Investigating Modern Communication Technologies: The effect of Internet-based Communication Technologies on the Investigation Process

Matthew Simon
University of South Australia
Mawson Lakes Boulevard
Mawson Lakes, SA, 5095
+61 8 8302 5688
matthew.simon@unisa.edu.au

Jill Slay
University of South Australia
Mawson Lakes Boulevard
Mawson Lakes, SA, 5095
+61 8 8302 25757
jill.slay@unisa.edu.au

ABSTRACT

Communication technologies are commonplace in modern society. For many years there were only a handful of communication technologies provided by large companies, namely the Public Switched Telephone Network (PSTN) and mobile telephony; these can be referred to as *traditional communication technologies*. Over the lifetime of traditional communication technologies has been little technological evolution and as such, law enforcement developed sound methods for investigating targets using them. With the advent of communication technologies that use the Internet – I*nternet-based* or *contemporary communication technologies* – law enforcement are faced with many challenges. This paper discusses these challenges and their potential impact. It first looks at what defines the two technologies then explores the laws and methods used for their investigation. It then looks at the issues of applying the current methodologies to the newer and fundamentally different technology. The paper concludes that law enforcement will be required to update their methods in order to remain effective against the current technology trends.

Keywords: digital forensics, digital investigation, communication technologies, telecommunications interception, post mortem analysis

1. INTRODUCTION

"*when I was your age,*
the phone was tied to the wall with a kinky, twisty three and a half foot cord,
it's hard to believe but it had a ring that could not be turned off or ignored,
we couldn't choose the sound of the ring, it was just the sound we called 'the phone',
we'd never heard of a ring tone"[1]

Digital communication technologies are fundamental to modern society and form a worldwide network allowing people to communicate efficiently. Traditionally, there have been relatively few distinct communication technologies. PSTN and Mobile Phones have dominated the communications landscape forming a single conceptual network. These technologies can be thought of as *traditional communication technology*. Traditional communication networks have changed very little over their extensive lifespan. With the recent widespread adoption of the Internet, novel communication technologies are increasingly available. In contrast to traditional communication technologies these can be referred to as *contemporary* or *Internet-based communication technologies*. There are many advantages to using Internet-based communication technologies and these have been realised by both users and providers of services. However, such advantages are one side of the proverbial "*double edged sword"* and may be disadvantageous within other contexts. This is particularly relevant to law enforcement as contemporary communication technologies present significant challenges to the ability to gain evidence and intelligence about their use in an investigation.

It is common for law enforcement agencies to conduct investigations as part of their duties. Recovering information about targets can be performed in many ways. Investigation methodologies may be thought of as a series of methods and procedures to recover information in a given context. Investigation methodologies for recovering information about a target's communications are commonly employed by law enforcement. Traditional communication technologies have been in use for many years and have changed very little over this time. This has allowed the development of highly effective and rigorous investigation methodologies for these technologies. Internet-based communication technologies by contrast are very different. Their technological operation is based on a fundamentally different paradigm; this leads to several fundamental functional differences. Due to these inherent differences, the existing methodologies used by law enforcement may not be adequate for situations involving contemporary communication technologies and this is a significant problem as they are becoming more prevalent.

In order to understand how the shift in technology affects investigation methodologies of law enforcement it necessary to understand the differences between the technologies. It is rudimentary to identify the primary technological difference however, it is necessary to delve deeper in order to find the issues that

[1] George Hrab, "When I was Your Age". Geologic Records, 2010

affect the investigation methodologies. An understanding of the underpinnings of all communication technologies is needed before exploring the specifics of both types individually. All technologies use the concept of '*services'* to designate functions of the various parts of the system. An understanding of what these services are and do is necessary in order to understand holistically how communication systems operate. The concept of services is also tied closely to the legislation that affects communication technologies in Australia. By exploring the background and operation of traditional and contemporary communication technologies, certain properties of the latter can be identified that are contrary to the former. These properties embody functional differences, which can be used to explore in a practical manner where the weaknesses in the current methodologies are.

The methodologies for investigation of communication technologies are comprised of three main methods: *communications interception*, *access of retained information* and *post-mortem analysis*. Each of these uses different vectors of access and gain different types of information; the situation context will dictate which should be used. These methods are well suited to the investigation of traditional communication technologies and it is a combination of many factors that contributes to their success. However, these methods may not be successful in many situations where contemporary communication technologies are being used. The reasons for this can be explored by looking at the application of the methods to traditional communication technologies and contrasting this with the known functional differences identified by comparing the technologies. This shows what properties of contemporary communication technologies are responsible for the ineffectiveness of the methods. The practical implications of the mismatch in methods can be further explored with a case study. Three separate incidences are presented that describe situations of criminal activity and how law enforcement used one of the investigation methods to gain information that was subsequently used as evidence in a court of law. A hypothetical alternative is then presented for each case to demonstrate how the methods used may have failed where the target used an Internet-based communication technology.

This paper seeks to show how the shifting paradigm of communications is changing the requirements for law enforcement. It is important that they are able to carry out their role effectively in order to prevent or stop criminal activity. Knowing the failings of the current methodologies may help the development of new methodologies for the current environment. This paper provides a first step for carrying out future research in this direction.

2. COMMUNICATION TECHNOLOGIES

Traditional and contemporary communication technologies are tools that support human-to-human communication. The ways in which they operate to fulfil this task however is very different. Common to all types of technology is the concept of services. A holistic communication service is itself comprised of multiple

services. These form a hierarchy, with the conceptually lower service layers supporting the conceptually higher service layers. While any number of service layers can be employed, any holistic communication services can be conceptualised as being formed by two: the *carrier* and *carriage* service. The definitions of carrier service and carriage services depend on the context. A specific definition exists as defined by relevant legislation and a generic definition exists (defined here) that is more useful in the discussion of communication technologies in general. Understanding the structure of services is necessary in order to understand the operation of both traditional and contemporary communication technologies.

A cursory study of traditional and contemporary communication technology is sufficient to define their fundamental differences. However, the high-level fundamental difference is not the issue central to the ineffectiveness of law enforcement methods for recovering information about contemporary communication technologies. To discover the *functional* differences between the two types of technologies, it is necessary to explore the background and operation of both. A comparison can then be made that explores the operational differences. As the goal of the paper is to explore why existing methods are not equally effective for contemporary communication technologies, it is necessary to identify the properties of this type of technology that cause the functional differences.

This section looks at communication services as a background to the analysis operation of both contemporary and traditional communication technologies. After exploring both technologies, an in-depth analysis of the differences is conducted to identify the functional differences; these are defined as a set of properties of contemporary communication technologies.

2.1 Communication Services

In order to understand both traditional and contemporary communication systems, it is necessary to understand how multiple services are used and constructed overall to deliver a service to the customer. This is fundamental to the operation of all communication systems. As telecommunications in Australia are predominantly regulated under the *Telecommunications Act 1997* (Cth) (Telecommunications Act), it is also prudent to review the relevant definitions that the Act specifies. In order to maintain consistency, the following concepts are explored in terminology consistent with that used in the Telecommunications Act. This terminology is also consistent with related legislation such as the Telecommunications (Interception and Access) Act of 2001 (TIA Act).

