DETECTING INVISIBLE TRACES GENERATED BY A CELLPHONE AT A CRIME SCENE

Hennie Lochner¹ and Rudolph Zinn²

ABSTRACT

Observations made by the authors of this article, suggest that investigators in South Africa may possibly be conditioned by tradition to limit their search for physical clues or traces to a crime scene and not to consider the use of new investigative approaches to find traces that are recorded at a remote location from the crime scene. The type of evidence presented in court cases also suggest that investigators focus exclusively on the Locard Principle or Contact Theory – traces left behind at a crime scene due to physical contact between objects and people at the scene. These observations suggest that the traditional concept of the Locard Principle is so strictly adhered to that it constrains the investigator who wants to think innovatively. For example conceptualising other places where traces of contact may be found. The objective of this article is to explore the concept of modern criminal investigation with regard to cellphone technology and critically analyse the relevancy of the Locard Principle regarding traces left by cellphones that were found at a crime scene. The article, furthermore, examines that the Lochner Principle determines that even though a cellphone signal might be present as a trace at a crime scene, proof of the signal can only be found on the electronic database of the cellphone service provider, which is kept at a location some distance from the crime scene. A discussion of the two principles and practical examples show how traces are left behind in terms of Locard's principle and the effect that the application of both these principles would have had on recent criminal cases. The authors further postulate, as a second focus point in the article, that data automatically generated by the cellphone on the computer server other than when a call or text messages is made, can be used as additional data to determine the location of a cellphone at a crime scene. The article, therefore, aims to provide additional dimensions to be considered when thinking about the detection of traces according to the Locard Principle. The data is based on a review of current literature and applied research on how cellphone technology can be used by investigators. The analysis of the data, among others, is done in the context of the authors’ experience as academics and former investigators and contains an element of action research.

Keywords: automatic continuous registration of a cellphone; cellphone records; electronic data; Contact Theory; Locard and Lochner principles; modern criminal investigation with regard to cellphone technology

INTRODUCTION

The underlying principle in the investigation of a crime scene is that traces will be left when a crime is committed (Newburn, Williamson & Wright, 2011: 320). If no traces are found, it may lead to the assumption that there are no traces or that no contact took place between objects at the crime scene. This is in contradiction to Van Rooyen’s (2004: 11) statement that an investigating officer can always safely assume that traces will be left behind at a crime scene. Van Rooyen (2004: 11) further argues that if no traces could be found, it is not because there were no traces, but because the techniques or the knowledge necessary for identifying the traces and collecting them are either inadequate or the investigating officer is

¹. Senior Lecturer. Department of Police Practice, School of Criminal Justice, College of Law, University of South Africa. Email: Lochnht@unisa.ac.za
². Professor. Department of Police Practice, School of Criminal Justice, College of Law, University of South Africa. Email: Rzinn@unisa.ac.za
This article postulates, inter alia, that the use of modern electronic communication devices at a crime scene do not necessarily leave a visible trace at the crime scene, which requires an additional dimension to Locard’s Contact Theory in searching for traces.

Platt (2003: 88) points out that Locard’s theory is regarded as the cornerstone, basic dogma, and fundamental reason for investigating a crime scene and it is used in crime scene investigation when seeking to uncover traces of the truth. Locard’s principle or Contact Theory is also referred to as the transfer of traces as physical clues at a crime scene.

Most investigators use Locard’s principle as a starting point in their search for traces at the place or places where a criminal comes into contact with an object, persons or scene. Formulated in 1926, the Locard Principle is still of crucial importance, but was formulated long before the technological developments that constitute contemporary society. For example, cellphones have had a tremendous impact on our daily lives and the media regularly reports on how cellphones are used in the commission of crimes. Locard’s principle, does not per se contain a detailed description of the transferable traces left, the recording thereof; and the tracing of supportive evidence by a cellphone handset that was at or used at a crime scene.

The investigator might even find it challenging to prove that a cellphone was used at a crime scene. Developments in modern communication technologically also offer new possibilities for the investigation of crime and crime scenes. For example, the cellphone network always configures the geographical location of an active handset electronically irrespective whether the cellphone network is activated by making or receiving a call, sending or receiving a short text message (sms) or by automatic (mechanical) continuous registration of the handset (without the handset being used for communication by the user). The only requirement for a trace to be left on the computer database is that the handset must be switched on. In the instance of a call or text message, there are connections between two handsets or a handset and a landline or the other way around. In the instance of a cellphone that is switched on but not used, the cellphone network still communicates continuously with the handset. The data that is automatically recorded on the location of the handset in this instance can also be used to map the location of the handset. The connections are recorded as traces and in this way the trace which is left can be gathered and used as evidence. This information can determine the location of all persons involved in a crime at a given point in time.

