Chapter 19

LEGAL ISSUES PERTAINING TO THE USE OF CELL PHONE DATA

Charles Adams, Anthony Whitledge and Sujeet Shenoi

Abstract This paper examines the principal legal issues related to the use of cell phone data as evidence at trial and to establish a basis for obtaining wiretap orders or call detail records from service providers. Four scenarios are considered. The first three scenarios explore evidentiary issues related to data extracted from damaged SIM cards, partial data recovered from memory chips and deleted data obtained from handsets. The fourth scenario, which focuses on the so-called "Trojan defense," clarifies the important distinction between evidence admissibility and evidence sufficiency.

Keywords: Cell phone forensics, evidence, admissibility, sufficiency

1. Introduction

Cell phones contain large amounts of information – subscriber data, call logs, address books, text and email messages, images, and audio and video recordings [1, 3]. Due to the ubiquity of cell phones and the nature of their use, information recovered from cell phones can be vital in criminal investigations [2, 4]. Law enforcement agencies may use this information to establish a basis for obtaining wiretap orders or call detail records from service providers, and, of course, as evidence at trial.

Obtaining a search warrant or wiretap order requires a factual showing of "probable cause." Such a showing only requires the presentation of enough information to support a conclusion by a judge that there is a fair probability of finding evidence of criminal activity. On the other hand, the admissibility of cell phone data as evidence in a trial requires some verification that the data extracted from the cell phone was obtained by reliable scientific methods and is relevant to the material issues in the case.

This paper uses four scenarios to explore the principal legal issues related to the use of cell phone data to obtain wiretap orders and call records, and as evidence at trial. The first three scenarios examine evidentiary issues related to data extracted from damaged SIM cards, partial data recovered from memory chips, and deleted data obtained from handsets. The fourth scenario, which involves a "Trojan defense," clarifies the difference between admissibility and sufficiency of evidence.

2. Data from a Damaged SIM Card

Consider the following scenario involving the use of data extracted from a damaged Subscriber Identity Module (SIM) card in a cell phone.

> *Before FBI agents arrest him, a suspect in a kidnapping case throws his cell phone into a fireplace. The agents recover some melted plastic, burned electronic components and a damaged SIM card, which cannot be read by conventional means. Using a classified technique, the FBI is able to recover the International Mobile Subscriber Identifier (IMSI) and the name of the service provider from the SIM card. These facts form the basis of an application for a Section 2703(d) order to obtain from the provider the name and address of the subscriber and information about all calls made during the last thirty days. Phone company records show that a call was made to the kidnap victim's parents from a cell phone with that SIM card at the very same time they received a ransom call. Does the defendant have any basis to move to suppress the phone company records at his trial because they were the fruit of an unconventional and possibly improper forensic examination?*

The defendant would not have any basis for a motion to suppress the phone company records if they were offered against him at trial.

This scenario demonstrates the use of SIM card data for investigative leads, but not as direct evidence at a trial. Forensic data must meet evidentiary standards for authenticity and reliability before it may be introduced at trial. However, information used to develop leads or further an investigation does not have to meet these standards. Thus, the phone company records would have to satisfy the standards for admissibility in court, but the SIM card data used to obtain a search warrant or court order does not.

Section 2703(d) of Title 18 of the United States Code authorizes a court to issue an order to a phone company to disclose call records if law enforcement "offers specific and articulable facts showing that there are reasonable grounds to believe that ... the records ... are relevant and material to an ongoing criminal investigation" [16]. The House report that accompanied the legislation described the standard for Section 2703(d) as higher than that required for a subpoena in order to guard against

"fishing expeditions" by law enforcement, but less than that required for a search warrant based on probable cause [17].

The IMSI and service provider information recovered from the damaged SIM card are certainly "specific and articulable facts." Moreover, the circumstances under which the cell phone was retrieved would provide reasonable grounds for a judicial officer to believe that the phone company records would be relevant to the kidnapping investigation.

Even if the Section 2703(d) order was improperly issued, the defendant's only remedy would be a civil suit for damages, not the suppression of evidence in his criminal case. Under traditional Fourth Amendment principles, an individual does not have a sufficient expectation of privacy in a third party's records to challenge the use of the records against him at a trial, no matter how they were obtained [22–24].