Under the *Telecommunications Act 1997* (Cth) there are two entities that provide two different services: *carriers* and *carriage service providers* (CSP). A carrier is a body that provides infrastructure (either physical or wireless) in order to carry signals between points (with one point is within Australia); such infrastructure forms part of the Australian Telecommunication Network (ATN). The role of a carrier is to supply a *carrier service*. This term is not specifically defined within

the Telecommunications Act but is convenient for describing the service provided by a carrier and is therefore used frequently herein. A carrier service provides a means of moving indiscriminate signals between two distinct points. The Australian telecommunications company Telstra operates as a carrier by maintaining a copper cable network. A CSP is an entity that supplies communication services using a carrier's infrastructure. The service supplied by a CSP is called the *carriage service*. A carriage service is defined in the Telecommunications Act as "*a service for carrying communications*". Telstra also operate as a CSP by supplying PSTN services to residential households. Many other companies in Australia also operate as CSPs by selling PSTN services to residential households over Telstra's copper cable infrastructure.

In any communication system, multiple service layers are employed. In the PSTN, the carrier service is the copper cable that is supplied to a location (such a residence). A telephone or another carriage service is then supplied on top of the carrier service. The supply of an Internet connection also has multilayer service architecture. In the case of an Asynchronous Digital Subscriber Line (ADSL), the copper line is again the carrier service. An alternative carrier service for an Internet feed is a coaxial cable or one of many wireless options. An Internet service provider then supplies, over the carrier service, the Internet feed and this is a carriage service.

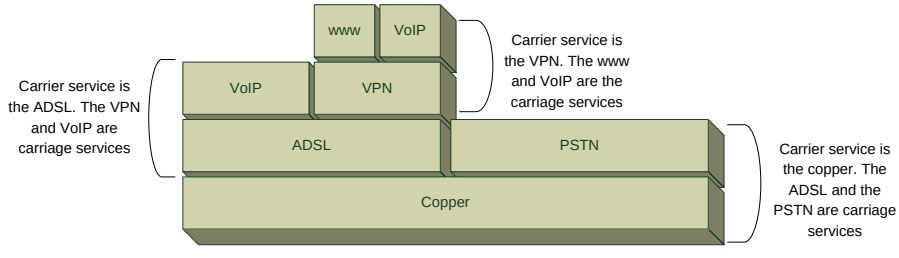

Figure 1: An example of a network hierarchy and a description of the carrier/carriage service layers.

The definition of carrier and CSP based on the Telecommunications Act is very specific and is too restrictive when discussing communication systems more broadly. In general, the important factor is the relationship between the services. To this end, a carrier and carriage service will be used to define any pair of communication services where one 'carries' the other. Internet communications are a pertinent example of where this definition is more flexible. Figure 1 depicts an example network hierarchy and indicates how the layers relate to each other. In this example, the copper/PSTN and copper/ADSL have a carrier/carriage service structure as defined under the Telecommunications Act. Based on the more general definition as specified here, the ADSL/VoIP and ADSL/VPN have a carrier/carriage service structure. Moving one layer higher the VPN becomes the carrier over which a WWW and VoIP service is carried.

This definition of carrier and carriage service will be used unless specifically stated. Where referring to service providers in relation to the Telecommunications Act specifically, the terms TA-carrier, TA-CSP, non TA-carrier and non TA-SCP will be used. The distinction is important when discussing legislation, for instance under the Telecommunications Act an ADSL connection is not seen as a carrier service and consequently is not lawfully bound as such. Additionally, if the VoIP service is not classified as a carriage service, it is not legally bound by the Telecommunications Act or the TIA Act.

All communication technologies, whether traditional or contemporary, are generally comprised of two main services, the carrier and the carriage service. The exact meaning of these depends on whether the specific (that defined under the Telecommunications Act) or the generic definition is being used. Understanding what the services are and how they are combined to supply a complete communication service is important in understand the operation of both traditional and contemporary technologies, and furthermore to gain an appreciation for how they differ at a functional level.

2.2 Traditional Communication Technologies

Traditional communication technologies are telephony implementations that have existed for many years. This name 'traditional' is an accurate designation as this type of telephony technology has been well established in society and for the greater part of its existence, has been the sole implementation. The traditional telephone began its existence in 1876 when Alexander Graham Bell famously said, "*Mr. Watson--Come here--I want to see you*" to his assistant in the next room over an early telephone prototype. At this stage, the telephone was merely a shadow of what it would become. For well over 100 years, telephony technology has developed and integrated into all facets of society. In 2004, there were over two hundred million PSTN telephones in use in the United States alone (Wallingford, 2005). While the PSTN is based on a physical cable, mobile telephony was developed in the late 20th century allowing users to keep their telephony service with them at all times. There are several common technologies on which mobile telephony is implemented including the very common Global System for Mobile Communication (GSM, from the original name, *Groupe Speciale Mobile*), 2.5G, CDMA, 3G and 4G. All of these technologies are different in specification but operate on the same basic principal and are fundamentally the same to the user. As such, all of these implementations can be referred to in a generic sense simply as '*mobile telephony*'.

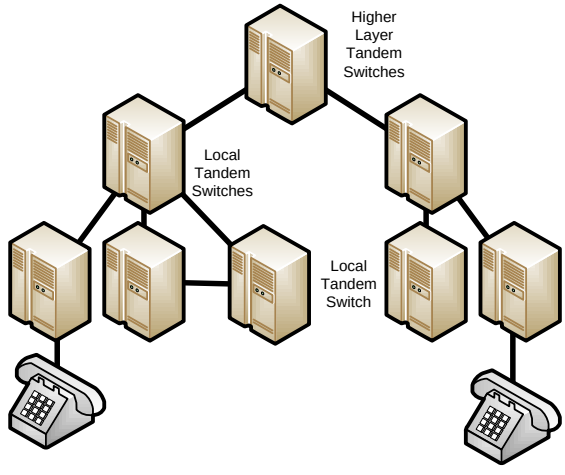

Figure 2: Simple Overview of the PSTN. Based on diagram from Davidson et al. (2007)

Traditional communication technologies operate using a style of network called a circuit switched network; this operational paradigm has not changed significantly since its widespread adoption. The circuit switched network paradigm is based on a fixed bandwidth connection between two endpoints (Davidson, Paters, Bhatia, Kalidinidi & Mukherjee, 2007). While major revolutions have occurred in telephony technology like the invention of automatic switches, the conversion from analogue to digital signalling and the invention of mobile telephony, the underlying architecture has always been a circuit switched network.

