Threats to Mobile Phone Users' Privacy

Contributors

Dr. Mohamed H. Ahmed (Memorial University of Newfoundland): Project Lead

Jacqueline Penney (McInnes Cooper, Partner): Lawyer and Privacy Consultant

Dr. Salama Ikki (University of Waterloo): Research Associate

Abdulazeez Salami (Memorial University of Newfoundland): Graduate Student

Tanya L. Bath (McInnes Cooper, Associate): Lawyer and Privacy Consultant

Mohamed Abd Allah (Memorial University of Newfoundland): Undergrad Student

Sherif Mansour (Memorial University of Newfoundland): Undergrad Student

March 2009

Contact Author

Dr. Mohamed Hossam Ahmed
Faculty of Engineering & Applied Science
Memorial University of Newfoundland
St John's, NL, Canada
A1B 3X5
Tel: 709-737-3801
Fax:709-737-4042
mhahmed@mun.ca
http://www.engr.mun.ca/~mhahmed/

Acknowledgement

The project team would like to acknowledge the financial support of the office of the privacy commissioner (OPC) of Canada for their support for this project through the research contribution program.

Table of Contents

Chapter 1

Introduction

Mobile phones have become essential tools for communication and information exchange in the last two decades. Many people rely on their mobile phones in their personal lives as well as their businesses. Most mobile phone users exchange very sensitive and private information using their mobile phones assuming that the mobile phone network is reliable and secure.

In March 2006, a big scandal shocked Greece (and probably the whole world) when it was discovered that the mobile phones of more than 100 high-profile politicians (including the Greek prime-minister, minister of national defense and minister of foreign affairs), diplomats and many others were *illegally* intercepted (through the operator equipment) for several months (from June 2004 to March 2005) [1].

In February 2008, another scandal was uncovered when Detroit's Mayor was accused to be involved in an affair with his chief of staff and both of them denied the allegation and lied under oath about it [2]. The main evidence against them was the text messages, which the operator (*legally* this time) had been storing for years.

These two incidents are examples to indicate that the privacy of the information and messages users send/receive by their mobile phones, can be *legally* or *illegally* breached by law enforcement officers, operators, or even other individuals or groups who have the technical expertise and the required equipment. What is even worse is that most users of mobile communication systems are unaware of (or unable to deal with) the many threats to their privacy.

Recent statistics show that there are more than 21 million mobile phone users in Canada and this number is expected to reach 20 million by 2010 [3]. Mobile phone users in Canada (as many others worldwide) always assume that there is no reason to worry about the privacy of their phone calls and text messages sent over their mobile phones. To the best of our knowledge, no previous study has investigated the privacy of mobile phone users in Canada. This study investigates the threats to mobile phone users' privacy in Canada from technical

and legal perspectives. We also propose a set of measures and recommendations to deal with these threats to improve mobile phone users' privacy.

1.1 Mobile Phone Networks

Mobile phone systems are hybrid (wireless/wirelined) communication systems. As shown in Fig. 1.1, the connection between the mobile phone and the serving unit (called base station) uses wireless communication. On the other hand, base stations are connected to a sophisticated switching center (called mobile switching center) through optical fibers or microwave links. The connection between the base station and the mobile switching center might be direct or through a controlling unit called base station controller. The mobile switching center connects the mobile phones to other mobile phones or to fixed phones through the public phone network. The connections between the base stations, base station controllers, the mobile switching center, and the public switching telephone network usually use optical fiber or microwave links. The connections between the mobile phones and the base stations constitute the radio access network, while the connections between the base station and the mobile switching centers and between the mobile switching centers to each other and to the public switching telephone network constitute the core network (also called the fixed network).

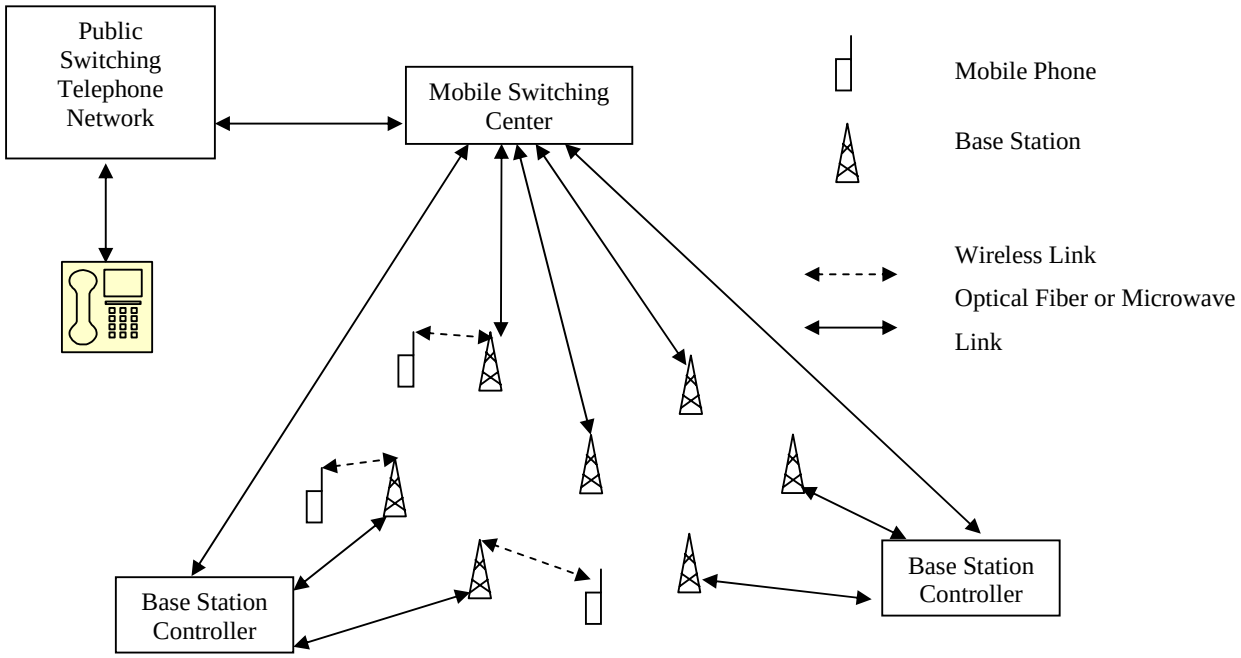

Fig. 1.1 A Simplified Model for the Mobile Phone Network Architecture.

1.2 Different Mobile Phone Systems in Canada

Early mobile phone systems such as the first generation North American system (advanced mobile phone system (AMPS)) have used analog signal representation and processing. AMPS is the mobile phone system standard developed by Bell Labs, and officially introduced, after the approval of the Federal Communications Commission (FCC), in the Americas in 1983 and Australia in 1987. During the 1980s and into the 2000s, it was the technology that was in vogue in North America and other localities [1]. Such analog mobile phone systems could be intercepted easily using radio receivers called frequency scanners.

Second generation systems moved to the digital era but with only voice communication and some sort of data communications as in Global system for mobile communication (GSM), code division multiple access (CDMA) (also known as IS-95 or cdmaONE) and digital AMPS (D-AMPS) (also known as TDMA, IS-54 or IS-136). One of the many advantages of the digital mobile phone systems is the ability of encrypting the signals for better privacy and security.

Advances in mobile technology led to the proliferation of third generation (3G) systems with added features like multimedia communication, mobile commerce, etc.[2]. Third generation systems (also known as cdma2000 and UMTS) are based on CDMA technology as explained in Chapter 3.

AMPS and D-AMPS are obsolete now in Canada. Mobile phone operators provide mainly two systems: GSM and CDMA (cdmaONE, cdma2000, or UMTS). Table I below shows the main mobile phone operators in Canada, the adopted wireless technology and the province(s) where the service is offered.

Different mobile phone systems vary widely in the system design and the underlying technology. However, all second and third generation mobile phone systems try to offer high levels of security and privacy to the user through user authentication, signal encryption and user anonymity. Nevertheless, these techniques, unfortunately, do not guarantee the privacy of mobile users as will be discussed in the next chapters.

Table 1.1. Major Mobile Phone Operators in Canada [3].

Operator	Technology	Province	Number of Subscribers (in Millions)
Bell Mobility (including Aliant)	CDMA	ON, QC and NL	6.5
Rogers (including Fido)	GSM	ON, QC	8
Telus Mobility	CDMA	AB, BC, ON, QC, NL	6.1
MTS Mobility	CDMA	MB	0.435
SaskTel	CDMA	SK	0.452

1.3 Privacy of Mobile Phone Users

There are various threats to mobile phone users' privacy. The main threats include the following:

i. Signal Interception: The most notable threat to mobile phone users' privacy is the signal interception (phone tapping). The signal can be intercepted either on the radio access network or on the core network. The former case can be implemented by detecting the wireless signal but this needs cracking of the encrypted signal (if it is encrypted), while the latter case can be implemented by tapping the signal in the switches or transmission medium (optical fiber, coaxial cables, or microwave links) but this requires access to the core network infrastructure. Although the two options seem challenging, both options are feasible particularly for operators, law enforcement officers or even individuals with enough expertise and tools.

ii. Access to text messages: When a mobile phone user sends text messages using his/her mobile phone (e.g., SMS messages using GSM) this message can be intercepted in the same way voice signals are intercepted. Furthermore, most of the operators keep text messages on their servers for certain durations ranging from few days to years. When the text messages are available at the operators' servers, these messages can be accessed by the operators and/or law enforcement officers. Getting access to the stored text message (by outsiders) is very challenging but not impossible.

iii. Access to user records: Mobile phone users' records at the operators' servers include private information such as the calling activities (called and calling numbers, times and duration of phone calls, etc.), user location, and billing information. This information is mainly handled by the operator. Similar to the text message case, having access to the user records (by outsiders) is highly unlikely to happen but should not be excluded as a possible threat.

iv. Access to stored information on mobile phone sets: When a mobile phone set is lost (or stolen), all information stored in the mobile phone becomes available to those who have access to the phone even if the stored information is password protected. Many people erase the stored information before they sell or discard old mobile phone sets. Doing this does not necessarily guarantee privacy of the stored information since it is possible, using special software programs, to restore this information [5]. Access to stored information on mobile phone sets by intruders can happen even if the user does not lose/sell his/her phone set. This can be done by the intruder through devices (mobile phones, computers, etc.) equipped with Bluetooth connections.