Another purpose of this article is to demonstrate that even though electronic communication in the form of a handset’s invisible signals can be left behind at a crime scene, the evidence thereof is not left or traceable at the crime scene. The argument is based on the fact that the network’s record of its internal communication; operational functioning; the possible transfer (switching) of the handset’s signals between cellphone towers (base stations) or the sectoral micro or pico cells within a cellphone tower’s area of coverage (locational area including a crime scene) is stored on a computer databases away from the crime scene. The record or proof of the activity of the signals at the crime scene is continuously recorded off site as data on the computer software that operate the server of the cellphone network provider.

The traces generated by the use of cellphone handsets, therefore, mean that Locard’s principle is not the only valid guideline that can be used for detecting where traces that were transferred during a crime can be traced. The concept of accommodating new developments in criminal investigation is in line with the approach by Inman and Rudin (2001: 94) who state that no one has yet been able to disprove Locard’s principle, and that it should be up to forensic science to begin a process of testing the principle scientifically. Knowledge of the Lochner Principle that was established in 2006 and registered as a patent in 2010, brings about confirmation of the Locard Principle with regard to cellphone technology, but also
expands the concept of where these traces should be searched for. This is an additional and supplementary perspective to the Locard Principle.

RESEARCH FRAMEWORK
The data for the study is derived from an in-depth analysis of literature, the applied knowledge of the authors as academics and former investigators; and qualitative data based on an interview with a renowned expert on cellphone technology. One of the authors also received specialised in-service training on cellphone technology while he was still a detective. Marshall and Rossman (2011: 59) and Flick (2011: 89) are of the opinion that qualitative research can be done which is based on the experience of the researcher.

The expert interviewed was Dr Peter Schmitz of the Council for Scientific and Industrial Research (CSIR), who is the leading scientific expert in the field of cellphone technology in South Africa. He has, on several occasions, testified about his field of expertise in court. One of the most recent cases in which he testified on behalf of the prosecution was the case heard in the Western Cape High Court against Thandi Maqubela and Vela Mabena for murdering former High Court Judge, Patrick Maqubela (Schmitz, 2013; Seapoint CAS 141/06/2009). Schmitz has also published articles on cellphone technology and the mapping thereof in accredited journals and presented papers on the topic at various national and international conferences (cf. Schmitz, 2000; 2002; 2007; 2009; & 2010).

KEY TERMS
The automatic continuous registration of a cellphone
A cellphone that is switched on (activated) but not used for communication by the user automatically (mechanically) communicates with the cellphone network on a continuous basis. During this automatic continuous process the information on the activity of the handset is sent to the "Visitor Location Register" (VLR) (Schwartz, 2005: 199; Marshall, 2008: 116).

Cellphone record
This is the total version of all the activities of the cell phone that have been registered by the network and are reflected in the cellphone documents (Lochner, 2007: 68).

Electronic data
The Electronic Communications and Transactions Act 25 of 2002 defines data as an electronic representation of information in any format and a data message as data that is produced, sent, received or stored electronically (South Africa, 2002).

CRIMINAL INVESTIGATION
Gay, Beall and Bowers (1984: 50–55); Rheinier, Greenless, Gibbens and Marshall (1979: 15); Hough (1980: 344-357); Ronczkowski (2004: 4); and Higgens (2004: 71) have all shown that the police infrequently use [or consider] new technological aids and techniques. They ascribe this, inter alia, to a closed police culture, an unwillingness to experiment, fixed ideas, short-term financial planning, and in some instances a lack of vision and insight into the advantages associated with new technology. The new technology would include the latest development in cellphone technology and its relevance to the Locard and Lochner principles. The Locard and Lochner principles are applied as part of a criminal investigation. It is, therefore, necessary to contextualise the role of the principles in the criminal investigation process.

Criminal investigation in South Africa is a statutory obligation of the South African Police Service (South Africa, 1996: sec. 205 (3)). It is also reflected in literature as core responsibility of a [any] police service or force (Wrobleski & Hess, 2000: 240; Maguire, 2003: 366; Rogers & Lewis, 2007: 150). The aim of a criminal investigation is to uncover the truth with the intent of solving a criminal incident (Rogers & Lewis, 2007: 151; Gilbert,
To determine the truth, requires a criminal investigation that is logical, objective, and a legal enquiry into a possible criminal activity (Gilbert, 2010: 34). The truth includes determining who committed the offence, but could also include determining whether a person charged with an offence is guilty or innocent (Wroblewski & Hess, 2000: 241; Rogers & Lewis, 2007: 151). Maguire (2003: 366) postulates that criminal investigation has played three critical roles as an edification to combat crime: it is a ‘gateway’ for criminals into the justice machinery; it is a deterrence factor for anyone tempted to offend that there is a high risk of getting caught; and it reassures the public that the police is effective in protecting them from the worst offenders. A criminal investigation can be viewed as an integral part of the police function in the formal social control structure in which internal order is maintained (Grové, 1985: 53).