In a circuit switched network, connections are made between endpoints by physically connecting a series of cables to form a single circuit. Early incarnations of the PSTN were based on a mesh network where all endpoints were connected to every other endpoint, creating a mesh of connections. The concept of a mesh network is intractable for more than a small number of endpoints (Wallingford, 2005). To allow for an arbitrary number of endpoints in a scalable manner, switches are used to switch one endpoint's connection to any other endpoint. The role of switches in a circuit switched network is to physically connect and disconnect cables in order to establish a circuit between the two endpoints. The circuit need only exist for the duration of a call; in this way, less physical infrastructure is required for a greater number of endpoints. The first manual switch came into operation in 1878 where a person would physically connect different circuits together. The automatic switch was invented in 1891 negating the need for a human operator in favour of an electronic signalling system (Dryburgh & Hewett, 2005). In a modern setup, the PSTN contains a hierarchy of switches. At the lowest level in the hierarchy each endpoint connects to an office exchange switch. A series of office exchanges will in turn connect to a tandem

switch which will then connect to a higher level switch (Davidson et al., 2007) Figure 2 depicts a typical version of a PSTN network. When a circuit is established between two endpoints, it only needs to be routed as high as necessary in the network. Additionally, physical infrastructure may be installed between office exchanges where traffic volume is sufficient. This allows traffic flows to be localised and negates the need for large volumes of traffic to be routed through the higher level switches (Davidson et al., 2007).

From early implementations of manual switches and analogue signals, the PSTN has developed into a monolithic and highly complex digital network where switching is performed automatically (Davidson et al., 2007; Sicker & Lookabaugh, 2004). Much of the complexity of the network is due to the myriad of services that are available such as voice mail, call waiting and automatic callback. As the endpoints in the network have no processing capability, the core of the network is responsible for implementing all of the service logic.

In supporting all of the functions required of traditional communication systems, the various components of the network must communicate with each other in order to appropriately carry out their required functions. When manual switching was in use, the initiator of the call signaled to the operator using a hand crank that would light a bulb on the operator's desk. The operator would then talk to the calling party to find out where the call was to be routed and would subsequently perform the required actions (Dryburgh & Hewett, 2005). By talking to each other the users of the system could setup the network to fulfill the primary goal i.e. makes a telephone call to another endpoint. Automatic switching fulfills the same goals without human intervention and uses a signaling protocol to do this. The PSTN uses a signaling system called Signaling System Number 7 (SS7), mobile telephony commonly uses an extended version of SS7 (Dryburgh & Hewett, 2005). Signaling within the core of the network is possible as the core systems are all intelligent. Signaling between the core and the endpoints within the PSTN is not possible, as the endpoints do not have the capability to process such signals. Mobile telephony has had much more scope to evolve as the endpoints have processing and storage capability.

2.3 Contemporary Communication Technologies

Contemporary communication technologies are those that use the Internet to transfer data between endpoints. This designation is appropriate as they are the revolutionary form of the long existing traditional communication technologies. The Internet is a packet switched network that is fundamentally different to that of the circuit switched networks used by traditional communication technologies. While circuit switched networks are inherently based on the concept of a connection that exists between two end-points, the Internet has no such conception (Black, 2002). In a circuit switched network, a connection that is created is leased for a period of time and for that duration the allocated bandwidth is wholly dedicated to that connection regardless of how much is actually being

used. In a packet switched network, only bandwidth that is required for transmitting the message content is used.

Like traditional communication networks, packet switched networks also are comprised of interconnected switches. However, the switches do not connect circuits; they are simply responsible for receiving and then 'forwarding' discreet 'chunks' of data called packets. Instead of a dedicated, fixed bandwidth connection between the endpoints, the packets are sent through the network, from switch to switch, getting closer to the destination with each step. This is analogous to the postal service where physical cables are akin to haulage routes, switches to post offices (or a postal distribution centre) and packets to letters. When a letter is sent over the postal network, there is no 'connection' between the sender and receiver. The letter/packet is forwarded through the network to a post office/switch that is closer to its destination with each step. In this way, an end-point can send data to multiple discreet endpoints at the same time without using additional infrastructure. Similarly, an endpoint can receive data from multiple discreet endpoints simultaneously. However, unlike a circuit switched network, the Internet cannot guarantee delivery of data, the network makes the "best effort" it can to deliver the payload (Black, 2002). The basic functionality of the Internet is largely useless on its own. To increase its utility, a range of protocols is used on top of the basic structure. This is the same concept of layered services discussed in section 0, but used in a different context. Such protocols at the lower level are used for sending messages that span over a range of packets (sequencing), guaranteeing delivery and allowing for multiple discreet message streams. At the higher level, there are many protocols for implementing application specific functions such as the World Wide Web.

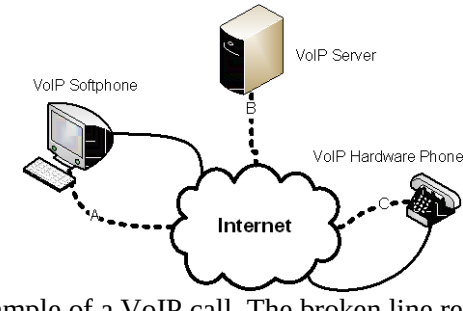

Figure 3: An example of a VoIP call. The broken line represents signaling sent to setup the call. The unbroken line represents the media (content) that is sent between the VoIP network endpoints.

So far, the discussion of contemporary communication technologies has focused on the underlying network and little on the communication service aspect. The discussion of the carriage service aspect is separate from the carrier aspect as the two parts are quite distinct. The Internet is not designed to carry any particular type of data and human-to-human communications is only one use.

Communication services are implemented with protocols that are carried by the Internet. These higher-level protocols are generally developed for a specific purpose such as VoIP or Instant Messaging. A communication system is comprised of one or more protocols sent between one or more endpoints to fulfill the function of communication. The endpoints can be any device that understand the required protocols; both software and hardware endpoints are common. An example of such a system is a VoIP phone network. If a call is placed between two VoIP network endpoints, several protocols may be used for call management (e.g. setup and teardown) and for transferring the content. The VoIP endpoints may be a hardware phone and a software application both of which 'understand' the required protocols. Figure 3 shows an example of a VoIP network. The solid and dotted lines indicate different protocols used in the network.

As with traditional communication networks, signaling does occur within a packet switched network however the purpose is very different. The switches in packet switched networks need to be able to forward packets closer their destination. They generally have many physical connections to other switches in the network and must be able to decide where to forward each packet. Routing protocols are used to build information stores about a network that is used to make packet-forwarding decisions. The signaling within the network has nothing specifically to do with the communication technologies (or any other technologies) using the network.

2.4 Traditional vs Contemporary Communication Technologies

The exploration of the operation of traditional and contemporary communication technologies in the previous sections results in a clear distinction of the major fundamental difference, namely the types of networks over which they operate. The functional difference between the technologies however, is deeper than just the underlying network operation. At the lowest level, the physical infrastructure of a packet switched network is similar to that of a circuit switched network in that there is a network of cables connected together with switches; it is how the networks are used that has the significant impact on communication technologies.

Circuit switched networks as a concept has been in place for a long time. The original PSTN system contained no logic besides that of the human beings in within the network. When automatic switching was introduced, the intelligent humans were replaced with intelligent machines to fulfill the same role. A highly simplistic signaling system was added to the endpoints to replace the dialogue with the operator. Through the development of traditional communication technologies, the complexity of the core systems has grown while the endpoints have evolved little. In supporting the functions for which it was designed – the provision of voice communication – traditional communication networks perform adequately. However, the provision of new function and features is difficult due to the limited endpoints.

