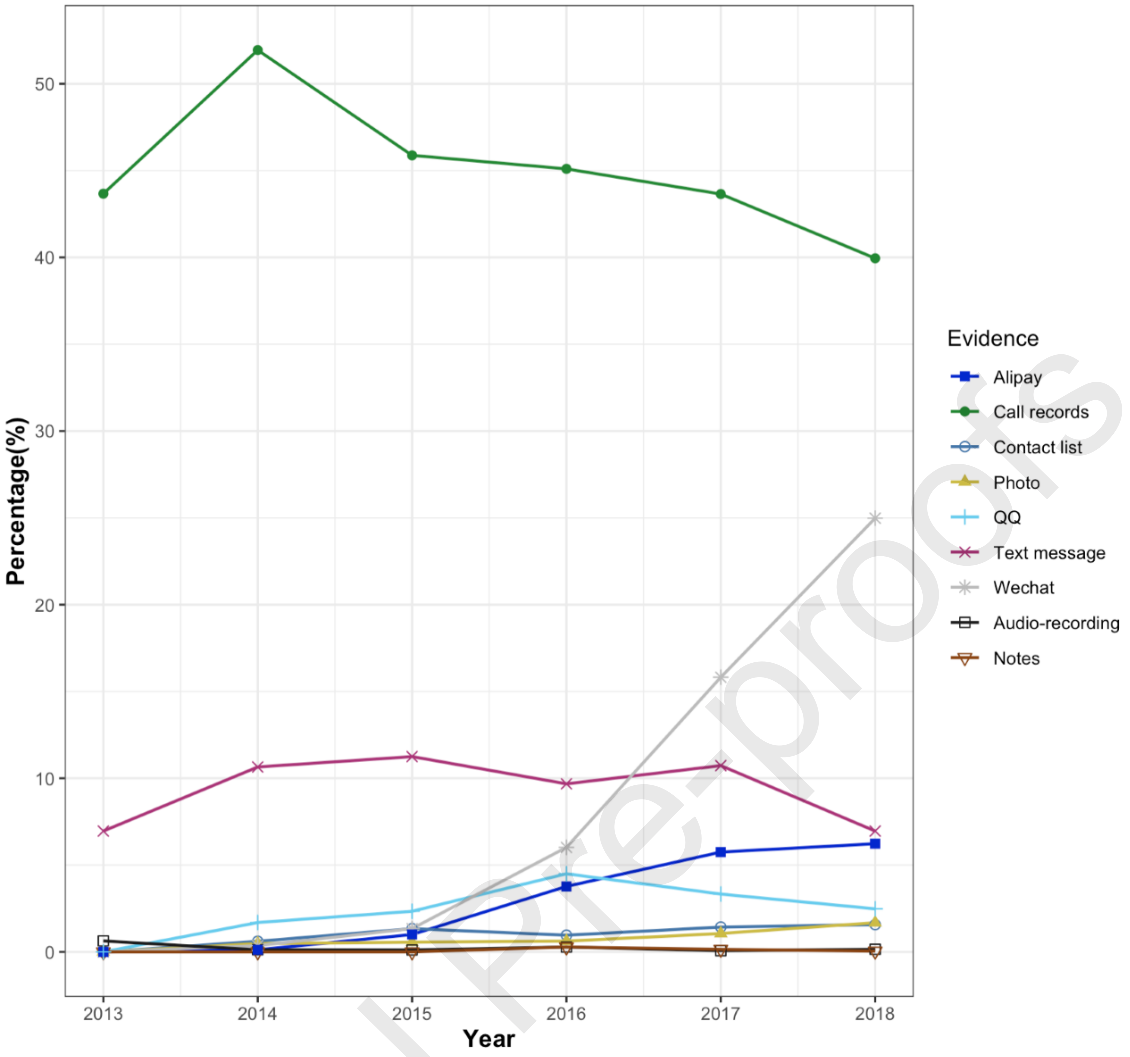

Figure 6 Proportion of each evidence category in all mobile phone evidence

Although there is a large number of text messages in the evidence, there is not a clear change in the proportion of text message evidence in different years. Apart from call records, text message, WeChat and Alipay, the proportion of evidence from QQ, audio-recordings, notes, and cell-site analysis remained a small proportion of the total across all years (all under 5%).

3.4 Average numbers of evidence used in different crime types

To assess the use of mobile phone evidence in various types of crime investigation, the average amount of each type of evidence used in a specific type of crime was compared. Table 6 provides the number of cases with each mobile phone data type under each category of crime type. There was great variation in the number of sample cases for each combination of evidence and crime type; in other words, some cells reach hundreds of cases, but some cells include no cases. Analyses regarding audio-recording, notes, and cell-site analysis evidence were excluded in the analysis, owing to the very small sample sizes of these evidence types.

Figure 7 compares the *average* number for each type of evidence used in cases involving different crime types. Overall, there is a small variation in the average amount of each evidence type across different crime types, with two exceptions, call records and WeChat which were frequently used across many different crime types.

	Drug	Sexual offences	Property	Fraud	Violence	Market-related	Corruption	Terrorism
Call records	913	7	42	30	235	85	1	1
Contact list	73	1	2	2	8	10	0	0
Text message	366	2	13	22	59	40	0	0
Photo	61	1	4	2	7	4	0	1
Audio recording	3	1	0	1	5	0	0	1
Cell-site analysis	2	1	0	0	0	0	0	0
Notes	4	0	0	0	1	1	0	0
WeChat	300	3	11	15	69	52	0	4
Alipay	144	1	4	2	9	6	1	0
QQ	100	2	4	5	19	14	0	1

Table 6 Number of cases that used each type of evidence by crime type

The highest average number was call records used in sexual offences; specifically, on average five pieces of evidence related to call records were used for every case of this crime type where mobile phone evidence was used. Moreover, considering the scale (from 0-5), there is a significant variation (SD = 4.52) in the number of call records mentioned in court proceedings of sexual offences. Apart from the use in sexual offence cases, call records were used as evidence 2.49 times (SD = 3.11) in violent crime cases, on average, and 2.13 times (SD = 2.76) in drug-related cases. By contrast, call records were less commonly used in terrorism and corruption cases where mobile phone evidence was used, less than 0.5 times on average. In terrorism cases where mobile phone evidence was used, WeChat was used much more extensively than any other data type. On average, each case used 1.75 pieces (SD = 2.05) of evidence generated from WeChat.