1.4 Laws and Regulations Related to Mobile Phone Users' Privacy

Chapter 4 analyses federal and provincial privacy legislation in Canada and its impact upon the mobile phone user's privacy. The privacy aspects of the federal *Telecommunications Act* which regulates mobile phone service providers are reviewed in this chapter. Provisions of the *Charter of Rights and Freedoms* and *Personal Information Protection and Electronic Documents Act* and corresponding case law are analysed. The private communication interception provisions of the *Criminal Code* and the *Canadian Security Intelligence Service Act* is reviewed. The privacy laws and regulations in the United Kingdom are also analyzed for comparison purposes. Finally, the *USA Patriot Act* and its impact on the Privacy of mobile phone users in Canada are addressed.

1.5 Report Contents

The rest of this report is organized as follows. Chapter 2 discusses the threats to mobile phone users in more details including some case studies. The technical background of mobile phone networks and its operation is provided in Chapter 3. This chapter also discusses how the different threats of mobile phone users' privacy can happen. Chapter 4 investigates the mobile phone users' privacy from legal perspectives. Then, Chapter 5 discusses some

remarks obtained from surveys of mobile phone users. Finally, conclusions and recommendations are given in Chapter 6.

References

[1] Analog Mobile Phone System; Wikipedia; http://en.wikipedia.org/wiki/Advanced_Mobile_Phone_System.

[2] Mohammad Ghulam Rahman and Hideki Imai; “Security in Wireless Communication”; Journal of Wireless Personal Communications, Volume 22, Number 2, pages 213 – 228, August 2002; Springer Netherlands; http://www.springerlink.com/content/v52101t23m6r241n/fulltext.pdf.

[3] List of mobile network operators of the Americas http://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_the_Americas#Canada.

Chapter 2

Threats and Risks to the Privacy of Mobile Phone Users

This chapter is a comprehensive yet interesting treatise on the existent and imminent threats facing the mobile phone users. These threats can be broadly categorized into two, namely; signal interception and access to user information. Access to user information can be subdivided into access to text messages, access to user records and access to stored information on mobile phone sets. These four threats are the germs upon which the first four sections of this chapter were developed.

The first section commences by highlighting the background concepts underlying signal interception. This is followed with a proper definition for signal interception with special emphasis on the possible regions in the mobile phone network where signals can be intercepted. Afterwards, the reader is made to be aware of the some hardware and software techniques that can accomplish the task of signal interception. Upon discussing this, a critical review of analog mobile phone system is done and at the same time, analysis of the contemporary digital mobile phone system is done to reveal its vulnerabilities. This section ends with the discussion of pertinent cases to substantiate the claims made earlier in this section.

The second section begins with a systematic introduction of text messaging to the meaning of access to text messages. Afterwards, this section points to the fact that law enforcement agents have access to text messages. After discussing this point, instances were cited to buttress this claim. Subsequently, the threats from malicious attackers were also brought into view with cases to validate the existence of such threats. This section ends with the mention of the combination of software and/or hardware tools for data recovery.

The third section starts with a coherent description of what user records are and where they can be found. This is followed with the discussion of the various ways by which user records can be accessed from the mobile phone or the operator’s database server. This section ends with citing of relevant cases to reinforce the explanations made earlier in this section. The fourth section

commences the description of modern mobile phones and how they competently perform the role of data processing, storage and transmission. Subsequently, the different scenarios by which stored information can be accessed is brought to the reader's attention. This section ends with convincing real life instances to support the explications made earlier in this section.

The fifth section is an exploration of other possible threats. The first issue to be looked upon is the possibility of using a mobile phone for tracking and locating a person. This was adequately supported with a news report. The other issue that was investigated in this section is the possibility of malicious threats to mobile phone users as a result of Bluetooth technology. This was also sufficiently reinforced with a news report touching every nook and cranny of the issue. This section is concluded by a call for pragmatic and reliable mobile security solutions.

2.1 Signal Interception

Before delving into the details of signal interception, it is of utmost importance to trace its root back to its ancestor – eavesdropping. Eavesdropping is simply the act of secretly listening to a private conversation which can be viewed as either unethical or advantageous depending on the parties involved in this act and the underlying motives for indulging in such act. It can be done over telephone lines (phone tapping), email, instant messaging, and other modes of communication considered private [1]. It must be highlighted at this juncture that signal interception technically falls under phone tapping. Consequently, a brief explanation of what phone tapping is will undoubtedly shed more light on what signal interception really is.

Phone tapping is the monitoring of telephone and internet conversations by covert means with the aim of gaining knowledge about the transmitted information and/or altering this information [2]. Hence, in this context, signal interception can be simply described as the acquisition and/or interruption of data which is being transmitted on the radio access network which represents the connections between the mobile devices and the base stations or on the core network which constitutes the connections between the base station and the mobile switching centers and between the mobile switching centers to each other and to the public switching telephone network.

The issue of signal interception or eavesdropping has evolved in a dramatic manner from an occasional topic of discourse of technological insiders into a daily subject matter of everyone in the mobile communication community due to the undesirable effects that ensue from such hostile attacks. The rampant proliferation of signal interception hardwares [3], [4] and the realization of software techniques to make mobile devices hack prone [5] are all irrefutable evidences buttressing the fact that signal interception is a major threat to all mobile customers' privacy.

In addition to what has been aforementioned, it must also be noted that this threat to wireless and cellular communications device is as a result of the interception of the radio frequency (RF) signal transmitted from the mobile unit which is at the user's end or from the base station. The Advanced Mobile Phone System (AMPS) is a good example to reflect upon. Although this technology is more or less obsolete now, it is of vital importance to mention that when the use of this technology was still in vogue, a conversation can be easily intercepted by a frequency modulation (FM) frequency scanner that operates in the 824 – 849 MHz range for mobile transmit and 869 – 894 MHz range for mobile receive range [6]. This evidently demonstrates that such intrinsic deficiencies are long-existing issues calling for pragmatic solutions.

Apart from the elucidated vulnerabilities in the AMPS technology, careful thought must be given to the fact that the current mobile phone technology is not impregnable to the vicious attacks of signal interceptors and eavesdroppers. In fact, the most notable threat to mobile customers' privacy is signal interception which is also known as phone tapping. This can be done by using either of the following two techniques: (1) by intercepting the signal on the radio access network or (2) by intercepting the signal on the core network.

The first technique can be implemented by detecting the wireless signal in transmission but this needs cracking of the signal if it is encrypted, while the second technique can be implemented by tapping the signal in the switches, servers, or transmission medium (such as optical fiber, coaxial cables or microwave links) but this requires access to the core network infrastructure. Although the two options seem challenging, they are in fact quite feasible for special parties like mobile operators, law enforcement officers, organizations or individuals equipped with the requisite sophisticated skills and tools to gain access to the network. This is also validated in a report

which shows that satellite and cellular networks require expensive radios along with other software and hardware for signal interception and manipulation [7] but this is quite viable for the special parties mentioned.

There are numerous pertinent instances which substantiate the expositions in the previous paragraphs on how the vulnerabilities in modern-day mobile devices can be exploited by malicious attackers. To start with, an older incidence is that of an Ottawa-based web site that was streaming live audio from cellular telephones onto the Internet from a radio. This was realized because a scanner was intercepting cellular phone traffic. This same scanner was connected to a computer that was hosting a web site. Therefore, by connecting to this web site, anyone could listen to private mobile phone conversations [8].

Another hot case is the Athens affair. On 9 March 2005, a 38-year-old Greek electrical engineer named Costas Tsalikidis was found hanged in his Athens loft apartment, an apparent suicide. The next day, the prime minister of Greece was told that his cell phone was being bugged, as were those of the mayor of Athens and at least 100 other high-ranking dignitaries, including an employee of the U.S. embassy. The victims were customers of Vodafone Greece, the country's largest cellular service provider; Tsalikidis was in charge of network planning at the company and he committed suicide obviously out of the fear of being implicated. Given the list of people and their positions at the time of the tapping, who knows the amount of sensitive political and diplomatic discussions, high-stakes business deals, or even marital indiscretions that might have been routinely overheard and possibly recorded [9]?

GSM is used by many mobile companies worldwide but there is an alarming report by security researchers who announced the development of an ultra-fast method of cracking wireless GSM encryption in less than thirty minutes, meaning that with a GSM wireless frequency receiver and necessary gadgets, hackers will be able to eavesdrop on phone conversations comfortably [10]. All that has been comprehensively expounded emphasizes the salient point that there is a need for reliable and pragmatic solutions to hostile threats like signal interception and eavesdropping.