The Internet as a packet switched network was not built for a particular high-level

function. Its role is generic, centered on carrying packets of data between endpoints. In this way, the Internet is a generic data transfer medium. Traditional communication systems are limited by the complexity of the core systems, the simplicity of the endpoints and the limited signaling ability between. Systems built on the Internet do not have this problem as there is no limitation to what the Internet can carry between the endpoints. This difference can be described as the *logic shift property*. The provision of communication services over any network requires intelligent components that are responsible for implementing the application logic. In traditional communication systems such as the PSTN, all of the logic is comprised in the complex and intelligent core while the endpoints are "quite stupid" (Cherry, 2005). When additional functionality is added to the PSTN system (e.g. call waiting), the core systems' logic needs to be reprogrammed, however functionality cannot be added to the simple endpoint. In contrast to the logic-centric traditional communication networks, the Internet has relatively simple core systems (although are by no means 'stupid') and complex endpoints. The logic in contemporary communication systems is at the 'outside' of the network. Contemporary communication technologies use the Internet but are independent from it. Changing or updating the communication services has no effect on the underlying network. Another way to look at the logic shift property is that all of the logic of the system is comprised within the carriage service where in traditional communication technologies, the logic resides in both the carriage and the carrier service.

The independence of the carriage service from the carrier service in contemporary communication technologies, caused by the logic shift property, can be defined as the *service decoupling property*. In traditional communication services, the carrier and carriage services are tightly coupled. The telecommunications provider generally controls both and conceptually supplies them as a single service; this is a product of the logic centric network. In both PSTN and mobile telephone systems, the user cannot choose to use their carriage service over a different carrier service independently of the providers. In contemporary communication systems however, the two service layers are independent. Internet-based communication technologies are functionally separate from the underlying carrier service and therefore can easily be 'moved' when required. In general[2], the user is able to use their carriage service over any available carrier service and a carrier service may carry any carriage service.

The logic shift property also propagates a number of other significant differences between traditional and contemporary technologies. As the endpoints are complex devices and are responsible for some of the functionality of the network, users

[2] It is possible that the carriage and carrier service can be bound in contemporary communication services. For instance, a VoIP phone may derive its service number from the physical port to which it is connected. However, this is an artificial constrained added by the communication provider.

may be able to influence how the endpoint functions. In traditional communication technologies, the user has little control over the endpoint, as there is little that can be configured. This difference can be referred to as the *endpoint control property* and may give users greater control over a contemporary communication network than what they might have in traditional networks. Another significant change is the ability for entities to supply communication services. Traditional communication systems are extremely complex and require expensive hardware and software. For this reason, traditional telecommunication services are generally supplied by companies to consumers as a business. Providers of contemporary communication services however, need not invest in expensive hardware or software. This difference can be defined as the *lower barrier to entry property*. An issue related to this is the ability for providers of contemporary communication services to distribute their service globally; this is referred to as the *borderless supply property*. Providers do not need to have any physical presence in locations where their product is used, nor do they need to have physical infrastructure. This is very different to providers of traditional communication services who generally require both physical infrastructure and presence in localities where they distribute their product.

The legislation that relates to communication services is another notable difference between traditional and contemporary communication technologies. All traditional communication services are comprised of carrier and carriage service providers as defined under the Telecommunications Act. In Australia, only certain types of Internet-based communication services are deemed CSPs under the Telecommunications Act. Non TA-CSPs do not have any obligations under the Telecommunications Act or the TIA Act. Regulation of communication networks is overseen by the Australian Communications and Media Authority (ACMA). With the rise in popularity of contemporary communication services, ACMA has taken steps to ensure that where contemporary communication technologies are supplied as replacement to traditional communication systems, they are classified as TA-CSPs. ACMA has defined four classifications of VoIP:

1. Peer to peer – Internet only, calls do not use the traditional telephone network, the public switched telephone network (PSTN)
2. VoIP Out – a service where calls can be made from the VoIP network to the PSTN
3. VoIP In – a service which allow calls to be made from the PSTN to the VoIP service using a telephone number
4. Two way – a service which allows calls to be made both ways between the VoIP service and the PSTN using telephone numbers (Australian Communications and Media Authority, 2010b).

The ACMA web site states that all categories with the exception of the peer-to-peer category are "*generally*" classified as carriage services (It is unclear exactly what is meant by "generally" as no distinction is made in any of the relevant legislation) (Australian Communications and Media Authority, 2010b). Where a contemporary communication service is deemed by ACMA as a carriage service, the provider has the same obligations as traditional CSPs. Where the service falls outside of this classification, it can also be regarded as an *Internet application.* This difference between traditional and contemporary communication technologies can be designated as the *Internet application property*.

The Internet as a carrier service allows communication systems that operate and behave very differently from traditional systems. At an implementation level, the primary difference is the style of network; traditional communication systems use a circuit switched network where contemporary communication systems use the Internet, which is a packet switched network. The Internet does not have one particular function; it is generic in its nature. For this reason, the intelligent parts in contemporary communication systems reside at the endpoints of the network; this is the logic shift property. The logic shift property is important to understand as it gives rise to another four properties of contemporary communication networks: the service decoupling property, the endpoint control property, the lower barrier to entry property and the borderless supply property. These properties of contemporary communication technologies are important they are responsible for the differences in the two types of technology on a functional level. This paper explores the investigation methods used by law enforcement and the defined functional differences hold the key to the utility and effectiveness of the methods.

3. INVESTIGATION OF COMMUNICATIONS

This section deals with the way that communication technology is investigated. It first looks at the range of methods that law enforcement currently uses for obtaining information and at the techniques used for discovering what services a target is using, or who is using a given target. It then looks at the three primary methods for obtaining data about a target's use of communication technologies: communication interception, access of stored information and post-mortem analysis. Section 0 explores how the methods are currently applied to traditional communication technologies. It further looks at the application of the methods to contemporary communication technologies. The contemporary communication properties identified in 0 are used to identify where the incompatibilities lie. Finally, a case study shows examples of the application of communications interception, access of stored information and post mortem analysis where used by law enforcement. The case study further provides a hypothetical situation in each instance that seeks to explore the impact on the outcomes where targets used Internet-based communication technologies.

3.1 Lawfully Obtaining Information

In law enforcement investigations, it is common that a target's use of communication services should be explored. Information about the use of a telecommunication service can be one of two types, the content of the actual communication or data about content; the latter is called metadata. In both cases this data can be obtained from two sources, the core systems of the communication system or from the target if the data is in their possession (generally residing on the endpoint device). In Australia a person's right for their data to remain private is covered under various acts of legislation with the *Privacy Act 1988* (Cth) (Privacy Act) chief among these. The location of the data, within either the network or the endpoint, dictates the affecting laws under which the data can be recovered. When data are in the possession of the owner, the rights of that person concerning the data are the same as with anything, material or otherwise, that is owned by that person. Items owned by a person cannot simply be acquired without their permission or lawful request (search and seizure). When data are in the possession of the owner, it is irrelevant (in relation to legislation) whether the data are content or metadata; the law is applied equally to both. However, when data are obtained from within the Australian Telecommunications Network (ATN) (the infrastructure owned by the listed TA-carriers), there are three acts of legislation that govern a user's right to privacy, the TIA Act, the Privacy Act of 1988 and the Telecommunications Act. The TIA Act covers the interception and access of the content of communications as they pass over the ATN. The Telecommunications Act and the Privacy Act cover the privacy of a user's personal information, which includes their personal particulars and communication metadata.