Although WeChat only started becoming one of the more common evidence types after 2015, it is identified as the second most frequently employed format of mobile phone data in drug-related crime, violent crime, property crime and market-related crime. Furthermore, apart from terrorism cases, in most types of cases, differences in the average use of text messages (sent via short message service) and WeChat are relatively small.

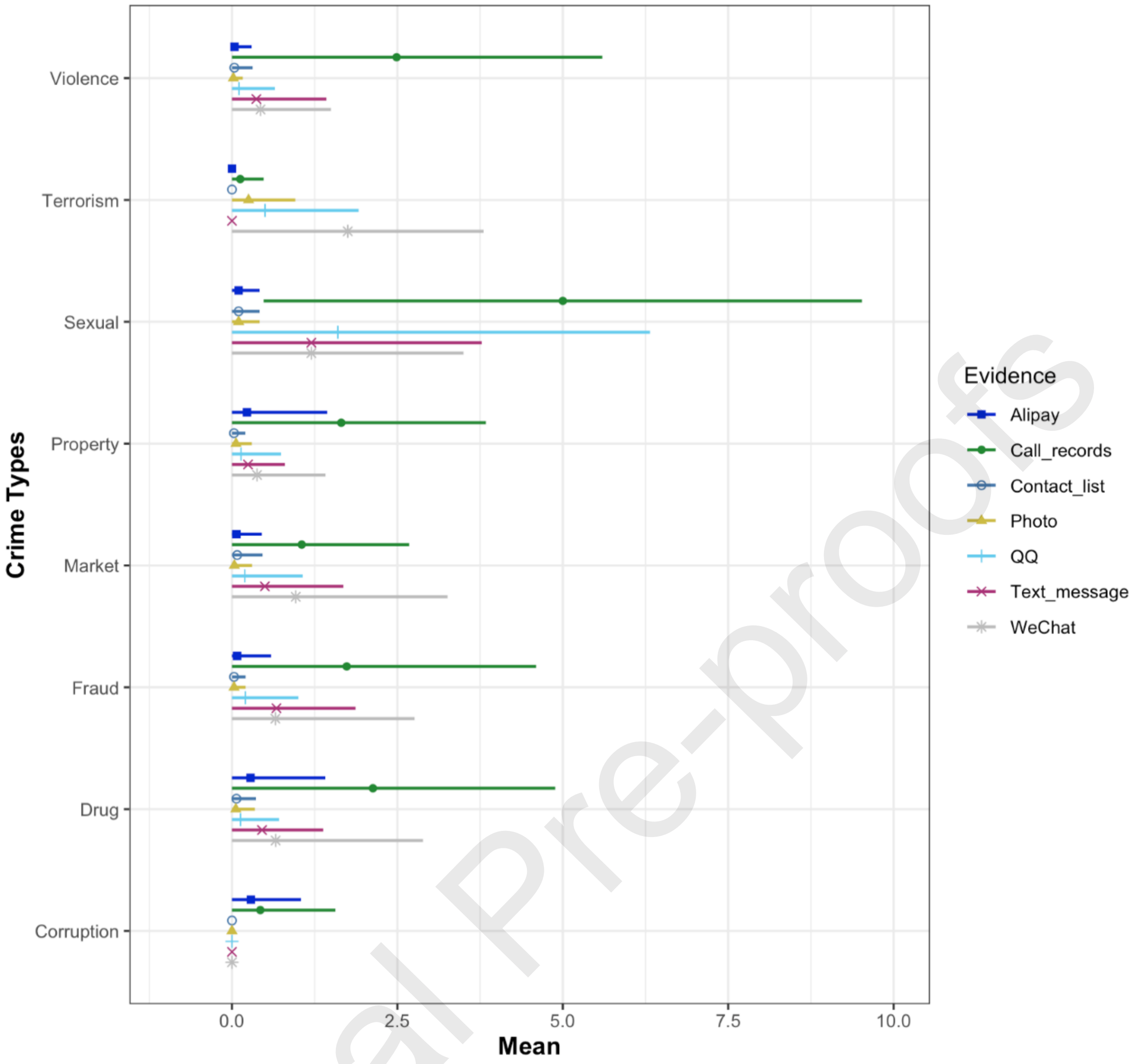

Figure 7 Amount of evidence used in each crime type (mean+/- 1SD)
Note that the lines were capped at zero.

In comparison to WeChat, another prevalent instant messaging tool, QQ, has slightly higher average uses only in relation to sexual offences (mean = 1.6, SD = 4.7). However, considering the range of possible values, this can be considered to be a small difference. For crimes related to terrorism, the average usage of QQ (0.5 times per case where mobile phone evidence was used) is second only to WeChat. As for Alipay, its average frequency for each type of crime is relatively low. Compared with fraud or other crimes related to online payment, Alipay is more commonly recruited in drug-related crime and corruption. With the limited number of corruption cases, Alipay and call records are the only two types of mobile phone evidence mentioned in judgement files of corruption cases.

3.5 Binary logistic regressions and evidence types

To compare the likelihoods of using different types of mobile phone evidence in different types of criminal proceedings that mobile phone data at least was mentioned, this study employed a series of binary logistic regression models which treated crime type (drug-related crime, sexual offences, violent crime, property crime, fraud, market-related crime, corruption, terrorism) the independent variable and one of the evidence types (call records, contact lists, text message, photo, WeChat, Alipay, QQ) as the dependent variable for every run of the model. Prior to the test, dependent variables were dummy coded, by which the number of pieces under each evidence type was binary coded with "0", indicating non-presence, and "1", indicating the presence of that type of evidence regardless of the times it appeared.

Table 7 presents the odds ratios of each type of evidence being employed in different crimes, with drug-related crime as the reference category in each case. Tests of statistical significance were carried out with the default function in Stata, which uses the *Z* statistic. Note that some of the results were omitted, owing to the limited number of sample cases. In addition, since the dataset includes the whole population of cases that employed mobile phone evidence it is reasonable to focus primarily on the effect size in the interpretation of the results [40]. However, the p-values may also be instructive in some cases.