2.2 Access To Text Messages

It is imperative to provide sufficient explanation of the fundamental concepts underlying the act of accessing text messages before prodding into the access issue. As a consequence, key concepts will be highlighted. Text messaging is the common term for the sending of text messages from mobile phones using services such as Short Message Service (SMS) on GSM, SkyMail on JPhone, Short Mail on NTT Docomo, SMTP on RIM Blackberry, etc. These text messaging services are communications protocol allowing the interchange of short text messages between mobile devices and as mentioned earlier, such services are available on most mobile devices with on-board wireless telecommunications [11], [12]. From the conceptual elucidations provided, access to text messaging can be described as the acquisition of stored or even deleted text messages from users' mobile device or operators' servers by special parties (mobile operators, law enforcement officers or hackers) for legal or illegal purposes.

Law enforcement officers have no problem with obtaining records of text messages and telephone conversations from the mobile operators. In fact, they gain access to such information quickly with ease in their electronic format for meticulous scrutiny. Private detectives working in Poland provide their clients with access to the text message archives of the person under surveillance, especially when investigating someone's private life [13]. To further substantiate these claims, it will be of vital importance to mention Disklabs Forensics Services that offers thorough mobile phone forensic investigative analysis. Upon request, they provide comprehensive report about the mobile phone user and all data and records contained therein. For instance, with respect to short message service (SMS), they provide detailed information about the (Subscriber Identity Module) SIM card SMS memory usage and confidential details about the SMS message itself like the originating address and the complete text that was sent [14]. These points to the fact that data stored or transmitted via mobile phones are not fully secure due to the vulnerability of mobile phones.

Researchers at Independent Security Evaluators (ISE) have shown that hackers can take control of an iPhone and gain access to text messages and contact information. Furthermore, they demonstrated that by tricking the phone into accessing a particular website, or by using a rogue wi-fi connection, hackers could take complete control of the device and force the phone to send

personal information of the mobile user such as text messages and contact numbers [15]. There are numerous instances where some parties have exploited these inherent flaws in mobile devices and hence infringing on users' personal life.

An interesting case is the text-messaging sex scandal between Detroit's Mayor Kwame Kilpatrick and his chief of staff Christine Beatty. The Detroit Free Press examined over 14,000 text messages obtained from Beatty's pager, publishing those that confirmed the two were having an affair and lied under the oath about it [16]. To make the cases cited in the previous paragraph more understandable, it will be necessary to explain the technicalities underlying access to text messages. When a mobile phone user sends text messages using his/her mobile phone (for example, SMS messages using GSM), these messages can be intercepted in the same way as voice signals are intercepted. Furthermore, most of the mobile operators keep text messages on their servers for certain duration of time ranging from few days to even years. As a consequence, when the text messages are available at the operators' servers, these messages can be accessed by the mobile operators and/or law enforcement officers. In the light of what has been mentioned, it must hence be put into cognizance that getting access to the stored text messages (by any third party) is a very challenging task but it is not impossible giving the requisite expertise and tools.

The advent of software that can competently recover and restore deleted text messages which are stored in the SIM card of users' mobile phone [17] and with a more powerful combination of software and hardware that can download entire contents of SIM card [18], [19] signifies a pressing need for reliable security solutions for mobile phones. All that has been meticulously and comprehensively explained points to the essential fact that there is a pressing need for authentic and practical security solutions for threats to mobile users' privacy, especially when it comes to the illegal and unauthorized access to text messages.

3.3 Access To User Records

A concise description of what constitutes user records in a mobile phone will be essential for the proper understanding of the mechanism of how mobile customers' privacy can be breached as a result of unauthorized access to their records on their mobile devices. Mobile customers' records

at the mobile network operators' servers are predominantly confidential information. The largest percentage of users' confidential information lies in calling activities such as logs of incoming and outgoing calls; detailed information about dialed and dialing number; precise and detailed records of times and duration of phone calls; user location at times of phone calls; billing information, etc. These data are usually managed by the mobile network operator. Just like the case of text message security, having access to the users' record by a third party is a tough and challenging task but it is not impossible as there are recent cases of infringement of mobile phone users' privacy by accessing their records. There are also cases where the mishandling and mismanagement of data on storage devices or even hardcopies of such data by the operator can pave way for intrusion and acquisition of information. It must also be noted that the technique for accessing user records is the same with the one mentioned in the previous section about accessing text messages.

The soaring list of mobile phone spy softwares [20], [21], web site [22] and tutorials [23], [24] caused a great deal of concern to savvy technical insiders, business experts and even government officials to the extent that a senate congress was held for the sole purpose of addressing the issue of protecting consumers' phone records [25]. This is to reinforce the claim that access to mobile phone users' record is a major threat to be reckoned with by looking for reliable security solutions that will protect mobile phone users' privacy.

To buttress what has been aforementioned in the previous paragraph, a number of recent and popular cases will be discussed. It is more befitting to commence with an interesting and recent case which in this case is a flashback to the anti-governmental food riots in the Egyptian town of Mahalla el-Kubra. In the midst of the outcry, a large number of protesters carried cell phones which were used to make calls and send text messages. About nine months after this incidence, twenty-two people were convicted as a result of their involvement in the demonstration [26], [27]. This is utterly enervating especially when one ponders on how the government mysteriously identified and nailed the protesters. Interestingly, this seeming mystery was demystified when Annie Mullins, Vodafone's global head of content standards, declared in a Westminster eForum event that they were forced by the Egyptian authorities to hand over

customer communications data following the food riots [28]. This is unquestionably a big ethical dilemma related to the retention and release of mobile phone users' records.

Another eye-opener is the case of Verizon Wireless that fired an unspecified number of employees for accessing President Barack Obama's old cell phone records without permission. In addition to the dismissal, Verizon Wireless disclosed the privacy breach and apologized to Obama [29]. In contrast to the first case, this act was perpetrated by a number of people. This distinctly delineates the parties involved in accessing mobile phone users' records.

A distressful case is that of hackers who stole confidential data on 60,000 Norwegians. They used a weakness on the web site of the mobile network operator Tele2 to procure the national personal identity numbers and addresses of subscribers, amounting to 1.3 percent of the country's population. The information would enable the hackers to change the addresses of the people concerned so as to intercept their mail, or order goods from their account [30]. Another case is a legal one between the Federal Trade Commission (FTC) and five Internet companies. The FTC sued these five companies alleging that they broke a federal law by selling cell phone records. One of the companies named in the lawsuit, Integrity Security & Investigation Services Inc., offers on its web site a "home infidelity kit" and private investigation service for people who suspect their spouses of cheating. The release of the records, which typically sell for $80 to $150 each, could leave consumers vulnerable to stalkers, private investigators or others who might want to track their calls. The lawsuit seeks to stop sales of the logs, which include records of incoming and outgoing calls and the times of those calls. The FTC also seeks to reclaim money made by the five companies that allegedly collected, advertised and sold the information to third parties [31].

All these worrying cases have stirred considerable level of awareness and action among the masses and the lawmakers. For instance, in the U.S., lawmakers on the House, Energy and Commerce Committee united in their call to take legal action against businesses that sell phone logs without the permission of the telephone customer [32]. All these show that there is a global awareness of the need for genuine and reliable security solutions for threats to mobile users'

privacy especially when it comes to the illegal and unauthorized access to their confidential records.

2.4 Access To Stored Information On Mobile Phone Sets

Due to the numerous advances in mobile technology, mobile phones are now equipped with more advanced and better features in addition to the existing standard voice functionality. Consequently, current mobile devices are built to support many additional features and accessories, such as communication protocols for text messaging, email, packet switching for access to the internet, gaming, Bluetooth, infrared, camera with video recorder and (Multimedia Messaging Service) MMS for sending and receiving photos and video, MP3 player, radio and GPS [33]. These whole spectrum of functionalities and the data they process as input or output constitutes the information stored on mobile phone sets.

It must be put into consideration that whenever a mobile device is lost or stolen, all information stored on the mobile device will become available to those who have access to the device even if the stored is password protected. Once again, this emphasizes how vulnerable mobile phones are. A lot of mobile phone users erase the stored information before selling or discarding old mobile phone sets but doing this does not necessarily guarantee security and privacy of the stored information since it is possible, using special software programs, to restore the deleted information [34], [35]. Access to stored information on mobile phone sets by intruders can occur even if the user did not lose/sell his/her mobile phone set. This can be competently done by a skilled intruder through devices like mobile phones, computers and others that are equipped with Bluetooth connection.

In order to adequately substantiate what has been aforementioned in the previous paragraph, some cases will be presented. Adam Gowdiak, a 29-year old Polish security researcher with the Poznan Supercomputing and Networking Center found two vulnerabilities in the cell phone version of Sun Microsystems' Java Software that under unusual circumstances could let a malicious program read private information from a mobile phone or even render the phone unusable. He figured out how to attack a Nokia 6310i mobile phone but before the vulnerabilities could be exploited, a mobile phone user would have to download and run a malicious Java

program [36]. With the rampant usage of web media facilities via the mobile phone by enthusiastic users, this can be a lethal decoy and many users will fall prey to it.

A perturbing case is that of Miley Cyrus whom a unanimous hacker preferred to be known as “K Dollars” camouflaged himself to the operator as being the legitimate owner of her account on the operator’s database. Consequently, he received her data from the operator by knavishly requesting for it. Her cell phone was also hacked into and some stored pictures was posted and distributed on various websites [37]. Another case is an iPhone embarrassment that makes it simple to access stored information from seemingly locked phones. It was exposed that an unauthorized user can exploit the inherent security flaws in the phone by simply double-pressing the button to make an emergency call. This brings up the user's preferred contacts and clicking on a number provides full access to the phone's features. Furthermore, clicking on an e-mail provides access to all e-mail and clicking on a contact name provides full access to all contacts data [38]. This is another evident proof compelling serious action on mobile phone security due to their apparent gullibility and vulnerability.