In addition, there is an impediment to the defendant raising a Fourth Amendment challenge to the use of information obtained from the SIM card. Since the defendant abandoned his cell phone when he threw it into the fireplace, he does not retain an expectation of privacy regarding the abandoned property [9, 27]. Thus, the defendant can look only to the statute for any remedy for its violation. However, Section 2708 of Title 18 states that the only remedies are a civil action for damages and disciplinary actions against federal agencies or departments for willful or intentional violations [11]. Consequently, there would be no basis for the suspect to move to suppress the phone company records on the grounds that the forensic examination of the damaged SIM card was improper.

In addition, the defendant could not force the government to disclose the classified technique used to recover SIM card data. The U.S. Supreme Court has recognized a state secrecy privilege. Also, it has noted that, in certain circumstances, the government may have to drop a criminal case in order to protect the privilege. In United States v. Reynolds, the court explained that "since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense" [18].

The data from the damaged SIM card would not be material to the suspect's defense, if the data was used only to obtain the Section 2703(d) order, rather than being admitted at trial as evidence against the suspect. The disclosure of a classified technique is analogous to the disclosure of the identity of an informant where there is a public interest in law enforcement maintaining the secrecy of the identity. The U.S. Supreme Court has ruled that the government is not required to disclose the identity of an informant if it relied on information from the infor-

mant to provide a basis for the issuance of a search or arrest warrant [21]. In contrast, disclosure would be required if the informant is to provide testimony relevant to the guilt or innocence of the accused [19].

Thus, the government could prosecute the suspect without having to reveal the means it used to extract the SIM card data, if these means were a valid state secret. If the government sought to introduce the SIM card data at trial, the judicial officer might require some information about the classified technique to verify its relevance and reliability. However, any disclosure could be made under seal in order to protect the classified recovery technique [12, 15].

3. Partial Data from Cell Phone Memory

Consider the following scenario involving the extrapolation of partial data recovered from cell phone memory.

> *After an explosion at a Metro station, law enforcement personnel recover a memory chip from a cell phone that they reasonably believe was used to detonate the bomb. A forensic examiner uses a chip programmer to recover data from the memory chip, including fragments of the call log. Many of the calls in the log were made to or received from known members of radical groups. More importantly, the last call was made to the phone from the number 789-012-XXXX immediately before the bomb exploded. Unfortunately, the last four digits of the phone number, indicated by XXXX, were unrecoverable. Further investigation reveals that Jane Roe, an individual with links to radical groups, has a cell phone number of 789-012-3456. Law enforcement agents use this information to obtain a wiretap order for Jane Roe's phone. The indictment charging her with participating in the bombing is based on the partial phone number in the call log as well as on the conversations recorded during the wiretap. Jane Roe moves to suppress all the evidence because the numbers recovered from the memory chip were obtained using unconventional and unreliable means and did not provide probable cause for the wiretap. How should the court rule on the motion to suppress?*

Unlike the previous scenario, law enforcement agents used the data recovered from the cell phone as a basis for a wiretap order and also as evidence at trial.

Only evidence that can be shown to have been derived from reliable scientific processes is admissible under the rules of evidence. Thus, if the court decided that the unconventional forensic technique used by the examiner was not scientifically sound and could not be shown to produce reliable results, the court would not allow the partial data recovered from the memory chip to be admitted into evidence. In contrast, the conversations were the product of a valid wiretap order and would not be suppressed, even though the information that identified the defendant came from the examination of the chip.

A court may issue a wiretap order under Section 2518 of Title 18 if the judge concludes that there is probable cause to believe that an individual has committed one of the crimes specified in the wiretap statute and that particular communications concerning the crime will be obtained from the wiretap. The U.S. Supreme Court has held that "probable cause does not demand the certainty we associate with formal trials" and that the probable cause requirement is satisfied if there is a "fair probability" based on the totality of the circumstances presented to the judge that evidence of a crime will be found [26]. The information that the judge may consider in issuing a wiretap order does not have to comply with the Federal Rules of Evidence because these rules are not applicable to the issuance of search warrants, and the requirements for wiretap orders are similar to those for search warrants [14]. Hearsay, for example, may furnish a basis for a wiretap order, even though, as a general rule, hearsay is not admissible at trial [7, 20]. The reliability of the information presented to the judge factors into the decision whether probable cause exists. The assessment of reliability is made on the basis of all the information presented, rather than on the basis of each item of information, so that the various items of information can corroborate each other to enhance their reliability [26].

