GUIDLINES FOR CRIMINAL EVIDENCE

PRINCIPLES OF EVIDENCE

What Evidence

The Law of Evidence of 1984 (Qanoon-e-Shahadat) contains a wealth of useful information that can be used to prove or disprove an alleged fact. Examples include testimony (spoken evidence from witnesses given under oath), written documents such as affidavits, contracts and medical records. It may be helpful to think of evidence as material that assists the court in discerning facts. Once the facts have been determined, the court must apply the facts to the law. Gathering evidence is therefore the starting point for trying to prove any case.

The Rules of Evidence

The rules of evidence determine what matters may be admitted (or not admitted) for the purpose of proving the fact or facts at issue. The rules set out what documents will be admitted into evidence, whether they must be served on the other party, and the time limits for doing so. The rules of evidence help the trial run smoothly and efficiently because testimony and documents are presented to the court in a predictable way, and they also provide for a trial procedure that is fair to both parties.

Admissible Evidence

Admissibility, as defined by the Law of Evidence (1984), means that a judge can consider a party's evidence only if it is admissible. This means that it is relevant to a material fact in the case and is not excluded by any rule set out in case law, relevant statutes or the other general rules.

Material Facts

A material fact is a piece of evidence, which is necessary to discern the truth according to either party's perspective, and without which a proper determination cannot be made. In the civil context, what is material is often determined by the pleadings (written statements of fact such as the statement of claim, statement of defence, and/or third-party claim, which are used to start and respond to a case), as the pleadings elaborate on what is being disputed.

TRIAL AND FORENSIC EVIDENCE

Relevance

Evidence is relevant if it can be used to make the existence or non-existence of any fact appear more probable or less probable than would otherwise be the case.

To decide whether evidence is relevant, one must ask whether it helps to prove or disprove the facts in a case.

RULES to exclude Evidence

There are a number of exclusionary rules that apply within the Law of Evidence (1984). For example, the judge may not allow the use of evidence in court if:

- the evidence is privileged (a party has the legal right to keep the evidence confidential)
- it is in the interest of procedural fairness to exclude it (e.g., one party wishes to rely on a document that they did not disclose to the other)
- The exclusionary rules can be quite complex and difficult to ascertain as they are in many cases derived from common law principles.

Burden of Proof

The burden of proof falls upon the person who approaches the court for a remedy. This means they have the obligation of proving or disproving a fact or issue. This also refers to the obligation to point of evidence already on the record to raise an issue to the satisfaction of the trial judge.

Standard of Proof

In a civil case, the standard of proof rests on a balance of probabilities. This means that one must demonstrate that the existence of a contested fact is more probable than its non-existence, or if one is trying to prove the negative of an issue, they must prove that its absence is more probable than its existence. In all civil cases, the court must scrutinise the relevant evidence with care to determine whether it is more likely than not that an alleged event occurred. The civil standard of proof requires a lower standard than its counterpart in criminal law, which requires proof beyond a reasonable doubt. The criminal standard of proof is never applied to civil cases.

Judicial Notice

A judge can acknowledge that a fact has been proven without the lawyer having to prove it if the community is generally aware of the fact; this is called judicial notice. A judge can only take judicial notice of facts that are beyond dispute by reasonable persons or if they can easily be confirmed by reference to an authoritative and accurate source.

Admissions

A party can admit that certain facts or issues are not in dispute. Also, both parties can inform the court that they agree on certain facts in the case; this is called an agreed statement of facts. It will speed up the trial process because those facts do not need to be proved in court.

EVIDENCE AT TRIAL

Evidence given by Witnesses

A witness is a person who gives evidence to the court orally under oath or affirmation (see below) or by affidavit (a sworn written statement). Witnesses are a critical part of the trial process whether they are giving evidence about what they saw happened or confirming that a document is authentic. A witness must be prepared to answer questions and give accurate information to the court. It is the role of the parties, not the court, to call and examine witnesses.

