No 34 November 2024

Trends & Policies in Criminology and Justice

Issues in Search and Seizure of Digital Evidence and Possible Improvements

Dr. Heesung Tak
Senior Research Fellow / heesung@kicj.re.kr

Contents ▶

Keywords

Digital evidence, Search and seizure, Criminal procedure law, Discovery of substantive truth, Privacy protection

KICJ Korean Institute of Criminology and Justice

1 Overview

The rapid development of information and communication technology (ICT) and the acceleration of non-face-to-face digital transformation, spurred by COVID-19, have significantly enhanced data encryption technologies for information protection. Additionally, the networking of data due to the widespread use of cloud services has created legal and technical challenges that traditional legal interpretations alone struggle to address. These issues create obstacles to the discovery of substantive truth, which is a primary goal of the criminal justice process. In this context, the need arises to depart from traditional search and seizure concepts that focus on physical objects. There is a growing demand to establish new methods and procedures compatible with the unique characteristics of digital data, along with securing legislative support to implement these changes. Thus, this study aims to explore: i) The direction for improving search and seizure provisions to better align with the realities of digital evidence. ii) Legislative guidance that balances the discovery of substantive truth and the protection of privacy in the investigative process within the digital environment. iii) The possibility of introducing new evidence acquisition methods that account for the technical nature and forms in which digital data exist. The rest of the study will follow these objectives by: i) Reviewing current search and seizure regulations in the Criminal Procedure Act and their incompatibility with digital evidence. ii) Analyzing changes and trends in relevant case law and legislation, highlighting major issues related to the seizure and search of digital evidence. iii) Comparing legislative and policy changes in major countries addressing the challenges of digital evidence search and seizure. iv) Examining the necessity for new methods of compulsory investigation to secure digital evidence.

2 Necessity and Purpose of Research

Necessity of Research

- Despite rapid advancements in IT technology, current criminal procedure laws still focus on physical objects in their approach to search and seizure, incorporating digital evidence under this outdated framework.
- The gap between law and reality is widening as investigative procedures apply a media-centric concept of search and seizure to digital information.
- Especially since the COVID-19 pandemic, digital transformation has accelerated, strengthening data encryption technology for information protection. The expansion of cloud ser-

vices has also created legal and technical challenges that cannot be solved with current interpretations of the law.

Purpose of Research

- Reconsider the direction of revising search and seizure regulations to fit digital evidence.
- Propose legislative directions that balance the discovery of substantive truth and the protection of privacy in the digital environment.
- Explore the potential introduction of new methods for securing evidence, considering the existence forms of digital data based on its technological nature.

Status of Digital Evidence Analysis

(Unit: Cases)

Year	Subtotal	Computer Devices (PC, Laptop, etc.)	Digital Devices (CCTV, Navigation)	Mobile Devices (Smartphone, Mobile Phone)	Files/Others (Hacking, Encryption, DB, etc.)
2012	10,426	3,830	393	5,870	333
2013	11,200	3,138	483	7,332	247
2014	14,899	3,079	510	10,656	654
2015	24,295	3,357	712	19,526	700
2016	32,281	3,923	794	26,408	1,156
2017	36,060	4,198	867	30,238	757
2018	45,103	6,239	1,065	36,986	813
2019	56,440	7,295	1,412	46,551	1,182
2020	63,935	9,113	1,557	52,479	786
2021	75,420	13,311	2,353	58,563	1,193
Year-on-Year Growth Rate	17.96%	46.07%	51.12%	11.60%	51.78%

* Source: National Police Agency, 2021 Police Statistical Yearbook, No. 65, November 2022, p. 373.

3 Research Method

Analysis of Legislation and Court Cases Related to Digital Evidence Search and Seizure:

- Review of legislative proposals related to digital evidence search and seizure submitted to the National Assembly over the past 20 years.
- Analysis of Supreme Court precedents on digital evidence search and seizure to identify issues with current laws.

Analysis of Changes in Regulations and Court Cases on Digital Evidence Search and Seizure in Major Foreign Countries

- Examination of changes and trends in regulations and case law in common law countries (the U.S., U.K.) and civil law countries (Germany, Japan).

Expert Interviews

- Interviews with police officers, prosecutors, and judges.