Apart from illegal access to stored information, there is also another scenario known as lawful interception. Lawful interception (LI) is the obtaining of real-time electronic network (including radio systems) forensics pursuant to lawful authority for the purpose of analysis or evidence. Such forensics generally consists of the signaling or network management information or in fewer instances, the content of the communications. If the forensics are not obtained in real-time, the activity is referred to as access to retained data (RD) [39]. In fact, a comprehensive report has been written on the topic of cell phone forensics under the auspices of the National Institute of Standards and Technology [40]. It must be mentioned at this juncture too that cell phone forensics is only successful because mobile phones are most of the time defenseless and vulnerable. Conclusively, all that has been exhaustively explained in the previous paragraphs points to the salient point of finding reliable security solutions to better safeguard users’ confidential data on his/her mobile phone.

2.5 Other Threats

Mobile phones have advanced tremendously beyond our imagination from a mere communication device to intelligent gadgets for upholding justice or in the other sense, smart tools for committing crimes. What can a mobile phone reveal? Surprisingly, much more than we might even want to disclose ourselves. If someone travels with a mobile phone, the device informs network transmitters about the change of that person's location frequently. By analyzing the speed at which radio waves travel, and employing the use of the triangulation technique, it is possible to determine the precise location of a person using his/her mobile phone for text messaging or calls, with a striking accuracy as that of GPS satellite navigation systems [13].

A news report explored every nook and cranny of mobile phone tracking by stating that mobile telephone technology is fast becoming a powerful tool of investigation in the hands of police investigators. By verifying the Call Data Record (CDR) maintained by cell phone companies, police investigators can access stored data on cell phone location and calls made by subscribers. Police can also reconstruct, down to the minute, the location of a cell phone user at any given time. The standard radio-tracking technology used by cellular companies makes it possible for police to gain valuable information about the precise location of a suspect [41].

A mobile telephone is usually associated with one particular individual and provides his/her minute-by-minute location. The technology detects the radio frequency sent from the mobile phone to service antennas. A method called triangulation helps the company detect the caller's whereabouts within its multi-antenna area of operation. Surveillance of mobile phone locations is done by measuring the signal strength from the phone to nearby towers. The company can get and store information about any cellular phone that is turned on and operating within the cellular network. This is because cell phones transmit handshaking signals to nearby cell phone towers to let them know that the phone is on and within the range of the cell tower [41].

Another news report exposed the vulnerabilities linked to Bluetooth technology. The report commenced by claiming that a study by research firm InsightExpress revealed that 73 percent of mobile phone users are not aware of security issues that could put their mobile phones at risk. To these naive users, terms such as "bluejacking", "bluesnarfing" or even "bluebugging" would

probably be totally unfamiliar. Bluejacking, also known as "bluespamming", is a technique used to send anonymous text messages to mobile users via Bluetooth. Phones that are Bluetooth-enabled can be tweaked to search for other handsets that will accept messages sent via Bluetooth. It simply presents a message, similar to e-mail spam. The recipient can ignore the unsolicited message, read it, respond or delete it [42].

Bluesnarfing is a more dangerous technique that can allow a hacker to access information stored on a mobile device without the user's knowledge. This technique takes advantage of an inherent security flaw in older versions of Bluetooth-enabled handsets, that allows an attacker to access and copy data stored on the device without the user's knowledge. Any potentially valuable information stored on the mobile phone such as address books, calendars, e-mail and text messages are at risk in a bluesnarfing attack [42].

The most serious of the three risks is bluebugging which allows attackers to access mobile-phone commands using Bluetooth technology without notifying or alerting the device owner. This vulnerability allows the hacker to initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations and connect to the Internet. As with all the attacks, the hacker must be within a 10-meter range of the targeted phone. Unlike bluesnarfing, which simply provides attackers with access to personal information, bluebugging allows the attacker to take control of the device [42].

A concluding news report highlights the issue related to the last threat in the context which is the abuse of in-built mobile phone cameras. The report describes a privacy technology known as Iceberg Systems which was built to stop people from taking pictures in sensitive places. Iceberg Systems is beta-testing Safe Haven, a combination of hardware transmitters and a small piece of control software that is loaded into a camera phone handset. When the handset is taken into a room or building containing the Safe Haven hardware, the phone is instructed to deactivate the imaging systems. The systems are reactivated as soon as the handset is out of range [43]. A concluding case is that of the civil liberties groups in the US who demanded that the Department of Justice expose details of its use of mobile phone tracking - particularly how often it is unjustly done when there are no solid justifications that a crime has been committed [44].

In conclusion, the aim of exposing all the threats from the previous sections till this section is to create awareness about the vulnerability of mobile devices and to instigate positive actions towards the creation of reliable security solutions for mobile communications.

References

[1] Eavesdropping, Wikipedia; http://en.wikipedia.org/wiki/Eavesdropping.

[2] Telephone tapping, Wikipedia; http://en.wikipedia.org/wiki/Wiretapping.

[3] The advertisement of Mobile Phone Signal Jammer DS-125 and GSM Signal Jammer DS-126 at http://www.ipmart.com/main/browse/Mobile,Phone_Phone,Accessories_Phone,Signal,Jammer,874.php?cat=874.

[4] The advertisement of Israel GPRS/CDMA-K2006 at http://www.wzzxnr.com/product.asp?id=1852.

[5] Jordan Robertson; "The cell phone as zombie PC: Hackers likely to target cell phones to build computer armies"; October 14, 2008; Associated Press; http://www.startribune.com/templates/Print_This_Story?sid=30990474.

[6] Steven C. Roberts; "Security and Privacy in the Information Age"; http://lyle.smu.edu/~levine/ee8320/SCRoberts.PDF.

[7] Mazda Salmanian; "Secure Mobile Networking: A Look Ahead"; Defence R&D – Ottawa; Technical Memorandum, DRDC Ottawa TM 2002-083; September 2002; http://pubs.drdc.gc.ca/PDFS/unc36/p518101.pdf.

[8] Part Two – Report on the Personal Information Protection and Electronic Documents Act; Annual Report to Parliament 2000 – 2001; Office of the Privacy Commissioner Canada; http://www.privcom.gc.ca/information/ar/02_04_09_02_e.asp.

[9] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair: How Some Extremely Smart Hackers Pulled Off The Most Audacious Cell-Network Break-In Ever"; IEEE Spectrum; July 2007; www.spectrum.ieee.org.

[10] J. Nicholas Hoover; "Black Hat Conference: Security Researchers Claim To Hack GSM Calls"; February 20, 2008; InformationWeek; http://www.informationweek.com/news/mobility/security/showArticle.jhtml?articleID=206800800&cid=RSSfeed_IWK_All.

[11] Text Messaging, Wikipedia; http://en.wikipedia.org/wiki/Text_messaging.

[12] Short Message Service, Wikipedia; http://en.wikipedia.org/wiki/Short_message_service#Vulnerabilities.

[13] Michal Nazarewicz; "The Spy In Your Pocket"; October 10, 2007; Technology and Society; http://www.warsawvoice.pl/view/16101/.

[14] Sample Forensics Report; October 1, 2004; http://www.mobilephoneforensics.com/forensics-report.php.

[15] Jonathan Richards; "Security Experts Claim First iPhone Hack", July 23, 2007; Times Online; http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article2125085.ece.

[16] Gina Hughes, "Text Messaging Privacy"; February 5, 2008; Yahoo Tech; http://tech.yahoo.com/blogs/hughes/22629/text-messaging-privacy.

[17] The advertisement of Pro Data Doctor SIM Card Data Recovery Software at http://www.data-recovery-mobile-phone.com/.

[18] Cell Phone Spy Gadget Recovers Deleted Text Messages; January 5, 2009; http://news.thomasnet.com/fullstory/553509.

[19] Gina Hughes, "Gadget Recovers Deleted Text Messages"; February 27, 2008; Yahoo Tech; http://tech.yahoo.com/blogs/hughes/23942.

[20] The advertisement of Ultimate Bluetooth Mobile Phone Spy at http://store.bigdaddyspy.com/ProductDetails.asp?ProductCode=BDSBLUE&gclid=CKHynbG3oJgCFQVuswodTzM0mQ.

[21] The advertisement of BlueStealth Bluetooth Mobile Phone Spy at http://www.phonestealth.com/ProductDetails.asp?ProductCode=EST001&gclid=CLOcs7e3oJgCFQJvswodNFv-nQ.

[22] Free access to cell phone records as advertised at http://web-investigation.com/Phone_Records/?gclid=CIqG8ci3oJgCFQRhswodCVhQnw.

[23] Chris Rempel, "The Truth About Acquiring Cell Phone User Records Legally"; http://www.streetdirectory.com/travel_guide/158575/cell_phones/the_truth_about_acquiring_cell_phone_user_records_legally.html.

[24] Hacking Mobile Tutorial, http://tech-xtreme.blogspot.com/2008/06/hacking-mobile-tutorial.html.

[25] Protecting Consumers' Phone Records (S. HRG 109 - 452); Hearing Before the Subcommittee On Consumer Affairs, Product Safety, And Insurance of the Committee on Commerce, Science, and Transportation; United States Senate; One Hundred Ninth Congress; Second Session; February 8, 2006; http://commerce.senate.gov/public/_files/HearingTranscriptProtectingPhoneRecords.pdf.