Preparing Witnesses for Trial

Preparing a witness prior to a trial involves meeting with the witness in order to review the evidence that he or she will provide. If there is more than one witness, the lawyer should review the case with each of them individually. These are the most important matters to review:

- Evidence that the witness will be giving in court
- Documents that will be shown to the witness in court
- Types of questions that will be asked in the direct examination (examination in chief)
- Types of questions the other party may be asked in cross-examination
- How to answer questions clearly (in other words, just give the facts)
- Courtroom etiquette

Refreshing the Witness Memory

Trials are often held several years after the event that led to the dispute. Unsurprisingly, witnesses may have trouble remembering the details that they are asked to provide to the court. A lawyer can help "refresh" the memory of their witness before and during trial

Before the Trial: It is reasonable for witnesses to refresh their memories on information and events that they will be asked about. It is advisable for a lawyer to talk to their witness about the issues in dispute and the type of questions that will be asked. They may also want the witness to review documents that will be introduced into evidence. It is important to remember that a well-prepared witness may affect the weight the judge gives to their testimony. For example, if a witness sounds as though they are reading from a pre-prepared script, the judge may not believe that their answers are genuine and may not give much weight to the evidence.

During the Trial: With permission from the judge, if a witness has no present memory, the witnesses can refresh their memory by referring to notes or documents that were made closer to the time of the event in dispute. The witness can do this if: the document was made by the witness at or near the time of the event while the witness's memory was fresh, or the document was created by a person other than the witness who was recording

events or matters observed or heard by the witness. In the case of the latter, the witness must confirm that it was indeed accurate.

Oral Testimony of the Witness

Most evidence is introduced at trial to the court through witnesses giving testimony (spoken evidence given under oath). Witnesses can be the parties themselves or others who have particular knowledge or information about the case. It is usually a good idea to ask the judge to exclude witnesses who are not parties during the trial. This means that they have to wait outside the courtroom until it is their turn to give evidence. It prevents the witnesses from hearing each other's testimony and changing their evidence in response to what they have heard.

Telling the Truth

Before a witness gives evidence to the court, they must agree to tell the truth. Witnesses can take an oath to tell the truth and swear that the evidence they are about to provide will be factual. In this case, there is no religious meaning to the commitment to tell the truth. An affirmation has the same effect in law as an oath. The judge will give the same amount of weight to the evidence provided whether the witness takes an oath or affirms to tell the truth.

Requirement to give Evidence

Witnesses who do not want to testify or cannot be relied upon to come to court can be compelled to give evidence at trial by serving them a summons, notice or warrant at their home or place of work. A summons to witness is a legal document that tells a witness that they are required to attend court in order to give evidence. If witnesses under summons do not appear in court to give evidence, a warrant can be issued for their arrest and they can be brought to court to testify.

EXAMINATION OF A WITNESS

Direct Examination (Examination in Chief)

The Law of Evidence (1984) reveals that when a witness has taken the stand to give evidence and been sworn in, their party will “examine” or ask them questions first. This is called “direct examination” or “examination in chief”. After a direct examination, the other party will be allowed to cross-examine that witness. Witnesses provide critical evidence at trial, but they do not take the stand and simply talk about issues in the case. It is the responsibility of lawyers to structure their questions for the witness so that the evidence is presented to the court in a logical way.

Questioning Witnesses

When asking questions, it is important to allow the witness to answer them in their own words. This makes their evidence more credible. Some examples of appropriate questions, in a hypothetical action arising out of a motor vehicle accident, are:

- What happened when you reached the intersection?
- What did the other driver say to you after the accident?
- Where were you looking?
- Why did you go there?

Leading Questions

Generally, a lawyer cannot ask "leading" questions when they are examining their own witnesses. The most common example of a leading question is one that suggests the answer to the witness. Note that you can ask leading questions when you are cross-examining the other party's witness.

What Is a Leading Question ?

"The car was speeding, wasn't it?" is a leading question. But asking "How fast was the car going?" asks the same question in a way that is not leading. There are some exceptions to this general rule regarding leading questions. It is appropriate to ask leading questions of one's own- witness when:

- The information is introductory (for example, the time, date, and location of the accident)
- People or things are being identified (for example, name and occupation of witness)
- The matter is not disputed (for example, ownership of the car)
- The court gives permission to ask a leading question (for example, when a party's witness is unwilling or unable to give responsive answers, the trial judge may decide, on the request of the prosecutor, to declare the witness as hostile.