In order to provide a more practical and tangible result than odds ratios, the margins command, a calculation tool installed in Stata 11[39], was used to calculated predicted probabilities for the use of the different evidence types in relation to the different crime types. This assists in the interpretation with effect size (Figure 8). Overall, the results of this analysis confirm the associations between evidence types and types of crime investigation, and indicate some common uses of various formats of mobile phone data in criminal proceedings that required mobile phone information.

Looking first at the model for the most commonly employed evidence type, call record, the results suggest that this type of evidence is more likely to be used in drug-related crime (the reference category), compared to all other crime types, since all odds ratios are less than one. However, there is little difference among uses of call records in sexual offences, violent crime, property crime, and drug-related crime (p>.1 in every case). As also indicated in Figure 8, among all criminal cases in which some sort of mobile phones evidence was mentioned, it is estimated that the probability of call records being used in these crime types were around .6-.7. But in terrorism and corruption cases the probability of including call records as evidence was less than .15. In other words, the use of call records was heavily concentrated in some crime types, but not in others.

In contrast, it is harder to identify a specific crime type where the use of contact lists as evidence was more frequent. Results from the contact list model might indicate that relative to drug-related crimes, court proceedings for sexual offences were more likely to discuss this type of evidence, with an OR of 1.83 – but note the very high p-value (.57). However, there is stronger evidence that the contact lists were less likely to be used in violent crime cases than drug cases (OR .4; p=.02). Overall, the use of call lists across case types was uncommon, and there was only a 0.1 probability of this type of evidence being used in sexual offence cases, which is the highest figure.

	Call record				Contact list				Text message				Photo			
	Odds Ratio	P>|z|	95% Conf. Interval		Odds Ratio	P>|z|	95% Conf. Interval		Odds Ratio	P>|z|	95% Conf. Interval		Odds Ratio	P>|z|	95% Conf. Interval	
Fraud	0.35	0.000	0.21	0.58	0.53	0.385	0.13	2.21	1.30	0.331	0.77	2.21	0.64	0.544	0.15	2.69
Market	0.43	0.000	0.31	0.60	1.06	0.862	0.54	2.10	0.79	0.231	0.55	1.16	0.49	0.178	0.18	1.38
Property	0.69	0.165	0.41	1.16	0.51	0.361	0.12	2.14	0.61	0.116	0.33	1.13	1.28	0.639	0.45	3.64
Terrorism	0.06	0.007	0.01	0.46									2.84	0.332	0.34	23.47
Sexual	0.93	0.911	0.24	3.60	1.83	0.569	0.23	14.64	0.62	0.548	0.13	2.94	2.21	0.455	0.28	17.73
Violence	0.92	0.548	0.71	1.20	0.40	0.016	0.19	0.84	0.53	0.000	0.39	0.72	0.42	0.033	0.19	0.93
Corruption	0.07	0.012	0.01	0.55												
	WeChat				Alipay				QQ							
Fraud	0.99	0.987	0.55	1.80	0.25	0.058	0.06	1.05	1.00	0.993	0.39	2.54				
Market	1.50	0.025	1.05	2.13	0.30	0.004	0.13	0.68	1.09	0.774	0.61	1.95				
Property	0.65	0.201	0.34	1.26	0.51	0.194	0.18	1.41	0.76	0.599	0.27	2.13				
Terrorism	3.25	0.097	0.81	13.07					1.68	0.630	0.20	13.78				
Sexual	1.39	0.633	0.36	5.42	0.87	0.898	0.11	6.94	2.94	0.177	0.62	14.02				
Violence	0.84	0.246	0.63	1.13	0.22	0.000	0.11	0.43	0.70	0.174	0.42	1.17				
Corruption					1.31	0.804	0.16	10.95								

Table 7 Binary logistic regression models predicting the use of different forms of mobile phone evidence

Unlike the conclusion of McMillan et al.[5], drug-related crime is not the only crime type that frequently retrieved text messages as evidence. Indeed, the odds of text messages being included in fraud cases was 1.3 times higher than for drug-related crimes (p = 0.331), although this difference is not statistically significant, and as Figure 8 shows there was a similar proportion of fraud (34%) and drug-related (29%) cases that, when a mobile phone was analysed, cited text messages. When looking at the category of photo (which in this study include both photos and videos saved in mobile phones), both terrorism and sexual offence cases with mobile phone evidence have higher odds of presenting photographic evidence, compared to drug-related crime, with respectively 2.84 (p = 0.33) and 2.21 (p = 0.46) times the odds of photographic evidence being used in drug-related crime. Around 10% of terrorism and sexual offence proceedings that used mobile phone evidence are predicted to draw upon photos or videos.