[26] Al Jazeera; "Egypt convicts food rioters"; December 15, 2008; http://english.aljazeera.net/news/middleeast/2008/12/20081211511544968722.htm.

[27] OpenNet Initiative Middle East and North Africa (ONI-MENA); "Can they hear me now? (On ICT regulations, governments, and transparency)"; February 24, 2009; http://opennet.net/blog/2009/02/can-they-hear-me-now-on-ict-regulations-governments-and-transparency.

[28] Tom Espiner; "Vodafone exec warns against tech regulation"; February 11, 2009; ZDNet.co.uk; http://news.zdnet.co.uk/itmanagement/0,1000000308,39614610,00.htm.

[29] Staff Sacked For Obama Cell Phone Snooping; NZ Herald News; November 24, 2008; http://www.nzherald.co.nz/mobile-phones/news/article.cfm?c_id=261&objectid=10544754.

[30] Internet Hackers Steal Confidential Data on 60,000 Norwegians; Brisbane Times; August 11, 2007; http://news.brisbanetimes.com.au/technology/internet-hackers-steal-confidential-data-on-60000-norwegians-20070811-spc.html.

[31] Yuki Noguchi, "FTC Says 5 Firms Sold Cellphone Records: Agency Sues to Stop Sales, Recover Money Made From Illegal Transactions"; The Washington Post; May 4, 2006; http://www.washingtonpost.com/wp-dyn/content/article/2006/05/03/AR2006050302145.html.

[32] Grant Gross, “Lawmakers Promise Action Against Phone Record Sales: House hold hearing on proposal to outlaw unauthorized sale of telephone records”; IDG News Service; February 1, 2006; http://www.pcworld.com/article/124592/lawmakers_promise_action_against_phone_record_sales.html.

[33] Mobile Phone, Wikipedia; http://en.wikipedia.org/wiki/Mobile_phone.

[34] The advertisement of Cell Phone Spy: Deleted Texts/Data Extractor at http://www.brickhousesecurity.com/cellphone-spy-simcardreader.html and its promotion at http://www.972telecom.com/index.php?main_page=product_info&cPath=126&products_id=582&zenid=1a0430ce51456cdaf39292bbfa3790a6.

[35] The advertisement of Cell Phone Tap SIM Bug Data Recovery Device at http://www.spyassociates.com/cell-phone-tap-sim-card-bug-data-recovery-device-p-2528.html.

[36] Stephen Shankland, “Vulnerability Hits Java For Cell Phones”; CNET News; October 22, 2004; http://news.cnet.com/Vulnerability-hits-Java-for-cell-phones/2100-1002_3-5423310.html?tag=txt.15.

[37] Christopher Null; “Miley Cyrus Cell Phone Hacker Speaks Out”; July 18, 2008; Yahoo Tech; http://tech.yahoo.com/blogs/null/99486.

[38] Apple won’t fix iPhone Passcode Hole Until September; Tech News; August 29, 2008; http://technews.blogs2k.com/tag/reference/.

[39] Lawful Interception, Wikipedia; http://en.wikipedia.org/wiki/Lawful_interception.

[40] Wayne Jansen, Rick Ayers, “Guidelines on Cell Phone Forensics”; Recommendations of the National Institute of Standards and Technology; NIST Special Publication 800 – 101; May 2007; Sponsored by the Department of Homeland Security & Technology Administration & U.S. Department of Commerce; http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

[41] G. Anand, “Cell Phone Technology Comes In Handy To Investigators”; The Hindu; October 8, 2002; http://www.hinduonnet.com/2002/10/08/stories/2002100803580400.htm.

[42] Lynn Tan, “Symantec Warns Users Over Bluetooth Security”; CNET News; September 21, 2007; http://news.cnet.com/Symantec-warns-users-over-Bluetooth-security/2100-1029_3-6209361.html.

[43] Munir Kotadia, “Privacy Technology Blocks Camera Phone Photos”; Mobile & Wireless Network Silicon.com News; September 12, 2003; http://networks.silicon.com/mobile/0,39024665,10005982,00.htm.

[44] Bill Ray, “America wakes up to the surveillance society: Who watches the watchmen's mobile phone”; The Register; July 3, 2008; http://www.theregister.co.uk/2008/07/03/us_phone_tracking/.

Chapter 3

Technical Aspects of the Privacy of Mobile Phone Users

This chapter contains profound technical knowledge about the mechanism of mobile phone networks, security measures adopted by different mobile phone systems and privacy threats. These are the three indispensable topics that must be covered if one must honestly and satisfactorily do a comprehensive study on threats related to mobile phones. As a result, a section has been dedicated to each topic in order to easily deliver the working concepts in an organized and understandable manner.

The first section looks into the ins and outs of mobile phone networks. This discussion begins with the clarification of the wired and wireless components of mobile phone networks. Afterwards, the reader is taken deeper into the mobile phone network by showing the two divisions in the network based on connections they make with the communicating units. Analog mobile phone systems are revisited with more practical details and special emphasis is laid on their pros and cons. Digital mobile phone systems are carefully introduced with sufficient technical and conceptual details. By comparing the two systems, the advantages of digital over analog mobile phone systems were brought into the view of the reader. This section ends by creating awareness about the flaws in the contemporary mobile phone systems.

The second section focuses on the security measures in the two dominant digital mobile phone systems, global system for mobile communications (GSM) and universal mobile telecommunications system (UMTS). This discussion starts by pointing to the threats posed by opting for communication via a wireless medium. Afterwards, detailed conceptual and technical details were provided on the security measures in GSM. This quickly follows by clear delineation of the limitations existing in GSM security by citing cases to validate the claims. Subsequently, UMTS was introduced by pinpointing its features, capabilities and security functions. This section ends with the exposition of the security flaws existing in UMTS and an optimistic remark about the future of mobile communications.

The third section deals with the technical foundations of the four major threats that were previously treated in Chapter 2. This discussion commences with the technical details of signal interception with reference to pertinent technologies like femtocells and IMSI-Catcher. Afterwards, the mechanism of man-in-the-middle attack is treated with special emphasis on its key role as the core technique for signal interception. Subsequently, the details of data acquisition from a mobile phone in the framework of forensic analysis are discussed as it covers access to user information via mobile phones. This is quickly followed by the various methods by which a malicious attacker might get access to user information via their mobile phones or through the mobile operators' database servers. This section is concluded by a call for practical and reliable security solutions for the contemporary mobile devices.

3.1 How Mobile Phone Networks Work

Mobile phone systems are hybrid of wireless and wired communication systems. This is because the connection between the mobile phone and the serving unit, otherwise known as base station is by wireless communication whereas connection between base stations to a sophisticated switching center, also known as mobile switching center, is through optical fibers or microwave links. The connection between the base station and the mobile switching center might be direct or through a controlling unit called base station controller. The role of the mobile switching center is to connect the mobile phones to other mobile phones or to stationary phones through the public switching telephone network.

In order to expatiate what has been aforementioned about wired communications, it is essential to further expound that the connections between the base stations, base station controllers, mobile switching center, and public switching telephone network are through optical fiber or microwave links. Knowing these basic functionalities and simple interrelationships between the communication and control units, it can be consequently conceptualized that the connections between the mobile phones and the base stations represent the radio access network, while the connections between the base station and the mobile switching centers and between the mobile switching centers to each other and to the public switching telephone network make up the core network which is also known as the fixed network. A reference to a concise summary of the mobile phone network architecture is the illustration in Section 1.1 of Chapter 1.

Casting our sight back into the past, we realize that early mobile phone systems such as the first generation North American system, popularly known as advanced mobile phone system (AMPS) used analog signal representation and processing. AMPS is the mobile phone system standard developed by Bell Labs, and officially introduced, after the approval of the Federal Communications Commission (FCC), in the Americas in 1983 and Australia in 1987. During the 1980s and into the 2000s, it was the technology that was in vogue in North America and other localities [1]. AMPS uses a range of frequencies between 824 megahertz (MHz) and 894 MHz. In order to stir competition and control prices, the U. S. government required the presence of two carriers in every market, known as A and B carriers. These carriers are each allocated with 832 frequencies: 790 for voice and 42 for data. A pair of frequencies, one for the transmission and the other for reception of data, is used to create one channel. The frequencies used in analog voice channels are typically 30 kHz wide. This 30 kHz was chosen as the standard size because it gives a voice quality that is comparatively as good as a wired telephone [2].

Relative to the contemporary digital technology, one will incontrovertibly observe that AMPS is suffering from many weaknesses since it is an analog technology. An evident flaw is in its inherently inefficient use of the frequency spectrum and the most perturbing of all its shortcomings lies in the fact that it could be intercepted easily using radio receivers called frequency scanners. This claim is best reinforced with an historical account to foster clarity and better understanding. In the 1990s, "cloning" was a technological epidemic that cost the industry millions of dollars. An eavesdropper with expert gadgets can intercept a phone's ESN (Electronic Serial Number) and MIN (Mobile Identification Number, also known as the telephone number). If an ESN/MIN Pair is intercepted, it could be cloned onto a different phone and used in other areas for making calls without paying [3]. Such distracting imperfections led to the development and shift to better and more reliable technologies.