Personally, giving Evidence

If an individual who wishes to personally represent their own case in court, they will not have anyone to ask them questions when they give evidence. Instead, the party in question will tell the court their own version of the case. This process involves getting into the witness stand, swearing or affirming to tell the truth and giving one's own version of events. It can be helpful if the individual in question imagines that they are responding to their own questions. This can make it easier to organise information in a logical and thoughtful manner.

Example: How to give Evidence

These questions from a hypothetical case involving a motor vehicle accident can be used as a guide for self-questioning:

- What day was it?

- What time was it?
- What was the weather like?
- Was it light or dark outside?
- Where were you going?
- Were you in a hurry?
- What was your route?

Cross-Examination

Cross-examination is when one party asks the other party and their witnesses questions. The purpose of cross-examination is:

1. To get testimony from the other party's witness that supports a case
2. To discredit the witness (make the witness's evidence look less believable).

The scope of questions in cross-examination is broad; you can ask any questions that are relevant to the case, as long as you do not harass the witness. Unlike the direct examination of a witness, lawyers will often ask the witness from the opposing party leading questions. When a witness takes the stand to give evidence, their credibility is on the line. Therefore, in cross- examination, it can be advantageous to ask leading questions in order to make the witness appear less credible.

Case Study on Cross Examination

In a hypothetical case a witness may have testified under direct examination that they drove straight home after work on the day in question. A cross-examination from the opposing party may focus on their knowledge that, in fact, he or she was seen hanging out with friends at the restaurant for three hours after work.

A cross-examination can focus on the following areas:

- Showing that the witness favours the other party (he or she is biased)
- Showing that the witness has contradicted himself or herself in previous statements
- Challenging the witness's memory on certain points
- Challenging the witness's version of events

Neither party is required to cross-examine every witness, but if they choose not to cross- examine a witness, his or her evidence may be accepted because nothing has been introduced to contradict it. During cross-examination, the witness should have a chance to explain things that are being introduced as evidence against them. It is not appropriate to "ambush" the witness by bringing in unexpected evidence that they have not had a chance to explain or disagree with.

Re-Examination

A lawyer can choose to re-examine their own witness if the cross-examination raised an issue that they did not deal with in their direct examination. Re-examination is an

opportunity to respond to new issues raised in cross-examination, but it should not be viewed as not an opportunity to raise new issues which may have been forgotten in the original examination. The judge may also give permission for a second cross-examination of a particular witness. This may happen if the other party raised new issues with the witness during their re- examination.

Hearsay

Hearsay is an oral or written statement that was made by someone other than the person testifying at the proceeding, made outside of court, that the witness repeats (or produces) in court in an effort to prove that what was said or written is true. As a rule, hearsay is generally not admissible as evidence in trial

Opinion Evidence

A witness's role is to tell the facts to the court, and the judge's role is to draw a conclusion based on those facts. The opinion of a witness is generally not admissible; however, there are many exceptions to this rule.

Expert Witnesses

An expert is someone qualified with special knowledge, skill, training, and experience (such as an engineer or a doctor). An expert can express an opinion based on information that they have personally observed or information that was provided by others. An expert in motor vehicle accident analysis could go to the scene of an accident, measure skid marks, and give the court an expert opinion about the speed of the cars involved in the accident. Or, the expert might be able to give an opinion based on photographs of the accident scene. An expert witness's opinion is admissible if:

- It is relevant
- It helps the judge to make a decision
- The expert is properly qualified
- There is no other reason to exclude the evidence
- If a party in a trial hires an expert to give evidence to support their case, they must get the expert to give his or her opinion during the direct examination. The expert must explain:
- Their professional qualifications (specifically how it related to that particular issue)
- Their professional opinion
- The facts considered in reaching this opinion
- Any tests or experiments performed

During cross-examination, the other party will try to find reasons why the court should not accept the expert's opinion. For example, the other party may question the expert's qualifications and experience or the facts on which the expert's opinion was based. If the expert witness does not have personal knowledge of the facts of the case, the expert may be asked to consider a hypothetical question or situation where certain facts are assumed to be true. The expert will give an opinion based on those facts.