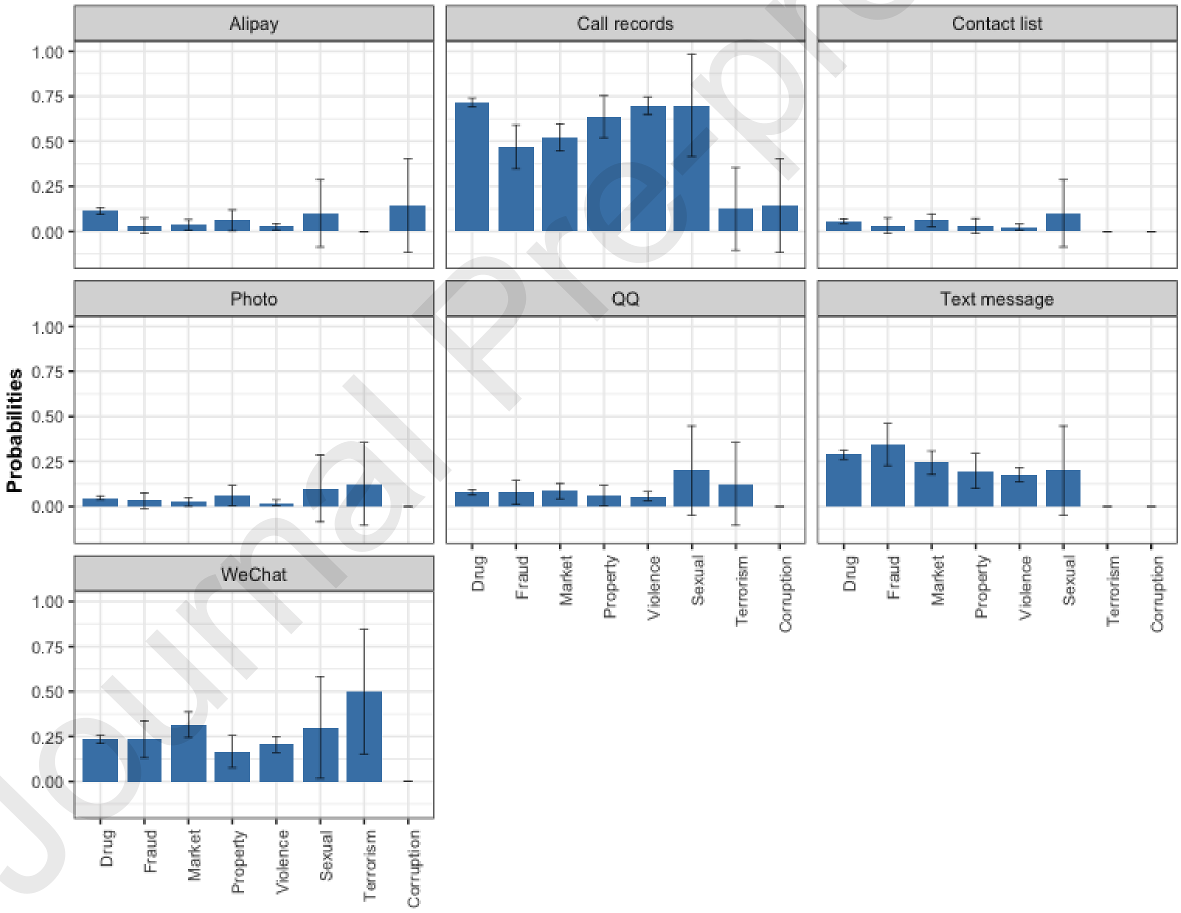

Figure 8 Predicted proportions of different types of criminal cases using each type of evidence (error bars 95% Conf. Interval)

The odds of the two popular instant communicating applications, WeChat and QQ, being used, given the use of some sort of mobile phone evidence, was relatively similar over the different crime types. One exception was that WeChat was used more often in terrorism cases and QQ was used more often in sexual offence proceedings. Specifically, the odds of retrieving WeChat data in terrorism cases were 3.25 (p = 0.097) times higher than the odds of referring to these data in drug-related crime. Looking at Figure 8, about 50% of terrorism cases that used mobile phones evidence used WeChat. For most other crime types this figure was around 20-25%. For QQ data, the odds of this data being employed when analysing mobile phone information in proceedings of sexual offences were 2.94 (p = 0.177) times the odds of their used in drug-related cases. Furthermore, among cases that used mobile phone information, around 20% of sexual offence proceedings employed QQ data, compared with 12.5% of criminal proceedings related to terrorism and less for the other crime types.

Alipay, as a mainstream online payment method, was more likely to be used in corruption cases. Relative to the odds of Alipay data being included in drug-related prosecutions, the odds in corruption cases were 1.31 (p = 0.804) times greater. Moreover, it is estimated that 14% of corruption cases that used mobile phone evidence used data extracted from Alipay in the court proceedings, as did 10% of proceedings of drug-related crime and sexual offences.

3.6 Evidence Weight

The evidence weight in each sample case was manually analysed and coded according to the three categories explained in the methodology section. With 20% cases randomly sampled in each year, the aggregated result is listed in Table 8. Overall, in the majority of criminal proceedings (80%) where mobile phone evidence was used this was not to directly prove (or disprove) crime facts or justify the sentence. Instead, it was most commonly used to support other evidence or facts that are not directly related to criminal activities (like relationships among individuals).

Weight	**N**	**%**
High	75	19.23
Medium	164	42.05
Low	151	38.72
Total	**390**	**100**

Table 8 Evidence weight distribution

Considering the rapid changes in the prevalence of forensic tools and functionalities of mobile phones between 2013 and 2018, Figure 9 illustrates the percentages of cases coded with different degrees of evidence weight in each year. The solid lines refer to the counted proportions. To underline the trend of changes for each category of evidence weight, smoothed lines calculated from a linear model were depicted with the corresponding solid lines.

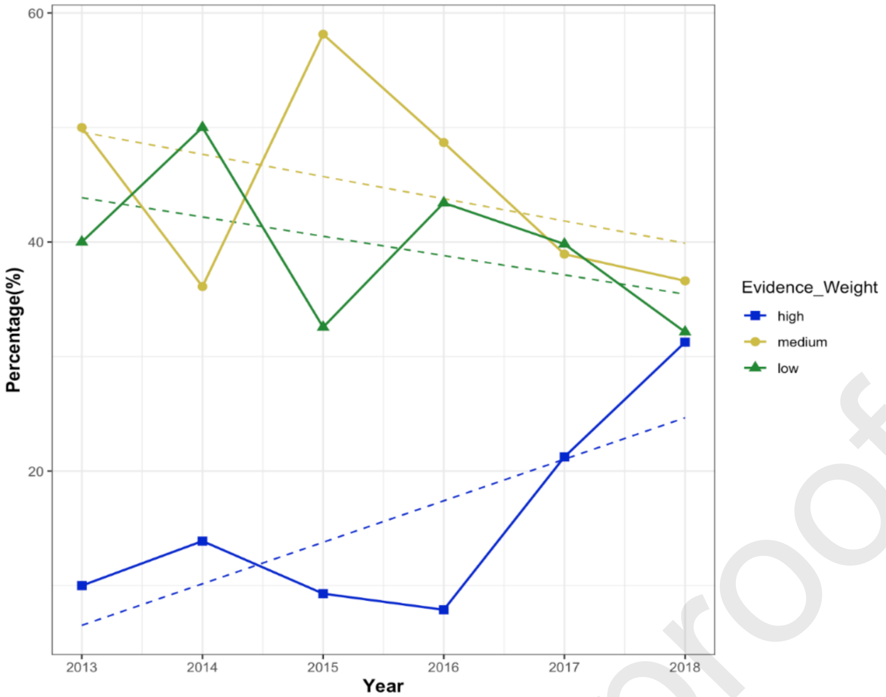

Figure 9 Changes of evidence weight coded with sample cases

The result indicates that although cases marked with high evidence weight account for a small proportion across these six years, there is a significant increase in this percentage, from 7 to 31%, over the period 2016 to 2013. In general, cases whose mobile phone evidence is graded as medium and low are of similar proportion over the study period; there are fluctuations in the two figures, with a general downward trend mirroring the increase in proportion of cases graded as 'high'.