Once a wiretap order has been issued, the determination of probable cause should be given great deference at a hearing on a motion to suppress the evidence obtained from the wiretap [26]. As long as there was a substantial basis for the conclusion that probable cause existed, a motion to suppress the evidence would be denied.

It is clear that there was a plausible basis for a determination of probable cause for the issuance of a wiretap order. The technique the forensic examiner used to recover data from the chip was outside the norm and, therefore, its reliability may be challenged. Nevertheless, the forensic examiner was able to recover the partial number of the phone that "called" the cell phone detonator along with phone numbers of members of radical groups. This information, coupled with the fact that the interpolated phone number belonged to a person affiliated with radical groups, furnish a plausible basis to believe that a wiretap on that phone number would capture communications concerning the bombing. Consequently, the court would reject the challenge to suppress the conversations recorded during the wiretap.

The court must apply a different standard to determine whether to admit the data from the memory chip into evidence. In the scenario, the defendant is challenging the scientific basis of the extraction technique upon which the examiner's testimony about the partial phone number and the other calls will be based. As a general rule, the results of a

forensic examination done using standard tools are considered to be reliable and are admissible because the tools have been tested, show consistent results, and are generally accepted by the forensic community.

As we discuss in the next scenario, in order to be admissible, expert testimony based on scientific evidence must meet the standards of Federal Rule of Evidence 702 and the Supreme Court's Daubert [25] and Kumho Tire [28] cases. These authorities permit the admission of testimony based on scientific evidence that can be demonstrated to be reliable, while denying litigants the use as evidence of the results of non-scientific tests or procedures of dubious reliability. That is, the results of scientific tests or forensic procedures are admissible only when the proponent can show such evidence comes from the application of sound science, and tools and techniques that can be demonstrated to produce accurate and reliable information.

The technique used in this case lies somewhere between an accepted digital forensic technique and a wholly untested approach that was developed for another purpose. Engineers and software developers routinely use chip programmers to read and write data to memory chips. Their use in cell phone forensics to extract data from memory chips is becoming more common [1, 3, 4], and the prosecution will rely on this fact. Nevertheless, the resolution of the issue will probably require a "Daubert hearing" in which experts testify regarding the soundness and reliability of the data extraction technique.

4. Deleted Data from Cell Phone Memory

Consider the following scenario where a programming interface that directly interacts with cell phone memory is used to recover deleted data.

> *Law enforcement agents have identified several members of a drug gang, but not the kingpin. During the execution of a search warrant on a nightclub frequented by crime bosses, law enforcement agents seize several cell phones. A forensic examiner uses a programming interface to recover deleted data from the seized phones. Deleted data from one of the phones indicates that it belongs to the kingpin. At his trial, the kingpin objects to the introduction of the data taken from his phone as evidence because the process that was used to recover deleted data is not reliable.*

Forensic examiners use many tools to extract data from electronic devices. In the early days of digital forensics, hex editors and utilities designed for administrators and software analysts were routinely used to recover data. Over the years, numerous tools and scripts written for other purposes have proved useful to forensic examiners. The main concern about unconventional tools and methods is their reliability. Does the tool or method do what the examiner expects and intends for it to

do? More importantly, does it do anything unintended – such as change data on the target system? The rules of evidence condition admissibility of evidence on a showing that it is reliable. Data recovered using unreliable tools or methods cannot be admitted into evidence.

Rule 702 of the Federal Rules of Evidence, which govern trials in U.S. federal courts, requires scientific evidence to be based on reliable principles and methods for it to be admissible at trial. The main factors used to determine reliability are: (i) whether the technique has been tested and was subjected to peer review and evaluation, (ii) the known or potential rate of error for the technique, (iii) whether standards and controls exist and have been maintained for the technique, and (iv) whether the technique is generally accepted by the scientific community. These factors were refined and articulated by the U.S. Supreme Court in Daubert v. Merrell Dow Pharmaceuticals, Inc. [25]. The Daubert notion of reliability was incorporated into Federal Rule of Evidence 702 in 2000. It requires the trial judge to serve as a gatekeeper in order to keep the jury from considering unreliable expert testimony and scientific evidence that is misleading or not helpful.

The programming interface technique would not satisfy the Daubert factors unless it has been extensively tested. The technique must be subjected to peer review and evaluation, and the rate of error should be known. Also, standards and controls must be enforced on its proper use, and it should be generally accepted by the scientific community.