Documents as Evidence

Documents can also be used as evidence in court. The word "document" has a broad meaning. In general, a document is any physical or electronic record of information that has been recorded or stored by means of any device (including photographs, films, sound recordings, etc.)

When thinking about what type of evidence can be used to prove a case, it is important to remember that a document is anything that contains information. Items such as a memo, invoice, letter, drawing, transcript, information on a computer hard drive, floppy disk, or CD would all qualify.

Proving Documents at Trial

At trial, a document can be put into evidence:

- To prove that it is authentic (real)
- To prove its contents.

To prove that a document is authentic, the person who created the document can be called as a witness to give evidence about it. Or, the document's authenticity can be admitted, for example, under a request to admit. If a document is put into evidence to prove its contents, it will be considered hearsay and therefore not admissible, However, if it falls within one of the exceptions to the hearsay rule, the use of documents as evidence is covered by the "best evidence" rule. Under these circumstances, the party in question must submit the original copy of the document if they wish to use it as evidence. If the original document cannot be produced, an explanation must be given to the court regarding the use of a copy. For example, the original might be lost, destroyed, or someone else may have it. The "best evidence" rule does not apply to a party who tenders a document solely for the purpose of identifying it or proving its existence.

FORENSIC EVIDENCE

Introduction

Evidence refers to information or objects that may be admitted into court for judges to consider when hearing a case. Evidence can come from a wide variety of sources such as genetic material, trace chemicals to dental history, fingerprints and many others. Evidence can serve many roles in an investigation, such as to trace an illicit substance, identify remains or reconstruct a crime.

Types of Forensic

- Forensic Anthropology and Forensic Dentistry
- Controlled Substances
- Digital Evidence and Forensics
- Why Traditional Forensics Techniques Are Less Effective With Digital Evidence

- Types of Images Captured by Digital Evidence Investigative Tools
- Case study

Forensic Anthropology and Forensic Dentistry

- **Forensic Anthropologists** examine "skeletonised" or otherwise compromised human remains to assess age, gender, height, ancestry, identify injuries, and estimate the time since death. Examination of these remains may give information that can assist investigators in identifying a victim.
- **Forensic Dentists**, or **Odonatologists**, examine the development, anatomy and any restorative dental corrections of the teeth, such as fillings, to make a comparative identification of a person.

Bones and teeth are the most durable parts of the human body, and they may be the only recognisable remains in cases of decomposition, fire scenes or mass fatalities. They are often used to identify an individual in such cases. For example, when law enforcement officials find unidentified human remains such as teeth, this critical piece of evidence may be the only resource investigators can use to compare to dental records of known missing persons to determine the person's identity.

Controlled Substances

Controlled substances are chemicals that have a legally recognised potential for abuse. They include “street drugs” such as heroin or ecstasy and prescription drugs such as oxycodone. Detecting and identifying controlled substances is a critical step in law enforcement's fight against drug-related crime and violence. Controlled substances present law enforcement and criminal justice professionals with the following problems:

- Large quantities of drug evidence are collected and submitted to crime laboratories, resulting in backlogs.
- New designer drugs emerge regularly, requiring crime laboratories to develop new analytical techniques and spend more time on analysis.
- Many drugs are similar in appearance and properties, creating a high degree of difficulty in distinguishing their exact identity.

New technology is needed to improve law enforcement efforts to address these issues. To achieve these goals, the following steps are important: -

- More sensitive detection tools to use at crime scenes.
- Improved tools and techniques to identify controlled substances including emerging “designer drugs” and evolving manufacturing techniques for existing drugs.
- New, faster and more efficient tools and techniques to analyse controlled substances in the laboratory.
- Improved ways to integrate tools, techniques and skill sets of other forensic disciplines to analyse controlled substances.

Digital Evidence and Forensics

Computers are often used for committing crimes, and, thanks to the burgeoning science of digital evidence forensics, law enforcement now uses computers to fight crime. Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other places. Digital evidence is commonly associated with electronic crime or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes. For example, suspects' e-mails or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their relationship with other suspects. In 2005, for example, a floppy disk led investigators to the BTK (Bind, Torture, Kill) serial killer who had eluded police capture since 1974 and claimed the lives of at least 10 victims. In an effort to fight e-crime and collect relevant digital evidence for all crimes, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics, into their infrastructure. Law enforcement agencies are challenged by the need to train officers to collect digital evidence and keep up with rapidly evolving technologies such as computer operating systems.