4. Discussion

Arguably the most important finding from this study was that the proportion of criminal cases that employed mobile phone evidence remained relatively low during the research period. Moreover, even when mobile phone data were used, in the majority of criminal cases the importance of this evidence was only low to medium (although the trends shown in Figure 9 suggest this might change). Call records, instant messaging and online payment tools were identified as the most frequently used sources of mobile phone evidence. The uses of data from applications, including WeChat, Alipay and QQ, witnessed an increasing trend from 2015- 2018. Results from the logistic regression analysis confirmed that some types of data were used particularly frequently in certain criminal proceedings, but for text message and application data, there was little variation across most of the crime types.

4.1 The context of jurisdiction

There are variations between the results of this study and previously published research [4, 5, 7, 21] which is likely to reflect the different contexts of the jurisdiction of China and its unique internet community. There was a significant increase in the number of criminal cases that used mobile phone evidence, and the number of all criminal cases in the online database used in this study. On the one hand, the use of mobile phone evidence was increasingly prevalent from 2013 to 2018. On the other hand, the increasing number and proportion of cases using mobile phone evidence could be also influenced by the law issued to standard the publication of judgement files on China Judgement Online, the online database. The rise in numbers of cases (Table 3-5) in 2014 may reflect the absence of criminal cases recorded in the database before the rules were set and standardized.

4.2 Practices and outcomes of the investigation

With such different contexts, it is difficult to compare the extent to which mobile phone evidence was used in criminal proceedings in China with the situation in other countries. But in China as elsewhere there may be a gap between the requests of mobile phone analyses in the investigation and the presence of mobile phone evidence in court proceedings. Although the number of criminal cases that employed mobile phone evidence is higher in this study than what was found in the previous research by McMillan et al. [5] in the UK, these incidents in both China and the UK did not account for a large proportion of all criminal cases. By contrast, research in Australia has documented thousands of cases requesting mobile device analysis in the investigation phase [4, 7]. It is not unreasonable to assume that in China, mobile phone evidence is commonly used in the investigation, but only relatively rarely introduced as evidence in court.

According to the results of this research (Figure 3), the types of mobile phone data that frequently used in the criminal proceedings are those can be accessed and gathered with a digital copy or a printed version as an admissible way for presenting evidence on the court.The paucity of forensic tools to enable the analysis of chat data could influence its use in evidence [41]. From the time that instant messaging applications like WeChat and QQ became popularised in 2013 [42], there was a lag of about a year before evidence from instant messaging applications began to be used in criminal proceedings. It is reported that the rate of internet users who use instant messaging applications reached 84% in the middle of 2013 [42]. In the same year, WeChat emerged and continuously introduced new users to instant-messaging tools. By the end of 2020, over 99% of internet users were using instant messaging services [43]. However, there were few uses of WeChat data in trials before 2015. Therefore, the extent of mobile phone evidence used in criminal cases is possibly influenced by the accessibilities of automated forensic techniques. Indeed, while it is acceptable to present in court application data with pictures or snapshots of chatting content collected via manual extraction, this can be labour and time consuming for investigators when it comes to recovering and presenting a large amount of data [24].

On the other hand, this lag in the use of instant messaging data could also have resulted from the standardising progress of relevant legislation. Since information and knowledge generated from the investigation need to be embedded in the correct legal frame to be admissible as evidence, the accessibility of related rules also influences the decision making of investigators. When comparing the most commonly used data type in this study with previous research [5], there is a concordance in suggesting that call-records are the most commonly used type of mobile phone data over the research period and across different nations. Since making calls is the foundational function of mobile phones, for legal professionals, it is much easier to trace back to call records to make inferences of criminal activities. Moreover, while sophisticated forensic techniques to extract data may be absent due to gaps in expertise, equipment or budgets for digital forensic examination, the authenticity and validity of call records can be justified with the documents provided by a service provider. Presenting call records is not limited by the absence of pertinent legislations or standards. Besides, when the *Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases*[10] (OEDE) was issued in 2016 to standardise the specific operations of using digital evidence, the uses of instant messaging and online payment data increased significantly. Thereby, the accessibilities in both technical and legal aspects could influence the decision making in the investigation.

Previous research has proposed that there can be associations between specific types of mobile phone evidence and specific crime types, for example, text messages were frequently used in drug-related crime [4, 5, 21]. However, in this study associations are not evident with the use of application data (WeChat, Alipay, QQ) in different crime types, as little variation was indicated by the logistic models. As a result, for further examination of mobile phone data, common applications which enable e-payment and instant messaging will be regarded as routine work. In these instances, application data were likely to be collected and reported altogether, regardless of the specific type of crime investigation.

4.3 Information enabled by the multi-media feature of applications

With instant messaging tools and online payment methods increasingly installed in mobile phones, data extracted from these applications may provide valuable information in criminal proceedings. The extent of dependence upon a mobile network to conduct daily work and routines in China makes data stored in applications extraordinarily informative about peoples' lives [43]. But what cannot be overlooked is the multi-functional feature of WeChat, QQ and Alipay. Each of them excels in diverse areas. WeChat provides social media for a general population; QQ facilitates a more unique and personalised social-networking function and is customised for younger generations; Alipay is used as a universal online payment tool. Yet, while

[10] Issued by Instrumentalities of the State Council, All Ministries, Ministry of Public Security in 2019

having different specialities, all enable both instant communication and online payment to individuals or entities. With texts, photos, videos and transactions compounded in data from these applications, it is hard to discern whether or not specific data types (e.g. text, photo, transaction) are more or less useful in relation to different crime types. Therefore, there is little variation among the predicted proportions of cases using instant messaging applications in different crime types. Compared with functionalities initially installed in mobile phones, (like SMS and photo albums), application data like WeChat and QQ are used more frequently. This finding to some extent implies the advances of multi-media data in crime reconstruction.