**PHYSICAL EVIDENCE AND DIGITAL TRACES**

To determine the truth, the criminal investigation process revolves around the collection of information. The information includes any leads that could be followed during the investigation, but also information that would be admissible as evidence in a judicial enquiry (Rogers & Lewis, 2007: 157-158; Gilbert, 2010: 52; Osterburg & Ward, 2010: 21). Information could be collected through a range of sources during a criminal investigation which include subjective and objective sources. Information that is admissible as evidence in a criminal proceeding is called evidence. Evidence that is tangible is known in literature as real or physical evidence. Physical evidence is considered to be an objective source. The advantage of physical evidence as an objective source is that it provides objective facts to a judicial enquiry. The inclusion of physical evidence in a judicial enquiry provides a safety net to ensure that the outcome of the investigation is not tainted by human emotion or compromised by other human errors (Saferstein, 2013: 20). The presence of physical evidence at a crime scene or on a human or object, however, relates to the mutual cross-transfer of material (Saferstein, 2013: 8). The cross-transfer of material is what is described by the Locard Principle.

The traces, clues and physical evidence identified and collected at a crime scene are currently regarded as synonymous in the investigative milieu. They are seen as evidence or proof which can be used to uncover the truth. If possible, they are physically presented to the court and form part of the evidence on which judicial officers make a decision (Brown, 2001: 49; Joubert 2010: 354).

Physical evidence is reliable and factual information which is never wrong or false and which is both observable and recognisable as a liquid, object or implement (Marais 1992: 6). The best feature of physical evidence is that it never lies because it is dumb. It is the duty of the investigating officer to identify the physical evidence, collect it and send it for expert analyses. In special cases (high profile cases), the investigating officer may use experts to collect physical evidence. It, however, remains the responsibility of the investigating officer to ensure that all traces (physical evidence) are collected through which the true facts of the crime can be exposed (Gardner, 2005: 25).

It is argued by Jordaan (in press) and Pollitt (2008: 17–26) that the Locard Principle forms the cornerstone of forensic science, and has evolved into guiding principles and processes that can apply equally to digital evidence, as much as they do to traditional physical evidence. Lochner, Benson and Horne (2012) and Lochner (2007: 120) also postulate that the signal from a cellphone, as digital evidence, meets with all the requirements for physical evidence.

A cellphone works through the concept of generating and receiving digital messages. Digital messages are information that is stored or send in electronic or magnetic form. When a cellphone is activated (whether by switching it on, making a call or receiving a call), it is
done by means of a signal between the handset and the cellphone tower. This can be seen as the activation of the cellphone on the cellphone network and is done through digital messages. The signal is invisible, but the data regarding the activation of the network is registered and stored on the cellphone network’s system. The entries on the cellphone record of a specific handset are a result of the activities on the cellphone and are processed by computer programs and recorded as data on the cellphone record. Computer printouts of cellphone records can be accepted as evidence in court (Ex Parte Rosch 1998 I All SA 319 (W); Mdlongwa 2010 (2) SACR 419 (SCA); S V Dos Santos 2010 (2) SACR 382 (SCA)). The information on the cellphone record that was recorded by software on the computer system of the cellphone service provider is considered to be direct and real evidence. This is due to the information not being dependent or subject to the credibility of a person (S v Ndiki 2008 (2) SACR 252 (Ck) 264h-265a; Ex Parte Rosch [1998] I All SA 319 (W) 321; Mashiyi 2002 (2) SACR 387 (Tk) 393d-e: Ndlovu v Minister of Correctional Services [2006] 4 All 165 (W) 173f-g).

ADMISSIBILITY REQUIREMENTS FOR PHYSICAL EVIDENCE
For physical evidence to be admissible in court it must meet the requirement of relevancy. The vital fact is that physical evidence should sufficiently connect the accused person with the victim, complainant or crime scene (Ingram, 2012: 565). According to Hosten, Edwards, Nathan and Bosman (1977: 791), Du Toit, De Jager, Paizes, Skeen and van der Merwe (1997: 24-12A) and Kriegler (1993: 510) the viewpoint of the South African courts is that the relevancy of physical evidence is based on a mixture of common sense, logic and experience.

To present physical evidence in court, the investigator must realise that his actions and investigation techniques should show that there was a constant chain of custody from the time the physical evidence was first discovered until it is presented in court. The accountability procedure is very important and if there is a break in the chain of evidence, the evidence will not be admissible in court (Gilbert, 2010: 92). This chain of evidence includes the correct packaging, labelling, and storage of physical evidence (Monckton-Smith, Adams, Hart & Webb, 2013: 69). According to Osterburg and Ward (2010: 108), the greater the number of people handling the evidence the greater the potential for conflict, contradiction or contamination. The chain of evidence, according to the authors of this article, is also applicable to the presentation of evidence in the form of cellphone records in cellphone investigations. The next section is a critical analysis of the Locard Principle with regard to physical evidence left at a crime scene.