4 Major Issues in South Korea and Anaylsis of Legislative Trends in Foreign Countries

Legislative History and Court Cases in South Korea

Legislative History

- Since the early 2000s, only 17 legislative bills addressing digital evidence have been introduced in the Criminal Procedure Act.
- Early Bills (before 2015): Focused primarily on protecting personal information and privacy rights.
- Recent Bills (after 2015): Shifted towards addressing concerns over investigative agencies' abuse of authority during the digital evidence seizure process.
- Post-Nth Room Case: Following the notorious case, newer bills emphasized the need for rapid and efficient methods to secure and preserve digital evidence, reflecting changes in priorities.

Digital Evidence Collection and Analysis Handled by the Prosecution

(Unit: Cases)

Category	Number of Cases										
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Search and Seizure	1,223	1,230	1,441	1,948	2,142	1,655	2,318	2,847	1,949	1,572	2,692
Evidence Analysis	4,787	5,368	6,708	8,179	9,766	9,880	8,819	8,940	6,606	4,712	6,920
Others	55	926	130	1,159	1,262	304	96	78	129	103	
Total	6,065	7,524	8,279	11,286	13,170	11,839	11,233	11,865	8,684	6,387	9,612

* Source
- 2012, 2013 : Supreme Prosecutors' Office, 『2014 Prosecutors' Yearbook』, 2014, p.529.
- 2014 : Supreme Prosecutors' Office, 『2015 Prosecutors' Yearbook』, 2015, p.576.
- 2015 : Supreme Prosecutors' Office, 『2016 Prosecutors' Yearbook』, 2016, p.556.
- 2016 : Supreme Prosecutors' Office, 『2017 Prosecutors' Yearbook』, 2017, p.602.
- 2017 : Supreme Prosecutors' Office, 『2018 Prosecutors' Yearbook』, 2018, p.453.
- 2018 : Supreme Prosecutors' Office, 『2019 Prosecutors' Yearbook』, 2019, p.420.
- 2019 : Supreme Prosecutors' Office, 『2020 Prosecutors' Yearbook』, 2020, p.394.
- 2020 : Supreme Prosecutors' Office, 『2021 Prosecutors' Yearbook』, 2021, p.420.
- 2021 : Supreme Prosecutors' Office, 『2022 Prosecutors' Yearbook』, 2022, p.411.
- 2022 : Supreme Prosecutors' Office, Pre-Announced Public Information, "Support Status for Digital Evidence Seizure, Search, and Evidence Analysis" (https://www.spo.go.kr/site/spo/ex/announce/AnnounceInfo.do, last accessed June 13, 2023).

Trends in Legislative Amendments

- Earlier bills concentrated on more detailed provisions to regulate the seizure and search process, ensuring privacy protection.
- Recent bills increasingly focus on securing digital evidence quickly, acknowledging the limitations of public authorities in keeping pace with technological advancements.
- Since 2019, amendments to the Criminal Procedure Act have concentrated more on improving investigative agencies' ability to perform searches and seizures efficiently.

Regulations on the Seizure of Digital Evidence under the Current「Criminal Procedure Act」

Article 106 (Seizure)

(1) If necessary, a court may seize any articles thought to be used as evidence or liable to confiscation, only when such articles are deemed to be connected with the accused case: Provided, That the same shall not apply where otherwise provided in Acts. <Amended on Jul. 18, 2011>

(3) Where the object to be seized is a computer disc or other data storage medium similar thereto (hereafter referred to as "data storage medium or such" in this paragraph), the court shall require it should be submitted after the data therein are printed out or it is copied within the specified scope of the data stored: Provided, That the data storage medium or such may be seized, when it is deemed substantially impossible to print out or copy the specified scope of the data or deemed substantially impracticable to accomplish the purpose of seizure. <Newly Inserted on Jul. 18, 2011>

Article 215 (Seizure, Search, and Inspection)

(1) If necessary for the investigation of crimes, prosecutors may seize, search, or inspect articles or persons according to the warrant issued by a judge of the competent district court upon request of the prosecutors, only when there are circumstances where a criminal suspect is suspected of having committed a crime and the articles or persons to be seized, searched, or inspected are deemed to be connected with the relevant case.