Nevertheless, the Supreme Court emphasized in a later case, Kumho Tire Co. v. Carmichael [28], that the Daubert factors were never intended to be a definitive checklist. Instead, the trial court's inquiry into the reliability of scientific evidence should be flexible, and recognize that the Daubert factors are not the only tests of reliability. Thus, it may be possible for the government to make a case for the reliability of the programming interface technique even though it has not been subjected to peer review and evaluation and may not be generally accepted by the scientific community.

Repeated tests with consistent results may be necessary to convince a trial judge that the programming interface technique is reliable. Also, it would be desirable to provide as much information about the technique as possible, e.g., whether it had been used in other cases and whether other forensic examiners had used or tested it. If the source code of the software were available, testimony about what it does and how it was used would be important to asserting that it produces reliable and consistent results.

Even if the trial court was inclined to admit the data taken from the cell phone over the kingpin's objections, the kingpin could argue that the data should not be believed – or given "weight" – by the jury.

5. Trojan Defense

The following scenario clarifies the important distinction between admissibility and sufficiency of evidence:

> *An executive of a high-tech company has been indicted for securities fraud. The centerpiece of the prosecution's case is a document discussing improper changes to accounting records to improve the company's quarterly reports. The document was recovered from the executive's smart phone, which was seized during a search warrant executed on his corporate office. The executive objects to the introduction of the document on the ground that it was placed on his phone by a rival. To support his argument, the executive points out that many company employees have the technical skills and equipment to hack his phone. Would the document recovered from the smart phone be admissible as evidence against the executive? May the executive raise the "hacker did it" defense if the document is introduced in evidence?*

The document recovered from the executive's smart phone would be admissible as evidence and the executive could claim that someone else put it on his phone. However, the jury would be free to believe or reject his defense as it chooses. As noted above, the threshold for admissibility is relatively low and the admissibility of an item of evidence depends on its relevance to the material issues in the case. Under Federal Rule of Evidence 401, an item of evidence is relevant if it has "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence" [13].

The facts that the document was found on the executive's cell phone and the phone was in the executive's possession are probably sufficient to connect the document to the executive and meet the admissibility standard. Proof that the document was recovered from the executive's smart phone would be relevant to establishing that the executive was the author or recipient of the document, because it would have some tendency to make it more probable that the executive had knowledge of the document. Even though there is no direct evidence to connect the executive to the document, the fact that the document was recovered from his smart phone is circumstantial evidence that he was aware of its contents. It is up to the jury to decide whether the executive was connected to the document because of its presence on his smart phone.

An inference may be used to connect an item of evidence to a material issue in a case only if the inference is reasonable and consistent with

experience, science and logic. If a case is tried by a jury, both the judge and jury have a role in deciding whether an item of evidence is admissible and relevant. First, the judge must decide whether the inferences on which the relevance of the item of evidence is based are reasonable and consistent with experience, science and logic so that it would be possible for a reasonable juror to conclude that there is a tendency to make a material issue in the case more probable or less probable. If the judge decides that this requirement is satisfied, the item may be admitted as evidence. It is then up to the jury to determine whether to believe the evidence, what weight to give to it and what inferences to draw from it. Thus, the jury has the ultimate responsibility for deciding factual issues, such as whether the executive was the author or intended recipient of the document, but the judge has authority to keep the jury from seeing a particular item of evidence if there is no reasonable connection between the evidence and the material issues in the case.

Two cases involving a "Trojan defense" illustrate these evidentiary principles. In the first case, Aaron Caffrey, a hacker from the United Kingdom, was charged with launching a distributed denial of service attack that brought down the navigation system at the Port of Houston, Texas on September 20, 2001. Law enforcement agents traced the attack to a computer in Caffrey's home. A forensic examination of the computer uncovered a denial of service script and a file containing the IP addresses of more than 11,000 servers that were vulnerable to the attack. When the denial of service software was executed in a controlled environment, it displayed the message: "IIS Unicode exploiter coded by Aaron." Law enforcement agents also recovered chatroom logs from Caffrey's computer stating that a chatroom user named "Aaron" had launched the attack at another user in South Africa in retaliation for insults against his girlfriend.

At his trial, Caffrey denied responsibility for the attacks, and claimed that two other hackers had installed a Trojan program on his computer so that they could remotely control his computer, and that they used it to launch the attack without his knowledge. The prosecution countered with expert testimony that there was no indication of a Trojan on the computer and no known software that could install such a Trojan without leaving a trace. The jury returned a not guilty verdict.