THE LOCARD PRINCIPLE
Doctor Edmund Locard was a scientist who founded the first police forensic science laboratory for the investigation of crime scenes in 1910. During the First World War he gained fame while working for the French Secret Service. He analysed the stains, soil, dust and marks found on the uniforms of soldiers and other prisoners of war to determine their movements during the war. It served as information for counter military decisions and operations (Newburn et al., 2011: 320). Saferstein (2013: 8) considers Edmond Locard as one of the most important contributors to the field of forensic science in that he established a workable crime laboratory already in the beginning of the twentieth century. Saferstein (2013: 8) also points out that Locard’s original work within a criminal investigation milieu focused primarily on microscopic particles that were carried from the crime scene to the criminal including dust and metallic particles. Although Locard’s contribution was later acknowledged as pioneering work in the investigation of crime, he never referred to his own theory in terms of contact and the transfer of traces. The first reference to Locard’s Principle of the exchange of traces was made only in 1940 by Reginald Morrish in an article entitled:
‘The Police and Crime Detection Today’ (Horswell, 2004: 48). Inman and Rudin (2001: 94) mention that the Locard Principle is interpreted in different ways, because the translations of the Locard Principle are done and cited differently. They show, however, that the principle remains applicable in its present form. This statement is confirmed by Yeats (2001: 12). Inman and Rudin (2001: 94), who further argue that if the Locard Principle were invalid, there would be no traces or evidence that could be investigated and offered as evidence.

According to Adams, Cadel and Krutzinger (2000: 3), the Locard Principle is still used today in the investigation of crime scenes and it is because of the implication of this principle that crime scenes are cordoned off to protect the evidence that is left at the crime scene.

CONTACT IN LOCARD’S PRINCIPLE
As stated previously, Locard’s principle is based on the Contact Theory which states that when two objects come into contact with each other, the one will leave a trace on the other (Van Rooyen, 2004: 11). According to Locard’s principle, the reciprocal transfer of traces takes place in two ways. The criminal will leave traces at the scene or will take traces from the scene with him. The two ways of transferring traces are referred to as trace donors and trace recipients (Newburn et al, 2011: 320). Fish, Miller, and Braswell (2012: 110) mentioned that according to Locard, it is impossible for a criminal to perform an action at a scene without leaving behind some traces. Locard also takes the nature and extent of the violence used regarding the number and extent of the traces left behind into account (Chisum and Turvey, 2012: 35). In effect this means that he always takes the degree of physical contact in his analysis of traces into account.

Horswell (2004: 49) explains Locard's principle as follows: "Wherever he steps, whatever he touches, whatever he leaves even unconsciously will serve as silent evidence against him. Not only his fingerprints and his shoeprints but also his hair, the fibre from his clothes, the glass he breaks, the tool market he leaves, the paint he scratches, the blood or semen that he deposits or collects, all prosthesis and more bear mute witness against him". However, Horswell (2004: 50) is one of the first researchers who has scrutinised Locard’s Contact Theory and has explained that no physical contact need to be made to transfer traces. He cites the example of a button that falls off a suspect's shirt without there having been any contact. The trace is, nevertheless, still physically visible.

Robertson (1995: 4) argues that if traces cannot be found where it is presumed that contact was made at a crime scene, it means that there are limitations to the techniques and methods of detection. He further states that technology will make it possible to find traces where no traces could be found in the past (Robertson 1995: 4).

The contact of a cellphone handset with a crime scene can take place in two forms. The first form of contact is when the handset is brought into physical contact with another object at the crime scene and reciprocal transfer of microscopically traces take place. These traces can, for example, be dust that is transferred between the two objects. An analysis of the dust particles can link the handset with the crime scene.

The second form of contact is the electronic data that is transmitted and received by the handset while the handset is at the crime scene. The electronic data is the signal received or transmitted by the handset. The signal is an invisible trace, but can be made visible through a printout of the data of the recording of the signal that is done by the computer system of the cellphone service provider. The location where a handset was used is referred to in cellphone terminology as the location area. The contact of the handset with the crime scene is, in this instance, referred to as the locational position of the handset that overlaps with the location of the crime scene. This type of contact of the handset with the crime scene is referred to by the authors of the article as the positional contact of the handset with the geographical location of
the crime scene. The trace that is left behind can also be described as the positional or location area contact trace.

According to the authors, the proof of the trace evidence in respect of a cellphone that is active at a crime scene lies on the database of the cellphone service provider company. Lochner (2007: 35-43) argues that the signal of a cellphone which is invisible at the crime scene, is electronically recorded and can only be detected in another place than the crime scene.

To understand the concept of the validity of evidence relating to cellphone signals, it is necessary to first discuss cellphone technology in more detail.