3.1.1 Communication Interception

Access to communication content while it resides within the ATN is governed by the TIA Act. The TIA Act defines this type of data as a "communication" and is defined as follows:

> communication includes conversation and a message, and any part of a conversation or message, whether:
>
> (a) in the form of:
> (i) speech, music or other sounds;
> (ii) data;
> (iii) text;
> (iv) visual images, whether or not animated; or
> (v) signals; or
> (b) in any other form or in any combination of forms
> (*Telecommunications (Interception and Access) Act* 1979).

Stored communications that reside on the ATN are also specifically accounted for under the TIA Act. A stored communication is one that is in transit between endpoints but is temporarily stored within the network. An example of a stored communication in this context is an SMS message that has not yet been transferred to the recipient's mobile phone. Prior to the *Telecommunications (Interception) Amendment Act 2006* (Cth), such communications were not considered as '*in transit*'. Stored communications then fell under the Telecommunications Act as retained data allowing easier access by law enforcement (Electronic Frontiers Australia, 2006b).

Intercepting communications en-route over the ATN is illegal. In order for law enforcement to lawfully to do this, the TIA Act provides exemptions. The TIA Act contains a warrant regime in Chapter 2 Part 2-5 and Chapter 3, the latter relating specifically to stored communications (*Telecommunications (Interception and Access) Act* 1979). Warrants for interception of communication content can be issued by authorised eligible authorities. Such authorities, nominated by the Attorney General, may be judges or members of the Administrative Appeals Tribunal (AAT) (Electronic Frontiers Australia, 2006c). Warrants for interception of communication can only be authorised for crimes that are considered "serious". Serious crimes are explicitly defined in section 5D of the TIA Act. In protecting the privacy of users of telecommunication systems, the TIA Act also specifies a range of issues of which the issuer of the warrant must be satisfied before providing authorisation. The authorising judge or AAT member must consider matters such as "*how much the privacy of any person or persons would be likely to be interfered*" and "*the gravity of the conduct constituting the offence* [that is being investigated]" (Electronic Frontiers Australia, 2006c).

The content of a communication may be considered the '*holy grail*' of information when investigating a target however the protection law surrounding access to this information is very clear. In comparison to retained data (discussed in 0), gaining lawful access to content data is much more difficult. Where clear need is established and proper judicial requirements are fulfilled, law enforcement can gain much information about targets and their activities. For this reason, this information gathering method is very powerful and an invaluable asset.

3.1.2 Access of Stored Information

In obtaining data from within the telecommunications network, law enforcement may collect a user's particulars or information about a user's activity that has been stored by the provider. Telecommunication providers collect various types of information about users and their activity. Depending on jurisdiction, data may be collected for business purposes of the provider (e.g. billing) or legislation may force the collection and retention of such data. In the latter case, such legislation may be consumer focussed for such requirements as itemised billing or for national security purposes. In 2006, the European Union (EU) adopted a directive that specifies policy for retention of such data (Council Directive (CE)

2006/24/EC). The Australian Government is currently considering adopting laws based on this directive (Grubb, 2010a, 2010b; LeMay, 2010). This would force some providers to store certain information for definite a period of time for increasing the power of law enforcement investigations. Communication metadata (such as the user's personal details) and activity details (such as call records) are considered personal information. Under ordinary circumstances, the average person has a right to privacy concerning their own personal information. The Australian Commonwealth Privacy Act 1988 defines personal information as:

information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion" (Privacy Act 1988).

The collection of retained data in a telecommunications system is governed by the Telecommunications Act and the Privacy Act. Section 13 of the Telecommunications Act states that "... carriage *service providers ... must protect the confidentiality of information that relates to ... (c) the affairs or personal particulars of other persons*" (*Telecommunications Act* 1997). There are no specific definitions under the law of what retained data is, however the European Telecommunications Standards Institute defines five categories of retained data: subscriber, usage, equipment, network element and additional service usage (European Telecommunications Standards Institute, 2009). Electronic Frontiers Australia (EFA) further define examples of retained data from the from an Internet Service Provider (ISP) point of view (Electronic Frontiers Australia, 2006a).

Before employing information gathering methods to gain either content or metadata, law enforcement investigators may need to identify services that are used by the target, or may need to identify the target that uses a particular service. In Australia, all traditional communication technologies that connect to the ATN are assigned a number, generally referred to as a '*phone number*'. Law enforcement has access to the Integrated Public Number Database (IPND). The IPND is a database of all numbers that can be used within the ATN for connecting carriage services. The database records current information about the numbers and includes information like the current user's details (name, address etc), the issuing carriage service provider, whether the number is unlisted and if the recorded address of the number is likely to be located at the customers service address. The IPND has several functions. The primary function is for the public and is to provide directory assistance. For this purpose, phone numbers can be supplied given an entity's particulars (the term entity is used here, as the 'owner' of a number may not be a person). The use of system in reverse, called a reverse lookup, is not allowed to the public, as this would contravene the privacy legislation. However, reverse lookups can be used for emergency services in order

to help locate users based on the originating number. Law enforcement agencies are also allowed to use the IPND this way. Access to the database for this reason is governed in the same way as other personal information stored by a carrier or CSP (under section 13 of the Telecommunications Act) (Australian Communications and Media Authority, 2010a).

For the lawful collection of retained data stored by telecommunications providers, the Telecommunications Act provides law enforcement agencies with several avenues. Any request for data made under law, such as a warrant, requires the carrier or carriage service provider to supply the relevant data. Section 282 of part 13 of the Act however, provides means for data acquisition that does not need to be made via a warrant. Law enforcement agencies can make requests to the provider that may be either certified or uncertified. Certified requests are issued with certification from a senior officer who declares that the disclosure is "*reasonably necessary*". Uncertified requests are not issued with such certification and provider must be satisfied that the disclosure is "*reasonably necessary*" for the enforcement of criminal law (Electronic Frontiers Australia, 2006a; Australian Communications and Media Authority, 2010c). In carrying out such requests, service providers must also comply with the Privacy Act.

There are several avenues that law enforcement can use to recover stored information about targets and their use of communication. The information is protected by law but in general, where there is a clear need, the information can be obtained with relative ease. In comparison to interception of communication content, the safeguards for accessing this type of information are less stringent. However, personal particulars and records of activity are in general considered less private that the content of communications.

3.1.3 Post Mortem Analysis

During the course of a lawful investigation, data may be seized from a suspect with the use of a warrant or during an arrest. In relation to traditional communications, items that may be seized are anything that contains information about the user's activities. An example of this is the seizure of mobile telephones that include phone call records and SMS messages (this is both content and metadata). A warrant is usually required as is the case with any search and seizure. Warrants for lawful search and seizure laws vary between different states and the federal jurisdiction. In South Australia, warrants can be issued under several acts of legislation most notably the Summary Offences Act of 1953 and the Crimes Act of 1914. Australian federal law enforcement can obtain warrants for search and seizure under the Commonwealth's Crimes Act of 1914.