Although there was sufficient evidence to allow the jury to conclude that Caffrey initiated the attack and find him guilty beyond a reasonable doubt, the jury was not required to do so. It is wholly within the province of the jury to decide what weight to give to evidence, to decide what the facts really are, and to decide guilt or innocence based on these facts. The members of the Caffrey jury may have believed Caffrey's claim

rather than the prosecution's expert testimony. On the other hand, the jurors may have voted to acquit Caffrey for other reasons without resolving the Trojan defense issue [5, 6].

A jury reached a different conclusion in United States v. Ray [8]. Thomas Ray was accused of attempting to extort $2.5 million from Best Buy by sending email messages that threatened to exploit a computer vulnerability. After tracing the emails to three AOL accounts, one of which belonged to Ray, the FBI obtained search warrants and conducted forensic examinations of the computers associated with the AOL accounts. The forensic examiner found portions of three of the sixteen extortion emails sent to Best Buy on Ray's computer. Ray raised the Trojan defense at his trial. An expert witness for the defense testified that Ray's computer had no firewall and an outdated anti-virus program, that the Internet Explorer 5.5 browser on Ray's computer had various security problems, and that traces of a Trojan were found on the hard drive. Despite this evidence, the jury convicted Ray on two counts of extortion, and the conviction was affirmed on appeal.

The appellate court ruled that the following evidence supported the jury's decision: (i) Ray admitted he used the computer to connect to the Internet several times a day, (ii) three of the emails sent to Best Buy were traced to the IP address he was using when the emails were sent, (iii) portions of three of the extortion letters were found on Ray's hard drive, (iv) the emails were created by someone typing on Ray's computer who connected to the Internet using Ray's screen name and password to send the emails, (v) no evidence of remote access or hacking was found on Ray's computer, and (vi) Ray had the knowledge and ability to process the monetary transactions that the extortion emails demanded. On the other hand, the decision whether to convict Ray was a matter for the jury, and the jury would not have been compelled to return a conviction.

These two cases and a recent "somebody else used my computer to do it" case (United States v. Shea [10]) demonstrate that, even in cases involving sophisticated technical issues, the jury is free to choose which evidence to believe and which evidence to reject. Where the prosecution can prove the defendant had access to the computer or device at the proper time, the technical ability to do what was done and the motive, the jury is free to infer guilt and reject defense claims that a hacker did it. Conversely, the jury is also free to believe the defense claims and acquit if the prosecution has not proved the negative.

In the case of the high-tech executive, the document would be relevant and admissible into evidence because its recovery from his smart phone would make it more probable that he knew about the document. The

executive would likewise be able to present evidence about the hacking skills of his associates and anything else relevant to his defense.

To overcome this defense, the prosecution might attempt to show that there was no evidence the phone had been hacked. It might also analyze the call log to show that the phone was always in the executive's possession and that it was unlikely that someone else had access to the phone to place the incriminating document.

6. Conclusions

The widespread use of cell phones provides new sources of evidence for criminal investigations. Law enforcement agencies may use this evidence at trial as well as to establish a basis for obtaining wiretap orders or call detail records from service providers. The legal standards for the admissibility of evidence at trial differ substantially from those for obtaining wiretaps or call detail records. The showing required for a wiretap order is essentially probable cause, which means that there is a fair probability based on the totality of the circumstances that the wiretap will produce evidence of a crime. The showing required for a Section 2703(d) order to obtain call detail records consists of specific and articulable facts that there are reasonable grounds to believe that the records are relevant and material to an ongoing criminal investigation. In contrast, admissibility at trial requires proof that the evidence offered has been obtained by reliable scientific methods and is relevant to the issues in the case. It is, therefore, extremely important that law enforcement agencies employ scientifically sound and reliable forensic tools and techniques to ensure that cell phone data recovered using new and evolving technologies will be admissible and useful in judicial proceedings.

References

[1] R. Ayers, W. Jansen, N. Cilleros and R. Daniellou, Cell Phone Forensic Tools: An Overview and Analysis, NIST Publication NISTIR 7250, National Institute of Standards and Technology, Gaithersburg, Maryland, 2005.

[2] Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, U.S. Department of Justice, Washington, DC (www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm), 2002.