**CELLPHONE TECHNOLOGY**

The basic concept of a cellphone dates back as far as 1947, when it was realised that wavelengths that could be re-used (at a distant geographical location) could increase the capacity of cellphone communication through signals significantly (The History of Cell Phones, 2003). A frequency is the wavelength at which signals are transmitted, and signals are moving conversation that ‘transport’ controlled messages between two points (Harte, Prokup & Levine (2001: 44).

A large, powerful signal device with a few wavelengths, which had to cover a large geographical area, was installed in early mobile radio systems – they were known as car phones (Arawal & Zeng, 2006: 17). There were only limited radio channels available to service mobile radios, because each radio channel needed a particular wavelength to operate on (Harte et al., 2001: 15; Schwartz, 2005: 63). To overcome the problem, the number of radio channels were increased by re-using frequencies in different geographical spheres (serviced by different cellphone towers) to create more radio channels. In order to do this, the computer system relied on the handset’s weakening signal strength the further away the user moved from the cellphone tower that relayed the signal. The cellphone tower is, in this way, able to measure the relative distance that the handset is from the tower and to transfer the signal of a handset to an adjacent tower closer to the location of the handset. These towers operate on different wavelengths to prevent overlapping and thus distorting of calls. It is sometimes also possible that the signal is transferred to a tower that is not necessarily nearest to the handset, but to a tower that receives the signal from the handset better. Each of these towers has a limited geographical area that it covers and operates on a specifically assigned radio frequency channel. This allows for towers that are spaced far from each other to use the same channels. The distance that these cellphone towers with the same channels are placed from each other must be big enough to prevent overlapping of the same frequencies, thereby preventing distortions (Harte et al., 2001: 16).

**Practical illustration of the transfer of calls between cellphone towers**

The four domed sketches in the top section of figure 1 indicate the catchment area for the four cellphone towers that are next to each other. Figure 1 shows how the handset's signal weakens as it moves away from a cellphone tower (base station). The solid line in the lower part of figure 1 shows how the handset's signal weakens as it moves to the right, and the dotted line shows how the signal strengthens towards the approaching (new) phone tower. At a point the signal is transferred from the one cellphone tower to the other. This is done while a call is active, or when the handset is on, but there is no communication (Harte et al., 2001: 33). The crux is that the mobile network always registers where the handset is in relation to a cellphone tower. If a handset is moved to a location outside the reception area (cover) of the cellphone service provider’s network, the computer software will register that the handset is out of range. Depending on how the computer is programmed, the service provider's
The database may also be able to record when the signal was lost and which tower was last in contact with the handset.

**Figure 1: Automatic and intentional registration**

![Diagram](source: Harte et al., 2001: 33)

**THE MOBILE SERVICE SWITCHING CENTRE (MSC) AS THE PLACE WHERE TRACES ARE FOUND**

The heart of the cellphone system is the electronic computer-based switching system of which the ‘mobile service switching centre’ (MSC) is the most important (Privateline.com: Digital Wireless Basics Wireless Principles 2004).

The Mobile Service Switching Centre (MCS) is the control centre of a cellphone system. It monitors the location and quality of a handset's signal and switches the handset over between the different cellphone towers and also the public telephone network (PSTN) (Harte et al., 2001: 28). The core of the MSC consists of control devices, switches, communication links and the electronic computer databases of the handsets using the system. The control apparatus of an MSC is the brain of the whole system and manages the MSC processing commands to and from the cellphone towers. The cellphone towers control the handset while the different cellphone towers in an area are controlled by the MCS.

The main computer database in the cellphone system is the ‘Home Location Register’ (HLR) and includes the recorded phone numbers dialled or received by the handset; the handset's phone number; the unique identification number of the handset; the ‘Location Area’ (LA); and the ‘Visitor Location Register’ (VLR) of the handsets using the network (Schiller, 2003: 104). The user database which is also located in the HLR contains the details of the users of the network and also handles the phone bills.

In summary, the MSC performs four important functions:

- It liaises between the cellphone system and the public telephone system (landline).
- It provides overall supervision and control of the mobile communications.
- It authorises the use of the system if the user has a valid account or prepaid account with a positive balance.
- It also controls and provides the accounts. It also keeps track of the system’s users.

Automatic registration of a cellphone as the trail of evidence

Even if a handset is not used to make a call, automatic activation of the cellphone tower is still triggered by a handset that is switched on and moved from one place to another including if moved from one sectoral micro or pico cells of a cellphone tower to another. If the cellphone is moved from the reception area of one cellphone tower to another the movement is recorded on the HLR as movement from the current location (LA) to a new location (VLR). Schwartz (2005: 199) quotes Privateline.com: Cellular Telephone Basics (2004) in describing the automated recording process as ‘registration’ and states it is a continuous process. Marshall (2008: 116) calls it a constant interaction.