3.2 Application of Investigation Methods

In order to determine how the functional differences between traditional and contemporary communication technologies affect the methods used by law enforcement, it is necessary to look at how these methods are applied. In section

0, six properties of contemporary communication technologies were defined. These properties represent functional differences between traditional and Internet-based communication technologies; Table 1 recaps the meaning of these properties.

Table 1: Properties of Contemporary Communication Technologies representing the functional differences to traditional communication technologies

Logic shift property	The 'intelligent' parts of the networks are conceptually located at the outside of the network.
Endpoint control property	The endpoints of the network are more intelligent and have increased flexibility and configurability.
Service decoupling property	The carrier and carriage service are independent rather than coupled as a single indecomposable package.
Lower barrier to entry property	The provision of carriage services is inexpensive and requires low technical knowledge allowing services to be supplied by more entities
Borderless supply property	Carriage service providers do not need local infrastructure or presence in order to supply service effectively.
Internet application property	The carriage service is categorised an 'Internet application' and therefore is not bound as a carriage service under the Telecommunications Act 1997.

After exploring how the methods are applied to traditional communication technologies, a direct comparison can be made with contemporary communication technologies. The identified properties are used to highlight where the incompatibilities between the target technology and the methods lie.

3.2.1 Communication Interception

The use of communications interception by law enforcement is a highly effective and robust method. This robustness is afforded due to the legislation under the TIA Act that forces TA-CSPs to provide and maintain an interception capability. When this method is used to intercept the content of traditional communication technologies, there is little the user can do to prevent this from happening as it is dictated by the endpoint control property. End-to-end encryption is one possibility however this is uncommon because it requires expensive hardware that is not

easily accessible to the layperson.

The application of content interception is quite different in relation to contemporary communication services. When considering this issue, the Internet application property must be taken into account. Where the carriage service is not deemed an Internet application, it falls under the Telecommunications Act and the situation is similar to that of traditional communications; however, the endpoint control property does not apply, affording the user greater flexibility to alter the operation of the service. The service decoupling property does not greatly affect this situation as the CSP intercepts the data at the carriage level[3]. As with traditional communication systems, the users can employ end-to-end encryption over the service. Due to the endpoint control property this is much simpler to implement as it can be performed in software; specialist hardware is not required. If users employ this method, collection of the content anywhere between the endpoints will result in only encrypted data; neither the service provider nor the law enforcement body will be able to easily recover the original communication. Note that encryption implemented by the CSP will not be an issue for law enforcement as the interception system must allow for collection of the unencrypted data.

Where the contemporary communication service has the Internet application property, interception of the content may be very difficult. Due to the service decoupling property, the collection may occur at either the carrier (i.e. the Internet feed) or carriage level with very different results. Collection at the carriage level requires compliance the CSP. Without lawful directive, the CSP may not be willing to carry out such actions, or may not have the necessary facilities to do so. Due to the lower barrier to entry property, the provider may be very different to that of a traditional communications provider. Providers of traditional communication services are generally locally based and sizable companies and in many cases have no reason to hinder police investigations. Providers of Internet application type communication services may be internationally based (borderless supply property) with no local presence or may even be a single individual with an amateur setup. Such providers can supply the same service as that of a local provider but may have less need or ability to provide assistance to law enforcement. The locality or size of the operation does not dictate the level of assistance that would be afforded to law enforcement officials, however it may be factor in many cases. Interception of this type of communication service at the carrier level negates the need to work in conjunction with the CSP. The issue with this approach is the carriage service mobility due to the service decoupling property. Any use of the carriage service over a carrier service not being

[3] Interception of content at the carrier level is possible but unlikely in the situation where it can be performed at the carriage level. However, if this does occur, the problems are the same as those described in the situation where the carriage service is not considered a carriage service as defined under the Telecommunications Act.

intercepted will be missed. Encryption is also a problem with this approach as both end-to-end encryption and that implemented by the service provider will render the approach ineffective.

3.2.2 Access of Stored Information

The access of stored information, like communication interception, is a robust data acquisition method. It is also supported in legislation by the Telecommunications Act. Law enforcement has avenues for accessing the information from the service provider both with and without a warrant. For the user of the communication service, there are few methods to avoid having this information collected. For the collection of personal particulars, the user may be able to obtain certain services with a false or alternate name preventing law enforcement from accessing the real information. For activity-related information (such as call data records or SMS activity records), there is no way to prevent the CSP from recording this information.

Again, when considering access of stored information as applied to contemporary communication services, the Internet application property must be considered separately. Where the implementation is not an Internet application, the situation will be the same as with traditional communication technologies. For user activity data, neither the service decoupling property nor the endpoint control property presents an issue for law enforcement as the CSP must be able to receive this data to perform the functions of the system (i.e. one cannot encrypt the intended destination of the communication as the communication system could not use this information to perform its functions). With the support of the Telecommunications Act, law enforcement agencies will always be able to access this information lawfully. Personal particular information, as with traditional communication technologies, must be collected by the CSP however in some cases it may be possible to provide false information.

Where the carriage service is an Internet application, law enforcement many be restricted in its ability to collected retained information. Such providers do not have any legal obligation to collect either information about users or information about their activities. Even where personal information is collected, police have limited options in forcing the provider to share the information. This effect is predominately due to the lower barrier to entry and the borderless supply properties of contemporary communication technologies. The former allows almost any person or company to offer services who may have no need for collecting such information, or may even explicitly not collect it as a ‘feature’ for a secure communication service.

3.2.3 Post Mortem Analysis

The application of post-mortem analysis for gaining information about communication technologies is quite different to the other common methods.

Post-mortem analysis relies on obtaining information from the source rather than via a service provider (or service provider's infrastructure). The information gained may be a mix of content, metadata and other types of communication and non-communication data. Unlike the other methods, there are no laws specifically supporting access of communication data by this method. Law enforcement practitioners must rely on good methods for extracting all of the information available on the target device.

In traditional communication technologies, post-mortem analysis is only useful for the analysis of mobile phones; PSTN endpoints have no processing or storage capabilities. Traditionally there have been little protections from the use of sound post-mortem analysis techniques on mobile phones; protections such as a PIN on the phone and SIM card are generally quite rudimentary to bypass with the aid of the telecommunication companies and forensic software and hardware. Full disk encryption has not generally been available to users on most mobile phone handsets.

The shift towards contemporary communications is somewhat blurred concerning mobile phones. The growth of smart phones has morphed the average mobile phone into a small but powerful computer. Smart phones still generally support traditional communication functions but also commonly support Internet and user installable applications and therefore also support contemporary communication technologies. The increased use of such devices for holding personal data has amplified demand for encryption and the increased power has supported this. Technically strong and properly supported encryption is an issue for law enforcement as decrypting may be infeasible. Furthermore, contemporary communication services used via the mobile phone may not use the local storage media and instead opt for a remote storage location. While analysis may confirm the service is in use, there may be no feasible methods for recovering the data stored on the remote server.