[3] D. Harrill and R. Mislan, A small scale digital device forensics ontology, *Small Scale Digital Device Forensics Journal*, vol. 1(1), 2007.

[4] W. Jansen and R. Ayers, Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-101, National Institute of Standards and Technology, Gaithersburg, Maryland, 2007.

[5] J. Leyden, Caffrey acquittal a setback for cybercrime prosecutions, *The Register* (www.theregister.co.uk/2003/10/17/caffrey_acquittal_a_setback), October 17, 2003.

[6] A. McCue, Revenge hack downed US port systems, ZDNet.co.uk (news.zdnet.co.uk/security/0,1000000189,39116978,00.htm), October 7, 2003.

[7] U.S. Court of Appeals (Eighth Circuit), United States v. Garcia, *Federal Reporter Second Series*, vol. 785, pp. 214–218, 1986.

[8] U.S. Court of Appeals (Eighth Circuit), United States v. Ray, *Federal Reporter Third Series*, vol. 428, pp. 1172–1175, 2005.

[9] U.S. Court of Appeals (First Circuit), United States v. Scott, *Federal Reporter Second Series*, vol. 975, pp. 927–931, 1992.

[10] U.S. Court of Appeals (Ninth Circuit), United States v. Shea, *Federal Reporter Third Series*, vol. 493, pp. 1110–1119, 2007.

[11] U.S. District Court (District of Kansas), United States v. Kennedy, *Federal Supplement Second Series*, vol. 81, 1103–1115, 2000.

[12] U.S. District Court (District of New Jersey), United States v. Scarfo, *Federal Supplement Second Series*, vol. 180, pp. 572–583, 2001.

[13] U.S. Government, Rule 401, Definition of Relevant Evidence, Title 28, Appendix – Rules of Evidence, Judiciary and Judicial Procedures, *United States Code (Volume 16)*, Washington, DC, pp. 863–864, 2001.

[14] U.S. Government, Rule 1101, Applicability of Rules, Title 28, Appendix – Rules of Evidence, Judiciary and Judicial Procedures, *United States Code (Volume 16)*, Washington, DC, pp. 930–931, 2001.

[15] U.S. Government, Classified Information Procedures Act, Title 18, Appendix, Crimes and Criminal Procedure, *United States Code (2000 Edition) Supplement V*, Washington, DC, pp. 1524–1529, 2007.

[16] U.S. Government, Section 2703, Required Disclosure of Customer Communications Records, Title 18, Crimes and Criminal Procedure, *United States Code (2000 Edition) Supplement V*, Washington, DC, pp. 1073–1075, 2007.

[17] U.S. House Judiciary Committee, Communications Assistance for Law Enforcement Act, Public Law No. 103-414, *United States Code Congressional and Administrative News, 103rd Congress, Second Session 1994 (Volume 5)*, West Publishing Company, St. Paul, Minnesota, pp. 3489–3515, 1995.

[18] U.S. Supreme Court, United States v. Reynolds, *United States Reports*, vol. 345, pp. 1–12, 1953.

[19] U.S. Supreme Court, Roviaro v. United States, *United States Reports*, vol. 353, pp. 53–71, 1957.

[20] U.S. Supreme Court, Jones v. United States, *United States Reports*, vol. 362, pp. 257–273, 1960.

[21] U.S. Supreme Court, McCray v. Illinois, *United States Reports*, vol. 386, pp. 300–316, 1967.

[22] U.S. Supreme Court, Smith v. Maryland, *United States Reports*, vol. 442, pp. 735–752, 1979.

[23] U.S. Supreme Court, Rawlings v. Kentucky, *United States Reports*, vol. 448, pp. 98–121, 1980.

[24] U.S. Supreme Court, United States v. Payner, *United States Reports*, vol. 447, pp. 727–751, 1980.

[25] U.S. Supreme Court, Daubert v. Merrell Dow Pharmaceuticals, Inc., *United States Reports*, vol. 509, pp. 579–601, 1983.

[26] U.S. Supreme Court, Illinois v. Gates, *United States Reports*, vol. 462, pp. 213–295, 1983.

[27] U.S. Supreme Court, California v. Greenwood, *United States Reports*, vol. 486, pp. 35–56, 1988.

[28] U.S. Supreme Court, Kumho Tire Co. v. Carmichael, *United States Reports*, vol. 526, pp. 137–159, 1999.