During this automatic, continuous interaction the information on the location of the handset is sent to the VLR. The VLR lies in the HLR and because of this automatic, continuous activity and process the system always registers and records the current geographical location of a handset (Schiller, 2003: 113; Marshall, 2008: 115). In practice, the automatic, continuous process is carried out by the cellphone tower that sends a signal to the handset, thus forcing the handset to respond and identify itself. All the information is automatically captured and saved on the computer database of the cellphone service provider.

A practical example to illustrate the continuous communication is when a cellphone is held near a radio or a speaker system and such a device makes a crackling noise. This noise is the audible interference of the radio frequency when the handset and the tower communicate without the mobile network having been deliberately activated and even if the handset is on silent.

During the investigation of the Brett Kebble (Norwood CAS 603/09/2005) case, one of the authors of this article was involved in the analysis of the cellphone technology as an expert. In the investigation it came to the attention of the author that the particular cellphone service provider’s system has the data on the continuous registration of a handset (when the handset is not in use to make a call or to receive or generate a message) on record. This information was, at the time, contrary to the belief among investigators that the data on the continuous registration other than those related to calls or messages were not recorded by cellphone service providers. The data on the continuous registration of the handset is thus available as evidence for as long as the data is not erased or overwritten by the computer software. It is, however, not known how long the cellphone service provider stores the data or categories of data concerning a specific cellphone account.

Schmitz is of the opinion that if the historical data on the automatic (mechanical) continuous registration of a handset is not on record anymore, the cellphone service provider can be requested to store all the data with regard to a specific handset that is under investigation prospectively. The availability and the type of data is obviously determined by what information is already captured as well as the cellphone service provider’s ability and preparedness to program the software that they use to capture or store any additional data (Schmitz, 2013).

Two sets of electronic records can, therefore, be used to place the cellphone in the location of a crime scene. The first record is the cellphone record of calls made or messages generated or received by the handset. Examples of cases where the cellphone records that were used as evidence will be provided in the latter part of the article. The second electronic record that can be used to place the cellphone in the location of the crime scene, is the record generated by the mechanical (automatic) and continuous communication (registration) between the handset and the tower without the cellphone being used to make or receive calls and messages. The data on these two sets of electronic records can respectively be used in geographical mapping to determine the location of the handset at a given time. The use of this data to map the whereabouts of cellphone handsets in an investigation serves as the basis for Lochner's principle.
REGISTRATION OF A CALL AND SHORT TEXT MESSAGE AS PROOF OF A TRACE

Although there are other activities that trigger the registration of a handset on the network, reference is only made to calls received or made and text messages sent or received on the handset. When the network is activated to make a call, to send a short text message or when a call is received, registration takes place on the network computer database just before the network activity is authorised. It takes only a few hundredths of a second for the automatic registration to take place.

When a cellphone call or a short text message sent by a handset is approved, the information about the interaction is stored in the MSC for accounting and inquiry purposes (Schiller, 2003: 104; McCullough, 2004: 25 and Marshall, 2008: 116). In practice this information is made available in the form of an account to customers who have cellphone contracts; or to users who make use of the prepaid facility, at their request. The account contains only the financial aspects pertaining to the use of the network. The information from other handsets that have made calls or sent messages to the handset in question does not appear on the account. However, the cellphone user can request it from the service provider.

In criminal cases, the information (the traces left by the handset on the network) can be obtained by summoning the network service provider in terms of section 205 of the Criminal Procedure Act. In terms of section 205 of the Criminal Procedure Act, a magistrate, may, at the request of the public prosecutor, require any person who may have material or relevant information on any crime to appear before him/her to answer questions regarding the material or information. In practice, the mobile network's representative will hand the information over to the investigating officer after the summons is served.

An incident where the cellphone network was summonsed in terms of section 205 of the Criminal Procedure Act (Act 51 of 1977) to make the record of continuous automatic communication between the handset and the tower other than when the user communicated via a voice or sms on the handset, available to an investigator has not been reported in South Africa yet.

THE EVIDENCE OF TRACES ON A CELLPHONE RECORD

As stated previously, there is a difference between the cellphone record and the cellphone account. The cellphone record is the document that shows the record of the use of a handset. Although there are similarities between a cellphone record and a cellphone account, the biggest difference lies in the fact that the cellphone record also contains information about other users that had interaction with a particular handset. In most cases, an investigating officer will subpoena the cellphone network for the following information:

- the handsets used with the subscriber identity module (SIM) card;
- the type of phone call or text message (received or made);
- the date and time of calls or text messages made or received;
- the duration of the calls; and
- the cellphone tower that handled the calls or text messages when the network was activated. One particular network service provider in South Africa is also able to provide information on the identity of the cellphone tower that was in use when the call was terminated. This is additional information that can assist in mapping movement of the handset between cellphone towers during a call.
Table 1: Example of a cellphone record