It is reasonable to assume that with the communication in WeChat and QQ, texts, photos, transactions information sent between individuals can be interpreted in a specific context. In this sense, more useful information can be provided to investigators or judges, consequently, application data were referred more frequently. It has been demonstrated that communication information makes up a large proportion of informative mobile phone evidence [7]. In this research, although data stored in WeChat and text messages were used at around the same rate across the whole research period, the uses of WeChat data surpassed the number of text message evidence in 2017. Moreover, compared to instant messaging tools, photo evidence was used less frequently. Although previous research identified that in sexual offences, photos and videos were commonly used [4, 21], the findings of this study identified WeChat and QQ as more commonly used rather than photos or videos saved on mobile phone devices.

4.4 Particular uses of application data

As discussed in section 3.4 and 3.5, application data were used commonly regardless of crime types due to the multi-media data it can provide. But there are still several crime categories with higher predicted proportions of using several specific types of mobile phone data. These distinctions may result from features of common criminal use of an application. Under the category of terrorism, cases are mainly related to the propagation of terrorist or extremist materials. By enabling the spread of multiple types of data, WeChat is more likely to be employed to distribute terrorist or extremist content. Apart from the implication on common criminal behaviours, the high proportion of terrorism cases that employed mobile phone evidence may reflect to some extent the proficiency of legal professionals in applying mobile phone evidence to deal with cases with terrorist propagation.

Moreover, when mobile phone evidence was needed, WeChat data were relatively often used in market-related crime proceedings. In the sample of this study, cases under this category mainly comprised smuggling and financial crimes disturbing the ‘socialist market order’. As WeChat enables instant transaction and messaging, evidence extracted from this application could provide informational support for the trades and transactions alleged to have been involved. Yet, Alipay was not used in market-related cases as frequently as WeChat. This may be because, in court proceedings for market-related crimes, official documents can be more informative than mobile phone evidence relating primarily to interactions [4], and compared to WeChat, a comprehensive online messaging tool, Alipay is seen mainly as an online payment tool; files or photos are very seldomly be sent via this app. Moreover, instead of official agreements or contracts, the information Alipay can provide is limited to transactions and individuals' relationships, as it is not a formal payment method. Since Alipay transactions between individuals at least indicate acquaintance between individuals, data stored in Alipay can provide information about social relationships. This feature may be reflected by the exclusive uses of Alipay and call records in corruption cases. Here, unlike market-related crime, further details of trades are not necessarily needed. Merely the record of contact, time and amount of money transacted could be regarded as key factors that could influence the decision making of judges.

4.5 The changing influences of mobile phone evidence

Prior to a discussion of evidence weight, it should be noted that the results here will have been influenced by the definitions of evidence weight and the procedures for categorising each case. With slightly differences in the definition of 'high evidence weight' in the present paper compared with the earlier research by McMillan et al. [5], the result of this study is not consistent with the previous study.

Even so, there is a similar trend with these two studies. Specifically, cases graded with high evidence weight overall account for the smallest proportion but with an increasing trend. Besides, in a majority of criminal cases mobile phone data were used merely to prove individuals' relationships or were just mentioned as a piece of evidence without any further explanation. What is different from the previous research is that the proportion of cases marked as high evidence weight increased over the research period to nearly one-third of all cases using mobile phone evidence by 2018. It is worth underlining that while from 2013 onwards there were already cases that employed mobile phone data and presented the results as a piece of evidence, meaning that there were accessible forensic tools for analysing mobile phone data less than one year after digital evidence was formalised in CPL, in the majority of criminal proceedings mobile phone data were not a significant factor in sentencing or judges' decision-making until 2016 when uses of digital evidence were standardised and application data were increasingly used in trials.

Without further investigation, it is hard to draw any conclusions regarding whether the accessibility of forensic tools and standards assist the flexibility or capability of mobile phone data use. Nevertheless, the increasing proportion of cases marked with high evidence weight is unlikely to solely reflect increased proficiency in using mobile phone evidence or capabilities for dealing with the expanding volume of digital data. Findings in this research indicate that there has been an increase in requests for mobile phone evidence, yet empirical research regarding cybercrime in China still finds that in the investigation stage, legal professionals face difficulties in extracting digital evidence, which could lead to challenges in the court proceedings [44].

4.6 Future developments

It is recognised that in this study the python script which was employed to automatically identify objects was limited to its rule-based approach which identifies evidence based on the given structure and keywords. As a result, file features that were not concluded by the research were not identified and analysed. To enhance the accuracy in identifying evidence, previous research employed multiple Named Entity Recognition approaches in machine learning or deep learning to extract information in Chinese judgment files [44, 45]. This method is capable of automatically identifying key features like individuals, time, locations mentioned in court records, but a more fine-grained recognition and categorisation is required [47]. Given the initial findings from this current study, it would be beneficial to develop the approach utilised here and implement data mining tools with Natural Language Processing in order to identify more factors that may influence the use of mobile phone evidence and offer a timely searching of files for legal professionals.

It would also be valuable to conduct more in-depth research to consider the context in which mobile phone evidence is used, in addition to understanding the context in which evaluations and interpretations are made. This would enable a more holistic approach to understand the broader factors that may impact the decision-making that takes place during the collection, analysis and interpretation of mobile phone evidence as outlined in the FoRTE model [48], and incorporate the crime scene where front-line police officers respond to digital evidence as well as the analysis, interpretation and presentation of mobile phone evidence in crime reconstruction.

5. Conclusion

This study employed content analysis to quantify the features of mobile phone evidence used in criminal proceedings in China, since digital evidence was officially listed in CPL. This study has identified that the proportion of criminal cases that used mobile phone evidence account for less than 4% of the cases in the dataset (with a small increase between 2013-2018). Compared to previous research [5], one evident difference is the frequent use of instant messaging data. While this research and McMillan et al. [5] study were conducted in different countries and over different periods, both of these studies identify call records as being frequently mentioned in evidence.

With tests of associations between each crime type and evidence type, the study identifies several trends; WeChat data in terrorism cases; contact list and photo materials in sexual offences; text messages in fraud cases. In addition, call records and WeChat were identified as the two evidence types most likely to be used routinely no matter what type of criminal proceedings were being undertaken. In over one-third of cases where mobile phone evidence was used, it was used to support other evidence or factors not directly related to final sentencing. However, there was an increasing proportion of cases that were marked with high evidence weight. Based on current findings, it can be implied that a large amount of mobile phone evidence is filtered out in the stages before court proceedings.