Digital Evidence Investigative Tools

Digital evidence investigative tools are needed to efficiently and effectively collect digital evidence from crime scenes.

As technology advances, so has the knowledge required by law enforcement officers at a crime scene. The scope of evidence to be searched for and collected at a crime scene now includes digital evidence such as cell phones and computer networking devices. Some of these devices might be hidden in ceilings or other locations that are not immediately evident. At the same time, forensics experts face an ever-expanding backlog of digital evidence due to the increased use of computers. Training and preparing first responders to perform preliminary investigations could help reduce the digital evidence backlog and help law enforcement make significant headway into solving a range of crimes including:

- Computer threats
- Missing person cases
- Fraud cases
- Theft

It allows law enforcement officers who are not computer experts to conduct basic analysis of digital evidence at crime scenes. Onsite analysis by first responders would speed up initial investigative tasks, reduce the workload of digital forensics experts and allow them to focus on more in-depth digital evidence analysis.

Case Study – Daniel Pearl's Case

In the case of the abduction, and eventual murder, of the journalist Daniel Pearl in Karachi,

the ransom notes were the tipoff. In sending those notes by e-mail, the kidnappers unintentionally gave investigators an electronic trail which they could trace back to the sender's computer. On February 4, 2002, the police traced the e-mails and photos announcing Pearl's kidnapping and ransom request to Speedy Internet, a Karachi Internet café owned by a Pakistani, Sheikh Naeem. The owner produced records showing that a young man, an unemployed computer programmer named Fahad Naseem, had sent the e-mails. The tipoff led police to him, and they successfully apprehended him. In addition, they found, sitting on a table in plain view, a laptop computer, hard drive and a scanner. For hours, at the U.S. Consulate, FBI computer forensics expert Ronald J. Wilczynski dug into the hard drive, which had been reformatted to hide its old contents. As he looked in the directory for clues, an initial search for Pearl's name produced nothing. He found a job inquiry letter that Naseem had written asserting, "I believe in personal ethics such as integrity, honesty, and accountability for actions taken." Finally, the computer forensics expert took a word from one of the ransom notes: "Amreeka." This provided him with his first real success: an electronic trail of the ransom notes. Wilczynski searched for photos and eventually found hostage photos of Daniel Pearl. The FBI agent also found web pages that showed browsing to news websites prior to the kidnapping and Naseem's resume and cover letter to potential employers. Fahad Naseem later pointed the kidnaping instigator as a man named Omar Sheikh, an all-around bad guy known in radical circles for kidnappings and ties to Pakistani militants.

Sample Qualification Questions for Digital Evidence/ Forensics Expert Witness

1. Please state your full name.
2. What is your official address?
3. Where are you employed?
4. What is your position there?
5. How long have you been employed at this organisation?
6. What is your job function at this organisation?
7. Where were you employed prior to your current job?
8. What was your position there?
9. How long were you employed there?
10. What was your job function at that company?
11. How long have you been doing computer forensics?
12. Have you ever been hired as a computer forensics expert in the past?
13. Have you ever testified in the area of forensics or appeared as a witness in a court?
14. How many times have you appeared as a digital forensics expert witness?
15. Have you received any training specific to computer forensics?
16. Do you hold any course certifications specific to digital forensics?
17. Do you have a degree or certificate in digital forensics?
18. Can you briefly explain what digital forensics is?
19. Can you briefly explain chain of custody?
20. Have you published any articles in the area of digital forensics?
21. Have you ever been invited to speak at any conferences related to digital forensics?

Some Useful Computer Terms

It is helpful to know the definitions of some terms related to electronic information when attempting to obtain discovery of computer-related information. The following list includes several basic terms that an attorney should know to assist in understanding electronic information.

Active Data - These are the currently-in-use data files. They may be stored on any computing device, not just the hard disks of a network server.