<table>
<thead>
<tr>
<th>MSISDN (Own cell phone no.)</th>
<th>IMEI (Handset series no.)</th>
<th>Call date (Date on which network was activated)</th>
<th>Call type (MOC = call made, MTC = call received)</th>
<th>Duration</th>
<th>Other Party (No called)</th>
<th>Cell ID (No of cell phone tower)</th>
<th>Cell name (Name of cell phone tower)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0942382442</td>
<td>65501600062</td>
<td>20-Nov-2010 10: 21: 46</td>
<td>MOC</td>
<td>3</td>
<td>0927223811</td>
<td>3423</td>
<td>Irene</td>
</tr>
<tr>
<td>0942382442</td>
<td>65501600062</td>
<td>20-Nov-2010 11: 01: 03</td>
<td>MTC</td>
<td>34</td>
<td>0923873501</td>
<td>4321</td>
<td>Springs</td>
</tr>
<tr>
<td>0942382442</td>
<td>65501600062</td>
<td>20-Nov-2010 12: 05: 04</td>
<td>MOC</td>
<td>62</td>
<td>0923333678</td>
<td>5320</td>
<td>Moloto</td>
</tr>
</tbody>
</table>

Table 2: Example of a cellphone account*

<table>
<thead>
<tr>
<th>Cell phone number</th>
<th>Account number</th>
<th>Date</th>
<th>Time</th>
<th>Duration</th>
<th>Number phoned</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>0973281441</td>
<td>0973281441</td>
<td>01/09/2012</td>
<td>22: 07: 49</td>
<td>00: 02: 59</td>
<td>27935331015</td>
<td>4.87</td>
</tr>
<tr>
<td></td>
<td></td>
<td>01/09/2012</td>
<td>22: 16: 03</td>
<td>00: 00: 02</td>
<td>27933881731</td>
<td>1.62***</td>
</tr>
<tr>
<td></td>
<td></td>
<td>31/08/2012</td>
<td>09: 59: 32</td>
<td>00: 01: 02</td>
<td>27123749081</td>
<td>2.34</td>
</tr>
</tbody>
</table>

* This is an extract from a real phone account excluding the number called and the account number to preserve anonymity.

In table 2, entry 2 under the heading ‘Vodacom calls to other mobile networks’, on 01/09/2012 at 22: 16: 03, the very short duration registered for the handset activity, indicate that there was no established connection. This entry serves as proof that a trace can be left without a connection been established during a call.

THE LOCHNER PRINCIPLE

The Lochner Principle premises on the electronic record that is kept at a sight away from the geographical location where a handset was at a particular point in time. In the instance of a cellphone call, a short message service (sms) or automatic (mechanical) continuous registration of a handset, the contact is made between the handset and the location of the crime scene and the invisible signal is momentarily present at the scene. The contact is, however, registered (captured) in the memory of the MCS (which is not the crime scene) of the cellphone system. The cellphone record or other printout of the data on the server in
practise serves as proof of the contact. The data given on a cellphone record or other printout is converted into a visual display by mapping. Lochner describes that the record of the contact between the handset and location area (or crime scene) can be used successfully in a criminal investigation in that it maps out the contact between handsets, timelines of calls or messages made or received, and location of handsets at a particular time and so forth. This prompted Lochner to register the Lochner Principle (2006/00362) and (2006: 00367) as a trademark in 2006 in terms of section 29(2) of the Trade Marks Act of 1993. The Lochner Principle is defined as follows: "in order to reveal invisible technological traces left at a crime scene by mapping them through telecommunication techniques and to render on a scientifically and technological basis a technological service to examine a crime scene with the aim of making the invisible trace visible."

This principle is supplementary to that which Locard propounded in his Contact Theory. The technological footprints referred to by Lochner are not only the traces left behind as a result of a call being made. They also include the traces left off site by the automatic, continuous registration of a handset without there having been a call or text message made, or physical contact between two objects. Marshall's (2008: 9) statement support Lochner, by stating that a handset does not need to be actively used, but its mere presence at the scene can prove that it was there. If it is argued strictly in accordance with the Contact Theory (of traces at a crime scene left behind only by means of physical contact), the insight of researchers on the transfer of traces will be reduced, although this was surely not the purpose of the Locard Principle (Horswell, 2004: 50).

The Locard and Lochner principles are scientific principles and not scientific theories. Both can, however, be tested scientifically and legally. Both principles will also allow researchers and investigators to contemplate more aspects of the contact and invisible traces as well as evidence that can be found on a remote computer database with regard to the transfer of traces.

COMPARISON AND APPLICATION OF THE LOCHNER AND LOCARD PRINCIPLES ON THE BASIS OF PRACTICAL EXAMPLES

The purpose of this comparison and discussion is neither to examine the investigative methods applied by the investigators concerned nor to judge them. It is merely to show how Locard's principle is still applicable, and how Lochner's principle could have been applied as an addition.