Second generation system moved to the digital era but with only voice communication and some sort of data communications. Advances in mobile technology led to the proliferation of third generation systems with added features like multimedia communication, mobile commerce, etc [4]. Global system for mobile communication (GSM), code division multiple access (CDMA)

and third generation (3G) systems are some of the widely-used digital systems of our time. CDMA refers to a technology designed by Qualcomm in the U. S., which employs spread spectrum communications for the radio link. Rather than sharing a channel as many other network interfaces do, CDMA spreads the digitized data over the entire bandwidth available, distinguishing multiple calls through a unique sequence code assigned. Successive versions of the IS-95 standard define CDMA conventions in the U. S., which is the reason why the term CDMA is often used to refer to IS-95 compliant cellular networks. IS-95 CDMA systems are sometimes referred to as cdmaOne. The next evolutionary step for CDMA to 3G services is cdma2000, TIA/EIA/IS-2000 Series, Release A, based on the ITU IMT-2000 standard [5], [6].

GSM is a cellular system used worldwide and it was designed in Europe, primarily by Ericsson and Nokia. GSM uses a time division multiple access (TDMA) air interface. TDMA refers to a digital link technology whereby multiple phones share a single carrier, radio frequency channel by taking turns. A packet switching enhancement to GSM wireless networks called General Packet Radio Service (GPRS) was standardized to improve the transmission of data. The next generation of GSM, commonly referred to as the third generation or 3G, is known as Universal Mobile Telecommunications System (UMTS) and involves enhancing GSM networks with a Wideband CDMA (W-CDMA) air interface [5], [7].

One of the plenteous advantages of the digital mobile phone systems is the ability to encrypt signals for better privacy and security. Although mobile phone signal is encrypted when it is transmitted over the radio access network, this does not absolutely guarantee the signal privacy because encryption algorithms are not crack-proof and they are susceptible to strategic interception attacks as in the case of the GSM encryption algorithm [8]. Another enlightening and cogent point is about multi-mode phones that can switch from digital mode to analog mode depending on the availability of system coverage. In this scenario, the wireless signal can be transmitted over the radio access network without encryption, while the user, in most cases, is unaware of this threat to his/her privacy.

In conclusion, it should be noted that the two concluding paragraphs, which is in fact a microcosm of this report, made some insightful remarks about the pros and cons of the existing

mobile technology. The ultimate goal of these incisive statements is to broaden our horizon, widen our perspective and most importantly, serve as a catalyst towards the amelioration of the existent mobile technology.

3.2 Security Measures in Different Mobile Phone Systems

In order to successfully carry out an in-depth, punctilious and competent investigation into the security measures in different mobile phone systems, the scope of this analysis will be limited to GSM and UMTS security as they are inarguably the dominant systems due to their widespread use and universal popularity.

Security limitations in mobile communication stem from the fact that communication is wireless, which implies that the transmission and reception of messages is conveyed through the air. This inadvertently creates vulnerabilities that jeopardize the mobile network as eavesdroppers and hackers can exploit these inherent weaknesses and gain free rein over the mobile phone system. With the goal of overcoming some of these shortcomings, security measures were integrated into GSM with the objectives of controlling access to the mobile services and protecting any vital information from being disclosed on the radio path in order to safeguard mobile phone users' privacy [9]. Succeeding paragraphs will be dedicated to the elucidation of these security measures.

The first security measure is anonymity. The goal is to make it difficult to identify the user of the system. Anonymity is provided by the use of temporary identifiers. When a new GSM subscriber switches on his/her mobile device for the first time, the real identity which is also known as the International Mobile User/Subscriber Identity (IMUI/IMSI) is used and a Temporary Mobile User/Subscriber Identity (TMUI/TMSI) is then issued to this subscriber. From then on, the temporary identifier is used. The only possible means of determining the temporary identity being used is by tracking the user. Consequently, the use of TMUI, prevents the recognition of a GSM user by a potential eavesdropper or hacker [4], [10].

In addition to anonymity, another security measure is authentication. The reason for the inclusion of this security feature is for the operator to know who is using the system for billing purposes

[4]. This security function checks the identity of the holder of the smart card and then decides whether this mobile device is allowed on a particular network. The authentication by the network is done by a challenge-response mechanism. A random 128-bit number (RAND) which is also known as authentication challenge is generated by the network and sent to the mobile device. The mobile device uses this RAND as an input and through A3 algorithm using a secret key K_i (128 bits) assigned to that mobile device, encrypts the RAND and sends the signed response (SRES-32 bits) back. Network performs the same SRES process and compares its value with the response it has received from the mobile device so as to check whether the mobile device really has the secret key. Authentication becomes successful when the two values of SRES match thus enabling the subscriber to join the network. As a consequence, security is achieved because every time a new random number is generated, eavesdroppers and hackers do not get any relevant information by listening to the channel [10], [11], [12]. This mechanism is illustrated in Fig. 3.1.

The last security measure is user data and signaling protection. The goal of user data protection is to secure user data passing over the radio path and the objective of signaling protection is to ensure that sensitive information on the signaling channel, such as telephone numbers, is secure over the radio path [4]. To protect both user data and signaling information, GSM utilizes a cipher key. After the authentication of the user, the A8 ciphering key generating algorithm which is stored in the SIM card is used. Taking the RAND and K_i as inputs, it results in the ciphering key K_c. To encipher or decipher the data, this K_c (54 bits) is used with the A5 ciphering algorithm. It must also be mentioned that A5 is performed by the mobile itself and not the SIM card, since it is a strong algorithm that needs relatively high processing capacity which is hard coded in the hardware of the mobile device for the encryption and decryption of data while roaming [10].

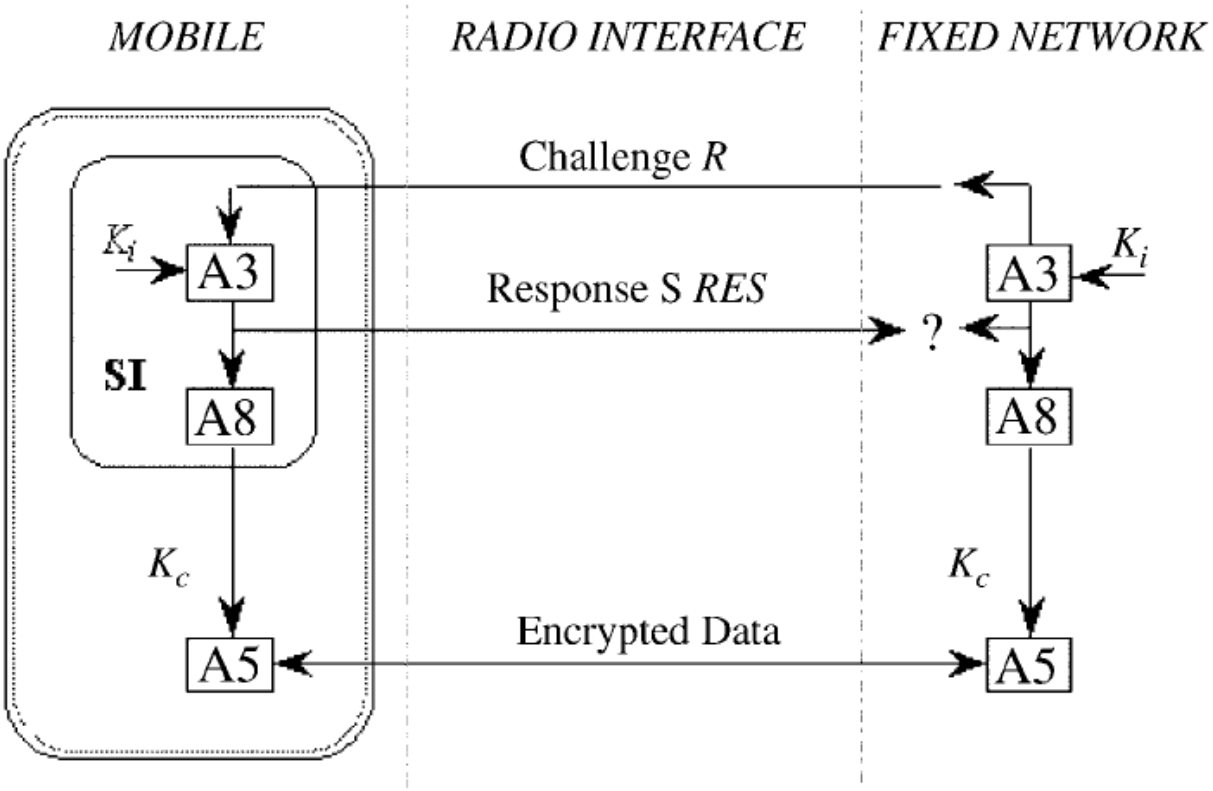

Fig. 3.1. Encryption for GSM [4]

In summary, one can easily deduce that GSM was designed with a moderate level of security. The system was designed to authenticate the subscriber using a pre-shared key and challenge-response. Communications between the subscriber and the base station can be encrypted but an impuissance lies in the fact that there are weaknesses in such encryptions. GSM uses several cryptographic algorithms for security. The A5/1 and A5/2 stream ciphers are used for ensuring over-the-air voice privacy. A5/1 was developed first and is a stronger algorithm used within Europe and the United States; A5/2 is weaker and used in other countries. Serious weaknesses have been found in both algorithms: it is possible to break A5/2 in real-time with a ciphertext-only attack [13], and in February 2008, Pico Computing, Inc. revealed its ability and plans to commercialize FPGAs that allow A5/1 to be broken with a rainbow table attack [13]. The alleviation of these deficiencies paved the way for the development of the next generation of GSM, which is popularly referred to as 3G, otherwise known as UMTS.

As aforementioned, the UMTS is an improvement over GSM and all parties in the mobile communication circus consider it as a successor to GSM. The quality of refinement in UMTS has enabled it to leverage some sophisticated and admirable functions such as remote diagnosis, vehicular internet and dynamic routing, to name a few. What distinguishes UMTS from GSM is that it handles a higher data rate per mobile user and most importantly, majority of the security limitations in GSM have been eradicated [14].