Backup Data - Information copied to removable media (tapes, zip TM drives, CD-ROMs, etc.) to be used to re-establish the system in the event of a failure. Normally the data is stored in a compressed form that must be "restored" before it is usable.

Bookmarks - More accurately called network addresses, these are shortcuts that mark a location on a network to which the computer can quickly return "at the push of a button." The marker is typically created automatically upon the request of the computer user and stored on the user's computer.

Cache Files - These files record Internet addresses visited by the user and graphic elements of the webpages visited. These files are created and stored automatically by the user's computer, and provide detailed trail markers identifying the path the user has travelled on the internet.

Cookies-These files contain bits of information about the user and/or the use of the computer, such as the user ID, details the user may have filled out on a form, past purchases and other personal data. The files are placed on the hard drive by the website operators. Cookie "crumbs" are sent back to the website every time the computer returns there, so the website can track the user's patterns and preferences.

Embedded data - This is information contained within an electronic version of a document that is not usually apparent on screen or in the printed "hard copy." Examples of the information revealed by these "byte-marks" are the date the document was created, the identity of the author, the identity of subsequent editors, the distribution route for the document, and even the history of editorial changes (for example, pieces of the drafts leading up to the latest version of the document may be invisibly and automatically saved by the computer and hidden in the files). This information is also called "metadata."

Legacy Data - Older information stored in an electronic format that can no longer be read using current software or hardware.

Replicant Data - These files are automatically created as part of a redundant system designed to eliminate system failures (or down-time).

Residual Data - This information includes the entirety or remnants of deleted files to which the file reference has been removed from directory listings making the information invisible to most application programs. Because the name is removed from the directory and from the file allocation table (FAT), the file does not appear to exist.
However, the digital information remains on the media until it is overwritten by new data.

Mobile Telephones

A mobile or cellular telephone is a long-range, portable electronic device for personal telecommunications over long distances. In addition to the standard voice function of a telephone, current mobile phones can support many additional services such as SMS for text messaging, email, packet switching for access to the Internet, and MMS for sending and receiving photos and video. Most current mobile phones connect to a cellular network of base stations (cell sites), which is in turn interconnected to the public switched telephone network (PSTN); the exception to this being satellite phones. Due to the high penetration rate of mobile phones, they will inevitably be connected to an increasing number of criminal activities. The following examples illustrate some of the possible ways in which a mobile phone can be involved in criminal activities.

- Mobile phones are the most common form of communication for people purchasing contrabands
- Mobile phones are common targets for thieves
- Telecommunication service theft (i.e. mobile phone theft, SIM cloning, etc.) make up a significant portion of telecommunications fraud.
- The relatively large storage space of modern phones makes them a useful tool for data theft. An employee could steal sensitive corporate information by uploading it onto their phone.
- They are the primary device used for sending threatening SMS messages and making abusive phone calls to the victim. The call records, and SMS messages between both parties can play a significant part in such a case.

Since they may contain information comparable to that of a desktop computer, they are a prime source of evidence. The following list of potential evidence that can be found in a mobile phone:

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook information
- Appointment calendar information
- Text messages
- Dialed, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging and Web browsing activities
- Electronic documents
- Location information
- Browsing history
- E-mails
- Audio and video recordings
- Pictures
- Appointment calendar entries

- GPS Data (locations the phone has been)
- Location of photos taken
- Hot list
- Pin data
- SIM card data
- Data stored on internal and removable memory service provider
- IMSI

Because of new features on mobile phones such as increased memory storage and third-party applications, both the quantity and complexity of the above evidence is increasing.

- The SIM card (if present)
- The phone's embedded memory
- The phone's removable memory (i.e. SD card), if present

In addition to these, subscriber and call related information is also stored by a service provider. Data can also be stored in a phone's memory. In addition to the SIM memory, memory is available within the phone to store phone software and additional data. This space can be used to extend the SIM memory, to store additional phone book data, call logs and so forth. The following are some examples of the additional information that may be found in a phone's memory:

- Phone settings
- Calendar information
- SMS / MMS messages
- Call log entries
- Time and date
- Ring tones
- Data required for / produced by the phone's extra features, such as audio and video recordings, and images
- Generic data stored in the phone's memory
- Application executables