(2) If necessary for the investigation of crimes, senior judicial police officers may seize, search, or inspect articles or persons according to the warrant issued by a judge of the competent district court upon request of a prosecutor who is requested by the senior judicial police officers, only when there are circumstances where a criminal suspect is suspected of having committed a crime and the articles or persons to be seized, searched, or inspected are deemed to be connected with the relevant case.
[This Article Wholly Amended on Jul. 18, 2011]

Regulations on the Seizure of Voluntarily Submitted Items under the Current 「Criminal Procedure Act」

Article 108 (Seizure of Voluntarily Produced Articles)
Articles which have been dropped or left, or voluntarily produced by their owner, possessor, or custodian may be retained without a warrant of seizure.

Article 218 (Seizure without Warrant)
A prosecutor or senior judicial police officer may seize an article which has been discarded by a criminal suspect or any other person, or those which have been voluntarily produced by their owner, possessor, or custodian without a warrant.

- Initially, the main issue was securing the right to participate in the seizure process, with a focus on procedural fairness.
- In and after 2020, the legal discussion shifted towards the seizure of voluntary submissions.
- With advancements in digital technology, the focus moved from ensuring procedural fairness to safeguarding privacy rights, given the expanded scope of digital evidence subject to search and seizure.

Issues of Incompatibility between Current Criminal Procedure Law and Digital Evidence

- The current Criminal Procedure Act faces several incompatibilities with digital evidence, which can be categorized as follows:
  - Conceptual Incompatibility: The Act limits the scope of seizure to tangible objects, but digital information cannot be seized in the same way, as it does not prevent the affected party from retaining access.
  - Methodological Incompatibility: Existing investigative methods struggle to secure digital evidence efficiently due to rapid advancements in technology, highlighting the need for new investigative procedures.
  - Legislative Structure Incompatibility: The organization of the Act does not differentiate between the trial and investigative processes, applying the same rules to both. This structural issue creates a gap between the law and the realities of modern investigations.

Legislative Trends in Germany, Japan, the United States, and the United Kingdom

Germany (Civil Law System)

- Over the past two decades, Germany has continuously incorporated new investigative methods into its laws based on the rule of law and the principle of proportionality.
- It has introduced legislation to offset potential violations of fundamental rights that were not foreseen by existing investigative methods.

Japan (Civil Law System)

- The 2011 amendment to the Code of Criminal Procedure introduced provisions for the seizure of electronic records, including: a) seizure of record media concerning electronic records, b) record order copy seizure, c) Remote search and seizure.
- Extraterritorial seizures remain contentious and were not fully addressed in the 2011 amendment.
- The new system for electronic record orders faces criticism for lacking enforcement mechanisms in cases of non-compliance.

The United States (Common Law System)

- The U.S. has made several legislative amendments to adapt the seizure process to the nature of digital evidence, including: a) specifying the information to be seized, b) introducing electronic warrant systems for faster warrant issuance, c) implementing the Network Investigative Technique (NIT) warrant for trans-jurisdictional seizures, d) Enacting the CLOUD Act to allow offshore data seizures.
- These multiple legislative efforts focus more on investigation efficiency than on strict procedural controls to protect privacy.

The United Kingdom (Common Law System)

- The 2001 Criminal Justice and Police Act (CJPA) expanded the scope of seizure to include electronically stored information.
- The 2016 Investigatory Powers Act (IPA) enables the government to request data provision from foreign telecommunication providers and intercept data on foreign requests.
- The 1990 Computer Misuse Act (CMA) provides for online search, while the 2000 Regulation of Investigatory Powers (RIPA) allows authorities to compel suspects to decrypt data, with non-compliance punishable by law.

- There has been criticism that existing laws cannot keep up with rapidly changing IT technology, leading to challenges in both crime investigation and personal data protection.
- The U.K. has continuously amended its laws to address these issues through ongoing legal reforms.

Analysis of Key Issues in Current Digital Evidence Search and Seizure Procedures

- Main issues include guaranteeing the right to participate in the seizure process and the legality of voluntary submissions.
- Legal clarity on the status and scope of participation rights needs to be established to ensure the realization of due process in digital evidence searches.
- To ensure the legality of voluntary submissions, the voluntariness of submission must be confirmed, the scope of voluntary submission should be limited, and legal procedural requirements for coercive seizure need to be clarified.
- New methods for securing digital evidence that are suitable for the digital environment—such as digital evidence preservation orders, electronic warrants, remote search and seizure, and online search systems—should be reviewed.