3.3 Case Study

In order to provide an overview of how the uptake of contemporary communication technologies may change the way in which investigations are conducted or may unfold, several cases are studied where information from communication systems were used. The case study does not seek to assert that the results would have varied in the referenced cases should contemporary communications technologies have been used, but rather it seeks to provide a thought experiment to assess the possibilities.

3.3.1 Case 1

This case involved a conspiracy to import illegal substances in commercial quantities (*El-Jalkh, Antoine v R [2009] NSWCCA 139* 2009). Law enforcement officials were notified of the conspiracy by an informant and subsequently obtained a warrant for the interception of communications on the target's mobile

telephone service; the collection included both voice calls and SMS to and from the target. Both the SMS content and voice recordings from the interception were used in the trial to establish the facts of the case.

If the key parties in the above scenario had been using contemporary communication technologies, the investigators may not have been able to collect as much relevant communication content. An application such as Skype could have been used for placing phone calls that were secure from interception. Interception of the target's Internet service (carrier level) would have provided no benefit due to the encryption. Interception may still have been possible if it occurred on another target's telephone service where Skype was used to place a call to, or receive a call from that service. SMS or SMS-like messages could also have been sent using Skype or other applications that provided encryption. Furthermore, the offender could have used alternate Internet connections to send data providing a further barrier to interception.

While the investigators collected evidence from a variety of sources including witness testimony and hidden recording devices, the case may have been weakened had they not been able to intercept the content of communications used for carrying out the crime and present it as evidence.

3.3.2 Case 2

In a case involving a homicide, stored records of phone call and SMS activity were used as evidence (*R v Wilkinson (No. 5) [2009] NSWSC 432* 2009). In this case, a pattern of activity was used to establish information about the mindset of the offender. By using source, destination and time information about the communications from the target's telephone service, the prosecution was able to demonstrate to the court the "*intensity*" of the relationship between two people. It was further able to indicate the state of mind of the offender by a change in the pattern of sent text messages around the time of a significant event. While the information was not used as a single piece of evidence, it was important information used to support the facts of the case.

In the above case, if the offender had used an Internet-based communication technology, the pertinent evidence may not have been available. Instead of standard SMS messages from a traditional mobile phone service, the offender could have used an application such as Skype to send SMS or instant messages. In such a case, the investigators may not have been able to access records about the communications between the two people thus potentially limiting the prosecution's case.

3.3.3 Case 3

In a case involving a person being charged for the supply of a prohibited drug, the contents of a text message on the target's mobile phone were used to support the prosecutors case that the person was a supplier of drugs (*Zahrooni v R; Director of Public Prosecutions (NSW) v Zahrooni [2010] NSWCCA 252* 2010). On

arresting the offender for the possession of prohibited substances, a search of his mobile phone revealed an SMS text message soliciting the procurement of drugs. The content of the message was subsequently used in convicting the offender.

The above case relied on a physical examination of the offender's device. The offender did not employ any countermeasures in order to stop examination of data on the device. If the offender had have been using an Internet-based communication technology, the retrieval of the evidence many not have been possible. Such an application may not store information on the local device and may have provided additional protection by forcing the user to supply credentials before being able to obtain the data. Additionally, the user may have been able to encrypt the contents of the storage volumes, protecting it from physical recovery of remnant information. Although such an application may not exist in this form currently, it would be easy for it to be designed and implemented. Such an application could include many measures that protect information for the specific purpose of avoiding law enforcement.

4. CONCLUSION

The digital age has seen a dramatic shift in the way that technology affects many aspects of daily life. As technology evolves, users will naturally gravitate towards the implementations that make their life easier, more convenient and more fulfilled. Communication tools are a prime example of the evolution of technology being embraced by both providers and users. The Internet has allowed the creation of novel communication services that surpass, in terms of functionality, traditional technologies such as the PSTN and mobile phones. While there are many advantages to explosion of new communication technologies through the community, there are several notable disadvantages. Among these is the ability for law enforcement to carry out information recovery during investigations effectively. Primarily, law enforcement needs methodologies for obtaining information about targets and their use of communication technologies. A set of sound and rigorous methods exist to target traditional technologies. However, newer Internet-based technologies are functionally very different and as a result, the existing methodologies that were previously quite effective are now largely incompatible for use on new and emerging communication technologies.

The investigation of communication technologies is an important activity that law enforcement agencies carry out. Traditional communication technologies are so pervasive in society that many crimes will inevitably involve their use at some point. It is important that methodologies are rigorous and well designed in order to be effective. The consequences of methodologies that are not built on rigorous principals are dire. Missing or improperly obtained information may lead to incorrect conclusions or inadmissible evidence in a court of law. Over the extensive lifespan of traditional communication technologies, methodologies have been built that support the acquisition of information in a legally sound and

rigorous manner. In obtaining information about the use of traditional communication technologies, police use a combination of communication interception, access of stored information and use of post-mortem analysis. Two major factors support these methods, legislation and the nature of the technology. The legislation is effective in allowing law enforcement to carry out certain activities but also in forcing service providers to operate in certain ways that support law enforcement (e.g. collecting certain types of information). The 'nature of the technology' is more nuanced. It effectively relates to the low level of control the user has over the technology that largely prevents the users from circumventing law enforcement methods of obtaining information.

The methodologies used for investigation of traditional communication technologies are well suited to their purpose. As the target technologies have existed for many years and have evolved little over this time, the methods have evolved and become sound and rigorous. However, they have also become specific to their intended use. This means they are inflexible and do not cope well with altered parameters. Internet based communication services are very different to traditional communication technologies. Primarily, where the operation of traditional communication technologies is very rigid, Internet-based technologies are highly variable. The methodologies that have developed for the investigation of traditional communication technologies may not be effective against contemporary communication technologies in many cases.

Internet-based communication technologies can have several properties that reduce the utility of current investigation methods. The logic shift property was discussed as the root of many of the properties that cause the ineffectiveness of current methods. From this property, the endpoint control property, service decoupling property, lower barrier to entry property and the borderless supply property are propagated. The Internet application property is also a major influence in the potential effectiveness of law enforcement methodologies. Each of the identified properties affects the application of methods for obtaining information in different ways. The Internet application property was shown to be very influential in determining whether the service providers had to meet obligations under the relevant legislation. It was shown that where a communication service was not an Internet application, it was generally susceptible to the current law enforcement methods. It is possible that users with some technical skills could implement end-to-end encryption over the carriage service to prevent communication interception. Similarly skilled users could also use encryption products for encrypting media sources preventing post-mortem analysis. In all cases, access to stored information still applies as users can do nothing to prevent this. For the average user, or those not deliberately implementing measures to impede law enforcement, current investigation methods will be successful where the communication service is not an Internet application.

Law enforcement investigation methods where the carriage service is an Internet application were shown to be ineffective in many instances. When carrying out communications interception, the provider has no legal obligation to assist law enforcement. The use of interception at the carrier level circumvents the carriage service provider but the service decoupling property will mean that communications may be missed, and the use of encryption will render this approach ineffective. Another layer of complexity is added by the lower barrier to entry and the borderless supply properties that affect both communication interception and access of stored information. The carriage service provider could potentially be anyone located anywhere in the world. This may make even attempting to interface with the provider very difficult, let alone accessing the required information. These properties potentially allow the provision of services for the direct purpose of secure communication that cannot be intercepted or recovered by third parties; this is contrary to traditional communication services where such a service would be illegal. Even users with low technical skills could employ these services to utilise secure communication greatly increasing the potential user-base.