UMTS security builds upon the security of GSM, and consequentially, it inherited the established GSM security features. This continuous stream of improvement optimizes the backward compatibility between UMTS and GSM in the core network, that is, GSM subscribers roaming in a UMTS network are supported by GSM security features [15]. A helicopter view of the entire UMTS security architecture is as illustrated in Fig. 3.2.

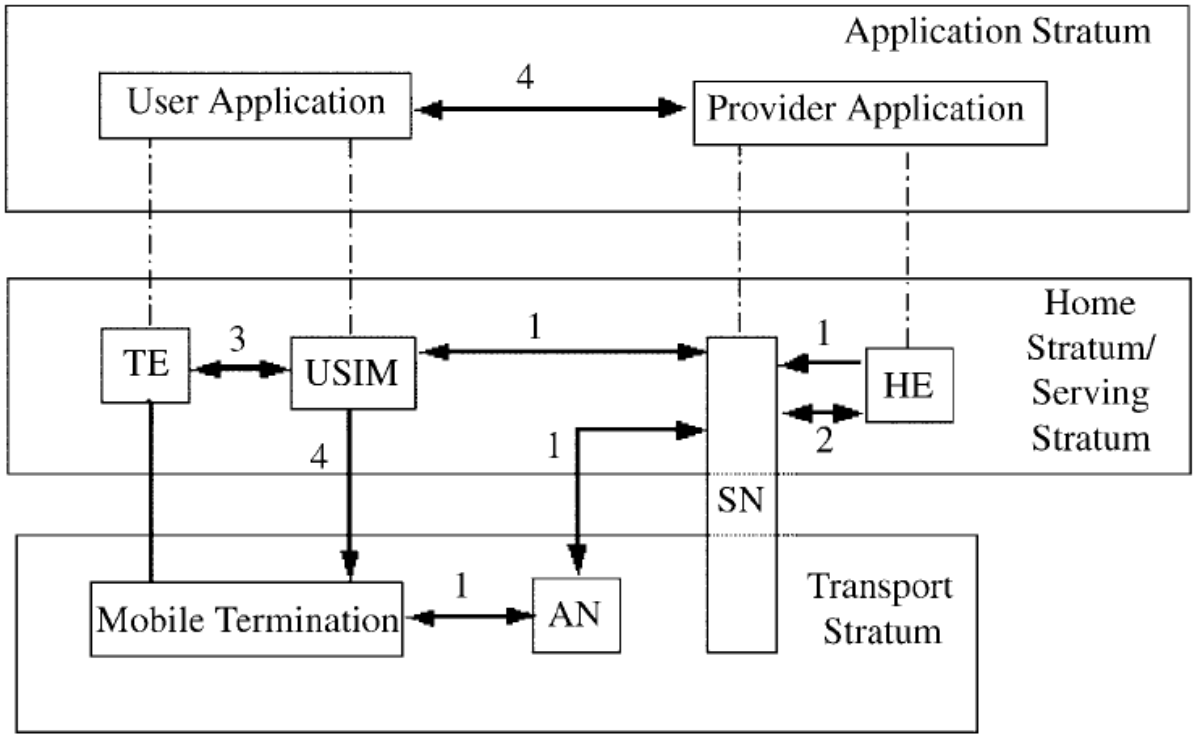

Fig. 3.2. UMTS Security Architecture [4]

TE: Terminal Equipment; USIM: User Service Integrity Module
SN: Serving Network; HE: Home Equipment; AN: Access Network

UMTS consists of five security features which will be meticulously fleshed out in the following paragraphs. The first feature (marked as 1 in Fig. 3.2) is network access security which provides users with secure access to 3G services and especially, protect against attacks on the radio access link. This feature provides user identity confidentiality, authentication of users, confidentiality of data on the network access link, data integrity and mobile equipment identification. The user identity confidentiality is achieved by the use of temporary identities just as in the case of the anonymity security feature of GSM. The transmission of the IMUI over the air interface in clear text is also avoided using a similar strategy as aforesaid in the same anonymity section of GSM security. Authentication of users is the same as in GSM where mutual authentication is achieved between the user and the network using secret key through the challenge-response mechanism. In order to achieve data confidentiality, a secret cipher key, K_c, is established as part of the Authentication and Key Agreement (AKA) process which is very much similar to the user data and signaling protection of GSM security. Data integrity is a new security feature included in 3G systems. The 3G integrity algorithm along with an integrity key (IK) will be used for providing data integrity. The IK is established as part of the AKA process. Mobile equipment identification is accomplished by using an International Mobile Equipment Identifier (IMEI) that uniquely identifies mobile equipment [4], [16].

The second feature (labeled as 2 in Fig. 3.2) is network domain security which enables nodes in the provider domain to securely exchange signaling data, and protect against attacks on the wired network. This feature provides entity (network element) authentication, data confidentiality between exchanges involving network elements, data integrity and fraud information gathering system. The functionality provided by this feature is highly important in the case where sensitive signaling information has to be exchanged between inter-network elements [4], [17].

The third feature (noted as 3 in Fig. 3.2) is user domain security with the responsibility of securing access to mobile phones. This feature provides user to user services identity module (USIM) and USIM to terminal equipment (TE) authentication. The user to USIM authentication is achieved by the means of a secret that is stored securely in the USIM. The user can have access to the USIM only if he/she proves satisfactorily displays knowledge of the secret. The user to terminal equipment authentication is realized by using a secret that is stored securely in

the USIM and the terminal equipment. Consequently, to gain access to the terminal equipment, the USIM has to unequivocally demonstrate knowledge of the secret [4], [18].

The fourth feature (denoted as 4 in Fig. 3.2) is application domain security which enables application in the user and provider domain to securely exchange messages. The 3G systems will enable mobile operators or third party providers to create applications, which will reside on the USIM. Therefore, this necessitates the security of messages which are transferred over the network to applications on the USIM with the level of security decided by the network operator or the application provider. The features provided to ensure security of messages are, namely; entity authentication of applications, data origin authentication of application data, data integrity of application data, replay detection of application data, sequence integrity of application data and proof of receipt [4], [19].

The fifth and last feature (labeled as 5 in Fig. 3.2) is visibility and configurability of security which enables users to be informed whether a security feature is operating or not and whether the use and provision of services should depend on the security feature. Customarily, all the security features should be transparent to the user but this is not always the case. Depending on the situation at hand and demands based on users' concern, users will be provided more visibility and exposure into the nuts and bolts of the mechanism of the security features [4], [20].

In conclusion, the series of contextual analysis that was carefully exposited in this section have irrefutably shown that the security provided by UMTS is far more superior to those provided by GSM. However, there are a number of issues calling for improvement. The robustness of 3G systems with respect to the security features is yet to be exhaustively and satisfactorily tested. Apart from this, a more disquieting issue is in the exposure of numerous weaknesses in the KASUMI cipher which 3G networks are using. All these points to an inspiring fact - that our mobile technology is not omnipotent and there will always be inherent imperfections but our consolation lies in the truth that there is no bar delimiting the heights that can be scaled by improving on this technology so we must continuously adapt to the emerging changes and find better solutions.

3.3 Privacy Threats from Technical Perspectives

After covering the essence of the mobile communication technology, it is vital to crown our understanding with a painstakingly careful and accurate account of the technical foundations underlying threats to mobile phone users' privacy. The provisioning of this technical account is the goal of this section. The strategy is to sequentially examine the ins and outs of signal interception, access to text messages, access to user records and access to stored information on mobile devices. These are the four dominant threats and they will be subjected to adequate clinical analysis in the succeeding paragraphs.

In order to concretize the technical details pertaining to signal interception, it is better to discuss the tools before the technique. This will foster a quick and easy understanding of concepts as the investigation cuts deeper into technical complexities. To start with, two surprisingly powerful devices will be examined. They are femtocell and IMSI-Catcher. A femtocell, originally known as an Access Point Base Station, is a small cellular base station, typically designed for use in residential or small business environments. It connects to the service provider's network via broadband such as digital subscriber line (DSL) or cable. A femtocell allows service providers to extend service coverage indoors, especially where access would otherwise be limited or unavailable. The femtocell incorporates the functionality of a typical base station but extends it to allow a simpler, self contained deployment. Although much implementation attention is focused on UMTS, this concept is also applicable to all standards, including GSM, CDMA2000, Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) and Worldwide Inter-operability for Microwave Access (WiMAX) solutions [21].

Although femtocell is a technology designed to meet benevolent needs, reports are recently emerging on how to secure this technology from being used for malevolent purposes such as unauthorized access and/or service theft, fraud and ID theft, privacy and confidentiality violations, etc [22], [23]. The underlying technique which can be used by malicious attackers is man-in-the-middle attack and unfortunately, there are two ways to implement this with femtocells. The first method is to directly intercept the signal that is being conveyed on the DSL link from the femtocells to the base station and the second way is to deploy decoy femtocells to

which mobile phones will be connected to unknowingly. The inevitable consequence of any of these means is signal interception and illegal acquisition of confidential and/or vital information. On the other hand, an IMSI-catcher is congenitally a malicious device. It is specially designed for forcing the transmission of the International Mobile Subscriber Identity (IMSI) and intercepting GSM mobile phone calls. It exploits a well-known security flaw in GSM which is the fact that the GSM specification requires the handset to authenticate to the network, but does not require the network to authenticate to the handset. Consequently, the IMSI-catcher pretends to be a base station and stores the IMSI numbers of all the mobile stations in the area as they attempt to connect to the IMSI-catcher. It induces the mobile phone connected to it to use no call encryption, thereby making the call data easy to intercept and convert to audio [24]. By paying close attention to the method adopted here, one would easily reach the conclusion that it is a variation of man-in-the-middle attack.