Exemplar case 1:
In the Inge Lotz case (Cloetesville CAS 92/03/2005) where the deceased's boyfriend was tried for her murder, traces in the form of a fingerprint, a shoe print and an indentation in the deceased's skull were left behind. The accused was acquitted and the guilty party has not been identified.

Exemplar case 2:
In the well-known case of the Brett Kebble murder, traces including bullet shell casings, projectiles, and residue were left behind at the crime scene (Norwood CAS 603/09/2005). The location of the physical evidence was used to determine the exact place where the shooting took place.

Exemplar case 3:
The role that cellphone evidence will play in the Oscar Pistorius (Boschkop CAS 110/02/2013) inquiry was highlighted when the magistrate who heard the bail application asked the investigating officer about the record of the handsets that had been found at the scene of incident. In the Pistorius case, traces in the form of bullet shell casings, projectiles and blood were left behind in terms of Locard's principle.
In the first two exemplar cases the record of all the handsets that were at the locational area that overlaps with the crime scene could have helped to identify the murderer by a process of elimination. A process of elimination is when the cellphone records are obtained from the cellphone service providers of all handsets that were at the locational area that overlaps with the crime scene; at the time of the crime and the alibi of each affected cellphone owner is followed-up to try and identify possible suspects. Through this process of elimination it would, for example, be possible to identify a specific handset that was at all of the crime scenes if there were a series of related incidence of crime. The important factor is that during the process of elimination the private messages of the owners of all of these handsets will not be intercepted or accessed, but the intention is to identify possible suspects that were at the locational area of the crime scene at the time of the crime. In the same process it is possible to also identify witnesses who might have been in the vicinity of the crime scene at the time of the crime. This would be a similar elimination process as to the screening of Closed Circuit Television CCTV camera footage of all patrons at a shopping mall to identify suspects if a robbery occurred at the shopping mall.

In addition, by applying the Lochner Principle, it is also possible to determine the location and timeline for activities registered with regard to the handsets found at the scene of incident. This aspect would have been a valuable tool in the Oscar Pistorius trial to have supported or refuted the sequence of events as described by the defendant.

Lochner's principle may also be applied once a suspect has been identified through other means, and the mapping of the activities of the cellphone of the suspect can either place an accused in the vicinity of the scene of the crime, or it can confirm or refute the accused’s alibi that he/she was elsewhere at the time of the commission of the crime.

**CONCLUSION**

Robertson (1995: 202) concluded that when evidence is brought before the courts, only those methods which have been published, tested and accepted are used. The courts will always be sceptical about the validity of new techniques. This article demonstrates that modern criminal investigation with regard to cellphone technology is a developing field that requires new detection techniques to detect traces left by a cellphone. It also demonstrates that both the Locard- and Lochner- principles provide guidelines with regard to where traces left by cellphones can be found. The article also explores the use of cellphone data that is automatically generated by the cellphone on the computer server other than when a call or text messages is made and can be used as additional data to determine the location of a cellphone at a crime scene. This information can be used in a criminal investigation as evidence to place a suspect at the crime scene location at the time of the crime. However, there is currently no evidence that the Lochner Principle with regard to data on the automatic (mechanical) continuous registration of a handset other than when the handset was used for communication has per se been tested or implemented in recent criminal investigation cases or that it will be utilised in South Africa in the near future.

Experts and authoritative persons with cellphone and legal backgrounds who are prepared to do further research on this, will help to develop and apply the potential benefit of these principles to enable courts to more readily accept the information discovered due to these techniques as evidence.
LIST OF REFERENCES
The history of cell phones. [s.a]. Available at: http://cseserv.engr.scu.edu/studentwebpages/jVillovos/history.htm/ (accessed 20 August 2013).


Decided cases
Boschkop CAS 110/02/2013
Cloetesville CAS 92/03/2005
Ex Parte Rosch 1998 I All SA 319 (W) 321
Mashiyi 2002 (2) SACR 387 (Tk) 393d-e
Mdlongwa 2010 (2) SACR 419 (SCA)
Ndlovu v Minister of Correctional Services [2006] 4 All 165 (W) 173f-g
Norwood CAS 603/09/2005
S V Dos Santos 2010 (2) SACR 382 (SCA)
S v Ndiki 2008 (2) SACR 252 (Ck) 264h-265ª
Seapoint CAS 141/06/2009

ENDNOTES
1. The case served before court and the case docket reference number and details of the case are a matter of public record.
2. The case served before court and the case docket reference number and details of the case are a matter of public record.
3. The case served before court and the case docket reference number and details of the case are a matter of public record.
4. The Oscar Pistorius case, at the time of writing of the article, had not yet been adjudicated and no inference should be drawn from the article that Mr Pistorius was involved in committing a crime. The case is before court and the case docket reference number and details of the case will become a matter of public record at a later stage.