Mobile phones are heavily relied on in China and this technology has become an all-in-one solution for internet users [26]. There should be much data that could be used by police during an investigation. But our results show that mobile phone evidence is only used in court in a small proportion of cases. As the analysis of evidence weight suggests, in many cases, it seems that mobile phones were not thoroughly examined and only data that was easy to access were used, and even then merely ‘mentioned’ as evidence. It is not possible to uncover the reasoning processes of investigators when interpreting and presenting evidence from this dataset. However, it is reasonable to assume that the accessibility of evidence is a consideration in their decision making. Moreover, it is possible that mobile phone data were used as intelligence and to generate other forms of evidence that then took precedence in the presentation of that evidence to the court.

This study has provided valuable insights into the use of mobile phones and mobile phone applications in different types of criminal activity in China. In so doing it has provided a broader picture of the use of mobile phone evidence globally and in a different jurisdiction to previously published work. Future research could consider how mobile phones are used in the investigatory phase, which would aid in understanding why, in a society as connected as China, court cases seem to rely relatively infrequently on mobile phone evidence.

References:

[1] R. Davis and K. Pease, “Crime, Technology and the Future,” 2000.

[2] Eoghan. Casey, *Digital evidence and computer crime : Forensic science, computers and the Internet*. London: Academic Press, 2000.

[3] P. Ekblom, “How to police the future: scanning for scientific and technological innovations which generate potential threats and opportunities in crime, policing and crime reduction,” in *Crime science*, Willan, 2013, pp. 27–55. [Online]. Available: www.policereform.gov.uk/implementation/scienceandtech.html

[4] B. Turnbull, R. Taylor, and B. Blundell, “The anatomy of electronic evidence - Quantitative analysis of police e-crime data,” in *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 2009, pp. 143–149. doi: 10.1109/ARES.2009.118.

[5] J. E. R. McMillan, W. B. Glisson, and M. Bromby, “Investigating the increase in mobile phone evidence in criminal activities,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2013, pp. 4900–4909. doi: 10.1109/HICSS.2013.366.

[6] D. Quick and K. K. R. Choo, “Impacts of increasing volume of digital forensic data: A survey and future research challenges,” *Digital Investigation*, vol. 11, no. 4, pp. 273–294, Dec. 2014, doi: 10.1016/j.diin.2014.09.002.

[7] D. Quick and K. K. R. Choo, “Pervasive social networking forensics: Intelligence and evidence from mobile device extracts,” *Journal of Network and Computer Applications*, vol. 86, pp. 24–33, May 2017, doi: 10.1016/j.jnca.2016.11.018.

[8] E. R. Mumba and H. S. Venter, “Mobile forensics using the harmonised digital forensic investigation process,” Nov. 2014. doi: 10.1109/ISSA.2014.6950491.

[9] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, “A critical review of 7 years of Mobile Device Forensics,” *Digital Investigation*, vol. 10, no. 4. Elsevier Ltd, pp. 323–349, 2013. doi: 10.1016/j.diin.2013.10.003.

[10] K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, “Current and future trends in mobile device forensics: A survey,” *ACM Computing Surveys*, vol. 51, no. 3, Apr. 2018, doi: 10.1145/3177847.

[11] A. Valjarevic and H. S. Venter, “A Comprehensive and Harmonized Digital Forensic Investigation Process Model,” *Journal of Forensic Sciences*, vol. 60, no. 6, pp. 1467–1483, Nov. 2015, doi: 10.1111/1556-4029.12823.

[12] Mark. Pollitt, Eoghan. Casey, Jaquet-Chiffelle David-Oliver., and P. Gladyshev, “A framework for harmonizing forensic science practices and digital multimedia evidence,” *The Organization of Scientific Area Committees for Forensic Science (OSAC)*, 2018, Accessed: Nov. 03,

2021. [Online]. Available: https://serval.unil.ch/resource/serval:BIB_32FB580596A3.P001/REF.pdf

[13] D. S. Wall, “The internet as a conduit for criminal activity,” in *Information Technology and the Criminal Justice System*, A. Pattavina, Ed. SAGE Publications Inc., 2015, pp. 77–98. doi: 10.4135/9781452225708.n4.

[14] R. M. Morgan, G. E. Meakin, J. C. French, and S. Nakhaeizadeh, “Crime reconstruction and the role of trace materials from crime scene to court,” *WIREs Forensic Science*, vol. 2, no. 1, Jan. 2020, doi: 10.1002/wfs2.1364.

[15] R. M. Morgan and P. A. Bull, “Forensic geoscience and crime detection Identification, interpretation and presentation in forensic geoscience,” 2007.

[16] R. M. Morgan, “Conceptualising forensic science and forensic reconstruction. Part I: A conceptual model,” *Science and Justice*, vol. 57, no. 6, pp. 455–459, Nov. 2017, doi: 10.1016/j.scijus.2017.06.002.

[17] M. Innes, *Investigating murder: Detective work and the police response to criminal homicide*. Oxford University Press, 2003.

[18] Eoghan. Casey, *Handbook of digital forensics and investigation*. Academic, 2010.

[19] H. Earwaker, S. Nakhaeizadeh, N. M. Smit, and R. M. Morgan, “A cultural change to enable improved decision-making in forensic science:

A six phased approach," *Science and Justice*, vol. 60, no. 1, pp. 9–19, Jan. 2020, doi: 10.1016/j.scijus.2019.08.006.

[20] T. Dearsley, "Mobile phone forensics-Asking the right questions," *New Law Journal*, vol. 155, no. 7187, pp. 1164–1165, 2005.

[21] A. Ali, S. A. Razak, S. H. Othman, A. Mohammed, and F. Saeed, "A metamodel for mobile forensics investigation domain," *PLoS ONE*, vol. 12, no. 4, Apr. 2017, doi: 10.1371/journal.pone.0176223.

[22] F. Marturana, G. Me, R. Bertè, and S. Tacconi, "A quantitative approach to triaging in mobile forensics," in *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011*, 2011, pp. 582–588. doi: 10.1109/TrustCom.2011.75.