Main Issues in Digital Evidence Search and Seizure(Procedural Controls)

Procedural Controls

- Right to Participate: This right is crucial for preventing violations of privacy and fundamental rights during the seizure of digital evidence, where irrelevant information can be mixed in. Current legislation lacks clear standards, leading to controversy. The law should clarify the legal status of the right, define who can exercise it, and establish procedures for excluding and disposing of irrelevant data.
- Seizure of Voluntary Submissions: Applying the logic of physical object seizure to digital information storage media leads to unreasonable results, such as the seizure of entire devices like smartphones, which contain vast amounts of personal data. To ensure the lawfulness of voluntary submissions, the law should address the voluntariness of the submission, limit the scope, ensure relevance, and protect the right to participate in the seizure process.

Main Issues in Digital Evidence Search and Seizure(New Evidence Securing Methods)

Digital Evidence Preservation Order

- Aimed at preserving important digital evidence by requiring telecommunications or remote computing service providers to store data temporarily to prevent loss or alteration.
- While less invasive as it doesn't involve data transfer, it is a compulsory measure and requires legal provisions on necessity, relevance, and time limits, with judicial oversight.

Electronic Warrant System

- The 2020 Act on the Use of Electronic Documents in Criminal Justice Procedures already legislates the electronic warrant system, but it needs further improvement in Korea's Criminal Procedure Act.
- Legal grounds for electronic warrants and exceptions to the warrant presentation principle should be clarified.

Remote Search and Seizure System

- Allows access to digital information stored remotely, such as in cloud services, based on the location specified in the warrant.
- Legal provisions should establish a framework for remote search and seizure, taking into account geographical scope, privacy concerns, and potential infringement on the jurisdiction of other countries.

Online Search System (Lawful Hacking)

- This method allows authorities to covertly access another person's ICT system for monitoring and data collection, also known as "lawful hacking."
- As it heavily infringes on fundamental rights, it should be limited to criminal suspects, with clear definitions of target crimes, time limits, and a dual control mechanism involving court oversight and follow-up regulation by the National Assembly.

5 Policy Suggestions and Expected Policy Outcomes

Policy Suggestions

Legislative Direction for Improving Digital Evidence Search and Seizure Procedures

- Amend regulations on participation rights.
- Maintain a balance between discovering substantive truth and protecting privacy.
- Separate the provisions for investigative procedures from trial procedures in the structure of the Criminal Procedure Act.

Legislative Improvements for Digital Evidence Search and Seizure

- Ensure the legality of information as an object of seizure and redefine the concept of seizure.
- Amend the regulations on the seizure of voluntarily submitted items.
- Propose legislative bills to introduce new search and seizure systems that align with digital evidence.

Strengthen the exclusion of illegally obtained evidence

- Enforce strict exclusion without exceptions to protect privacy and fundamental rights during digital evidence seizure.

Introduce procedures for deleting and destroying irrelevant information

- Develop clear guidelines for when and how to delete or destroy imaged copies of digital evidence to prevent misuse while maintaining fairness in criminal proceedings.
- Consider allowing courts to store evidence until final judgments.

Expected Policy Outcomes

- Raise awareness of the need for search and seizure procedures that align with the digital technology environment.
- Use as foundational material for preparing amendments to search and seizure regulations in the Criminal Procedure Act.

Note

- The Korean Institute of Criminology and Justice (KICJ) was founded in 1989 as the only national crime and criminal justice research institute in South Korea.

  Originally established as the Korean Institute of Criminology (KIC), it underwent a name change in 2021, expanding its research scope to include areas such as civil affairs, international law, and immigration law under the broader umbrella of justice.

  The KICJ conducts proactive interdisciplinary research to formulate and implement evidence-based policies for improved national crime prevention and criminal justice system, continually expanding its research endeavors in these diverse areas.

KICJ
Korean Institute of Criminology and Justice

114 Taebong-ro, Seocho-gu, Seoul, 06764, Republic of Korea
Telephone : +82 2 3460 9218
Email : secretariat@kicj.re.kr
https://www.kicj.re.kr/international