The increasing complexity of end-user devices is another change that works against law enforcement methodologies. Many devices now have built in encryption that can be easily activated by even technically low-skilled users. This will prevent the use of post-mortem analysis to recover any information stored on the device. More highly skilled users can employ advanced techniques such as data obfuscation or plausible deniable encryption to add a layer of complexity to an investigation.

The legislation supporting current methodologies and the inherent nature of traditional communication technologies provides an almost 'ideal' situation for law enforcement. However, contemporary communication technologies may always provide a challenge due to its very nature. Even with a widened scope of current laws to incorporate Internet-based carriage services in the same way as traditional carriage services, the lower barrier to entry and the borderless supply properties mean that such laws may be very difficult to enforce.

Many of the functional differenced defined here will only have an impact on law enforcement in the 'worse case' scenario. When discussing why a given methods may not be applicable to an Internet-based communication implementation, a common theme was a lack of help, or active hindrance by the provider. The case study also assume worst case scenario assuming that encryption *would* be used or providers *would not* provide law enforcement with information. In many cases, Internet-based carriage service providers may not hinder law enforcement investigations and may in actively help. Anecdotal information suggests that law enforcement is often aided by the providers of Skype to recover both metadata and content. However, Internet-based communication technologies may still pose issues in other ways, like identifying that they are being used.

The functional differences between traditional and contemporary communication technologies have been defined as a set of properties that are inherent to the latter. These properties are the core reason that in many cases the current methods used by law enforcement for obtaining information about the use of communication technologies are ineffective. As the uptake of contemporary communication technologies increases, law enforcement will be under mounting pressure to investigate their use effectively. They require additional methods to fit in with the current methodologies for obtaining information where these technologies are being used. The defined properties provide a starting point for the exploration of future methods to add to existing methodologies.

REFERENCES

Australian Communications and Media Authority. (2010b, July 14). *The Integrated Public Number Database (IPND)*. Retrieved November 3, 2010, from http://www.acma.gov.au/WEB /STANDARD.PC/pc=PC_1754

Australian Communications and Media Authority. (2010c, July 15). *VoIP for Service Providers*. Retrieved October 21, 2010, from http://www.acma.gov.au/WEB/STANDARD/pc=PC_310067

Australian Communications and Media Authority. (2010a, August 26). *Disclosure of customer details under Part 13 of the 1997 Tcomms Act FAQs*. Retrieved October 21, 2010, from http://acma.gov.au /WEB/STANDARD/pc=PC_1790

Black, U. (2002). *Voice over IP*, 2nd ed. Upper Saddle River, NJ: Prentice Hall.

Cherry, S. (2005). Seven myths about voice over IP. *IEEE Spectrum, 42*(3), 52-57.

Council Directive (CE) 2006/24/EC *on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*.

Davidson, J., Paters, J., Bhatia, M., Kalidinidi, S., & Mukherjee, S. (2007). *Voice over IP Fundamentals*, 2nd ed. Indianapolis, IN: Cisco Press.

Dryburgh, L. & Hewett, J. (2005). *Signaling System No. 7 (SS7/C7): Protocol, Architectures, and Services*. Indianapolis, IN: Cisco Press.

Electronic Frontiers Australia. (2006a, October 12). *Protections of Communications: Telecommunications Act 1997 (C'th)*. Retrieved August 11, 2010, from http://www.efa.org.au/Issues/Privacy/ta.html

Electronic Frontiers Australia. (2006b, October 12). *Telecommunications (Interception) Amendment Bill 2006*. Retrieved August 11, 2010, from http://www.efa.org.au/Issues/Privacy/tia-bill2006.html

Electronic Frontiers Australia. (2006c, October 19). *Telecommunications Interception & Access Laws*. Retrieved August 11, 2010, from http://www.efa.org.au/Issues/Privacy/tia.html

European Telecommunications Standards Institute. (2009). *ETSI TS 102 657 V1.4.1 (2009-12) Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data*. Sophia-Antipolis, Cedex, France: ETSI.

Grubb, B. (2010a, July 23). *No Minister: 90% of web snoop document censored to stop 'premature unnecessary debate'*. The Sydney Morning Herald. Retrieved August 13, 2010, from http://www.smh.com.au/technology/technology-news/no-minister-90-of-web-snoop-document-censored-to-stop--premature-unnecessary-debate-20100722-10mxo.html

Grubb, B. (2010b, November 6). *Govt wants ISPs to record browsing history*. ZDNet. Retrieved August 13, 2010, from http://www.zdnet.com.au/govt-wants-isps-to-record-browsing-history-339303785.htm

LeMay, R. (2010, June 11). *Govt may record users' web history, email data*. Retrieved August 13, 2010, from http://delimiter.com.au/2010/06/11/govt-may-record-users-web-history-email-data/

Sicker, D.C., & Lookabaugh, T. (2004). 'VoIP Security: Not an Afterthought.' *Queue, 2*(6), 56-64.

Wallingford, T. (2005). *Switching to VoIP*. Sebastopol, CA: O'Reilly.

Legislation

Privacy Act 1988.

Telecommunications Act 1997.

Telecommunications (Interception and Access) Act 1979.

Legal Authorities

El-Jalkh, Antoine v R [2009] NSWCCA 139 2009, New South Wales Court of Criminal Appeal.

Zahrooni v R; Director of Public Prosecutions (NSW) v Zahrooni [2010] NSWCCA 252 2010, New South Wales Court of Criminal Appeal.

R v Wilkinson (No. 5) [2009] NSWSC 432 2009, New South Wales Supreme Court.

AUTHOR BIOGRAPHIES

Matthew Simon is currently undertaking PhD research into the use of physical

memory forensics at the University of South Australia; and is an Electronic Evidence Specialist with the Electronic Crime Section of the South Australian Police. His research interests in digital forensics include the impact of evolving communication technologies, data volume management and digital forensic policy and procedure.

Dr Jill Slay is currently Dean: Research in the Division of IT, Engineering and the Environment at the University of South Australia and Professor of Forensic Computing. She is a very active researcher and research leader and well-known internationally as a pioneer in forensic computing research. Currently, she carries out collaborative research in Forensic Computing, Information Assurance and Critical Infrastructure Protection with industry, State and Federal Government partners in Australia, South Africa, USA and Asia, and works with the Malaysian and Lesotho governments, supporting them in research development.

She has extensive teaching experience in the tertiary sector at undergraduate and postgraduate level and has personally supervised more than 30 cross-disciplinary honours and coursework masters, and 7 PhD students (7 more still incomplete in their theses and projects). She has lived and taught in UK, Hong Kong and Australia. Jill has published one book and more than 100 refereed book chapters, journal articles or research papers in forensic computing, information assurance, critical infrastructure protection, complex systems and education.