[23] G. Grispos, T. Storer, and W. B. Glisson, "A comparison of forensic evidence recovery techniques for a windows mobile smart phone," *Digital Investigation*, vol. 8, no. 1, pp. 23–36, 2011, doi: 10.1016/j.diin.2011.05.016.

[24] R. Ayers, S. Brothers, and W. Jansen, "Draft Special Publication 800-101 Revision 1, Guidelines on Mobile Device Forensics," 2014.

[25] J. Henrich, Steven J. Heine, and Ara Norenzayan, "'Most people are not WEIRD.,'" *Nature*, vol. 466.7302, pp. 29–29, 2010.

[26] China Internet Network Information Centre (CNNIC), "Statistical Report on Internet Development in China," Aug. 2019. Accessed: Jan. 26, 2022. [Online]. Available: https://www.cnnic.com.cn/IDR/ReportDownloads/201911/P020191112539794960687.pdf

[27] M. Yip, "An investigation into Chinese cybercrime and the underground economy in comparison with the West," 2010.

[28] J. Lusthaus, *Industry of anonymity*. Harvard University Press, 2018.

[29] B. Liang and H. Lu, "Internet development, censorship, and cyber crimes in China," *Journal of Contemporary Criminal Justice*, vol. 26, no. 1, pp. 103–120, Feb. 2010, doi: 10.1177/1043986209350437.

[30] Y. C. Chang, *Cybercrime in the Greater China region: regulatory responses and crime prevention across the Taiwan Strait*. Edward Elgar Publishing, 2012.

[31] W. R. Hobbs and M. E. Roberts, "How sudden censorship can increase access to information," *American Political Science Review*, vol. 112, no. 3, pp. 621–636, Aug. 2018, doi: 10.1017/S0003055418000084.

[32] Y. Chen and D. Y. Yang, "1984 or the Brave New World? Evidence from a Field Experiment on Media Censorship in China," 2017.

[33] C. Su and T. Flew, "The rise of Baidu, Alibaba and Tencent (BAT) and their role in China's Belt and Road Initiative (BRI)," *Global Media and Communication*, 2020, doi: 10.1177/1742766520982324.

[34] Y. T. Hu, *Xin Xingshi Susong Wenshu Yangshi [New version of formats of litigation documents]*. Beijing: People's Court press, 2020.

[35] K. Soothill and C. Grover, "A note on computer searches of newspapers," *Sociology*, vol. 31, no. 3, pp. 591–596, 1997.

[36] D. Deacon, "Yesterday's papers and today's technology: Digital newspaper archives and 'push button' content analysis," *European Journal of Communication*, vol. 22, no. 1, pp. 5–25, Mar. 2007, doi: 10.1177/0267323107073743.

[37] A. Bryman, *Social Research Methods*, Fith ed. Oxford, United Kingdom: Oxford University Press, 2016.

[38] K. J. Berman, W. B. Glisson, and L. M. Glisson, "Investigating the Impact of Global Positioning System Evidence."

[39] R. Williams, "Using the margins command to estimate and interpret adjusted predictions and marginal effects," 2012.

[40] H. Chen, P. Cohen, and S. Chen, "How big is a big odds ratio? Interpreting the magnitudes of odds ratios in epidemiological studies," *Communications in Statistics: Simulation and Computation*, vol. 39, no. 4, pp. 860–864, Apr. 2010, doi: 10.1080/03610911003650383.

[41] K. Zhao, Y. Zhang, C. Xing, W. Li, and H. Chen, "Chinese underground market jargon analysis based on unsupervised learning," in *IEEE International Conference on Intelligence and Security Informatics:*

Cybersecurity and Big Data, ISI 2016, Nov. 2016, pp. 97–102. doi: 10.1109/ISI.2016.7745450.

[42] China Internet Network Information Centre (CNNIC), “Statistical Report on Internet Development in China,” 7, 2013. Accessed: Mar. 20, 2020. [Online]. Available: https://www.cnnic.com.cn/IDR/ReportDownloads/201310/P020131029430558704972.pdf

[43] China Internet Network Information Centre (CNNIC), “Statistical Report on Internet Development in China,” Sep. 2020. Accessed: Feb. 15, 2021. [Online]. Available: https://www.cnnic.com.cn/IDR/ReportDownloads/202012/P020201201530023411644.pdf

[44] T. You and Q. Yang, “Wangluo fanzui shizheng fenxi jiyu beijingshi haidianqu renmin fayuan 2007-2016nian shenjie wangluofanzui anjian qingkuang de diaoyan [An empirical research on cybercrime based on cybercrime cases from 2007-2016 recorded in People’s court of Beijing Haidian district],” *Journal of Law Application*, vol. 2, pp. 85–91, 2017.

[45] W. Huang, J. Zhang, Y. Xiao, Z. Han, and Z. Deng, “Named Entity Recognition in Chinese Judicial Domain Based on Self-attention mechanism and IDCNN,” in *Proceedings - 8th International Conference on Digital Home, ICDH 2020*, Sep. 2020, pp. 51–56. doi: 10.1109/ICDH51081.2020.00017.

[46] J. Li, A. Sun, J. Han, and C. Li, “A Survey on Deep Learning for Named Entity Recognition,” *IEEE Transactions on Knowledge and Data Engineering*, pp. 1–1, Mar. 2020, doi: 10.1109/tkde.2020.2981314.

[47] Y. Yang, Z. Wang, and Z. Jiang, “An Improved Tri-Training Based Named Entity Identification Approach for Legal Knowledgebase of Properties Involved in Criminal Cases,” Nov. 2021, pp. 655–660. doi: 10.1109/icnisc54316.2021.00124.

[48] R. M. Morgan, “Conceptualising forensic science and forensic reconstruction. Part I: A conceptual model,” *Science and Justice*, vol. 57, no. 6, pp. 455–459, Nov. 2017, doi: 10.1016/j.scijus.2017.06.002.

Acknowledgements
The authors really appreciate of all editor and anonymous reviewers for their feedbacks.

This research did not receive any specific grant from funding agencies in the public commercial or not-for-profit sectors.

Highlights

- In majority of criminal proceedings, the extent to which mobile phone data were used was limited.
- The analysis of instant messaging and online transaction applications is routine in China criminal proceedings.
- Mobile phone evidence was mainly used to support other evidence or factors not directly related to final sentencing.