From what has been aforementioned in the previous paragraphs, it can be deduced that the underlying technique giving these devices the capability to intercept signals is essentially the man-in-the-middle attack. As a consequence, the focus of the current investigation will shift from the tools to the said technique. The best way to do this is to highlight the pertinent findings of an excellent research paper on a man-in-the-middle attack on UMTS [25]. The researchers claimed that the attack allows an intruder to impersonate a legitimate GSM base station to a UMTS subscriber irrespective of the fact that UMTS authentication and key agreement are used. Resultantly, an eavesdropper can listen to all mobile-station-initiated traffic.

In order to execute this attack, the researchers assumed that the attacker knows the IMSI of his/her victim. This is quite realistic because the attacker can easily obtain the IMSI from the mobile device by initiating an authentication procedure prior to the attack and then disconnecting from the mobile device after receiving the IMSI. Having established this, the attack is divided into two phases which will be lucubrated in the following paragraphs.

In the first phase, the attacker acts on behalf of the victim’s mobile phone in order to obtain a valid authentication token from any real network by following the enumerated steps: (1) during the connection setup, the attacker sends the security capabilities of the victim’s mobile device to

the visited network, (2) the attacker sends the Temporary Mobile Subscriber Identity (TMSI) of the victim's mobile device to the visited network. In the case where the TMSI is unknown to the attacker, he/she sends a false TMSI which unfortunately cannot be resolved by the network, (3) if the network cannot resolve the TMSI, it sends an identity request to the attacker and the attacker will reply with the IMSI of the victim, (4) the visited network requests the authentication information for the victim's mobile device from its home network, (5) the home network provides the authentication information to the visited network, (6) the network sends the authentication challenge and authentication token to the attacker and (7) the attacker disconnects from the visited network [25].

In the second phase, the attacker impersonates a valid GSM base station to the victim's mobile device by observing the following steps; (1) the victim's mobile device and the attacker establish a connection and the mobile device sends its security capabilities to the attacker, (2) the victim's mobile device sends its TMSI or IMSI to the attacker, (3) the attacker sends the mobile device the authentication challenge and the authentication token that was obtained from the real network in the first phase of the attack, (4) the victim's mobile device successfully verifies the authentication token, (5) the victim's mobile device replies with the authentication response, (6) the attacker gains control and chooses to use "no encryption" or weak encryption which might be a cracked version of the GSM encryption algorithms and (7) the attacker sends the mobile device the GSM cipher mode command including the chosen encryption algorithm [25]. After this phase, the attacker gains free rein over the desired communication network and the ultimate goal, signal interception, is achieved.

From the description of this technique, it is vivid that there are challenges and limitations when it comes to the effectuation of this technique but we must bear in mind that it is not impossible especially with the recent increase in speed and computational power of technology gadgets. On a final note, this attack is in fact due to the inherent flaw in GSM technology which is the provision of only access security and not protection against active attacks. As a consequence, user traffic and signaling information such as cipher keys and authentication tokens are sent in the clear over the network which makes them vulnerable to interception and/or impersonation [26].

With this, series of questions start popping out of our mind: Can vital information be obtained from my mobile device while it is in the hands of a foreign user even when it is password protected? Can the mobile operator be tricked into producing my confidential data? Can mishandling of user data with the operator lead to the exposure of hardcopies of my private data? Can my text messages be intercepted and read? And the list of question continues. Even though it is challenging, the answer to these questions is yes because it is feasible as justified in the following paragraphs.

After a comprehensive explication of the underlying technical details of signal interception, the scrutiny of access to text messages, user records and stored information on mobile phone sets and at the mobile operators' servers jointly comes into view. Current network operators of mobile communication systems store a lot of user related information on network database servers, especially for mobile telecommunication networks. This is done to assist in user mobility support as well as billing and authentication purposes. Unfortunately, this makes the user information more widespread and highly vulnerable. There is also an uncertainty as to the safety and trustworthiness of the environment where this data is stored [4]. This is because inadequate security measures, insufficient backup and recovery strategies, and mishandling of users' data at the operators'' database servers might pave way for a third party to access user records.

In order to get a good grasp of how mobile phone users' information can be acquired from their mobile phones, adequate explanations will be presented over the following paragraphs from the viewpoint of a forensic investigator using a forensic software in his/her course of mobile phone data acquisition for forensic analysis. The steps involved in such forensic analysis can be broadly categorized into connection identification, device identification, data selection, acquisition and reporting. Each of these procedures will be sufficiently exposited in the succeeding paragraphs [5].

The initial step of connection identification entails identifying the type of medium for connecting to the mobile device. The three available choices in the order of preference are connecting via a

cable, an infrared interface, or a Bluetooth interface. This is not always the case as other forensic issues may necessitate the customization of the connection type when used with specific mobile devices. In such cases, the mobile device manufacturer's user guide and web site or an independent mobile device guidance database will be consulted for further clarification [5]. XRY, the leading system for mobile forensic investigations, supports Bluetooth and infrared connections and it also provides a number of high quality cables to be able to connect and extract sufficient data from older mobile phones as well as newer ones [27].

After connection identification, the next step is device identification. In this stage, efforts are made to identify the device through the mobile phone manufacturer's name and model number [5]. A good forensic tool for this is Paraben's Device Seizure that can automate this identification process and support both phone and universal subscriber identity module (USIM or SIM) acquisition [28]. The manufacturer also has a rich repository of guidelines touching key areas of forensic investigation. For instance, the manual for mobile device seizure can be easily located at [29].

Upon identifying the mobile device, the next step is to choose the subset of data to be recovered from the whole set of SMS history, phonebook entries, call log entries, calendar entries, SIM data and picture entries. It must be put into consideration that the amount of recoverable items depend on the mobile phone under investigation and forensic issues which might oblige the forensic investigator to skip recovery of a particular item for more vital data items [5]. XRY and Device Seizure are both competent tools that automatically list the items to be recovered, perform the recovery and generate a report of all items recovered [27], [28].

After the data items to be recovered are selected, acquisition begins. Depending on the depth of knowledge needed, acquisition may be done quietly or informatively with a viewable log as it progress. For example, SIM data may be acquired in two ways: indirectly through commands sent to the phone and passed on to the SIM or directly through commands sent to a SIM reader into which the SIM is placed [5]. An excellent forensic tool that provides capturing of a detailed log of the entire acquisition and searching for an item of interest within a body of digital evidence is Oxygen Forensic Suite 2 [30]. The most important benefit of having detailed logs lies

in the fact that they may occasionally contain advantageous forensic data items or even clues that might be overlooked when a logging is performed at a peripheral level.

The final step is reporting, which allows the generation of a report in a variety of formats such as HTML, XML, Microsoft Word, .XRY by XRY forensic software and many other formats. The report facility of the forensic software may also support adjusting the report output for the inclusion of laboratory names and logos and information acquired elsewhere, such as pictures of the mobile device at seizure or at reception at the laboratory [5]. This satisfactorily ends the ongoing discussion forensic analysis of mobile devices but there is an opposite dimension that needs to be treated too. This is related to the issue of a malicious attacker accessing user information via their mobile phones or at the mobile operators' database servers.

The aforementioned issue has been lingering around for a long time but it gained strong footing in the media when Wal-Mart fired an employee for intercepting text messages between the company's media-relations staff and a New York Times reporter [31]. There are several ways to intercept and/or access text messages and user records but a few of them will be discussed in this context. The most rudimentary way is when the mobile device is misplaced or lost or at worst, stolen. When any of these happen, the safety features on the mobile device will be disarmed and confidential and vital information will be accessed with specialized tools and techniques [4]. Another means is by phone cloning which lets an attacker to intercept incoming messages and send outgoing ones as if the attacker's mobile device were the original. If both mobile devices are near the same broadcast tower, the attacker can also eavesdrop on calls. To clone a mobile device, the attacker has to make a copy of its SIM card, which stores the mobile device's identifying information. This requires a SIM reader that can read the SIM card's unique cryptographic key and transfer it to another mobile device [32].

Another way is to intercept unencrypted or poorly encrypted messages directly as they are broadcasted over cellular channels. To steal messages with a mobile device, an attacker would need to upload illegal "firmware" onto his/her mobile device. As a result, the mobile device will undergo metamorphosis and change into a radio which allows it to pick up all the texts broadcasted on a given channel. This method is cheap since all that is needed is a computer,

mobile device and some firmware that could be downloaded online for free [32]. On a final note, hackers can study the strength of the defense mechanism at the mobile operators' database servers and try to spot weaknesses. Depending on the degree and potency of such vulnerabilities, the mobile operator might be tricked to provide confidential data or at worst, the hacker might gain access into the system and perform malicious actions on users' data.

In conclusion, all that has been meticulously and comprehensively explained in this section is to create awareness about the status quo of our mobile technology and most importantly, to instigate the drive for reliable and pragmatic solutions to the mobile security flaws.

References

[1] Analog Mobile Phone System; Wikipedia; http://en.wikipedia.org/wiki/Advanced_Mobile_Phone_System.

[2] Marshall Brain, Jeff Tyson and Julia Layton; "How Cell Phones Work" November 14, 2000; HowStuffWorks.com; http://www.howstuffworks.com/cell-phone.htm.

[3] Analog Mobile Phone System; Wikipedia; http://en.wikipedia.org/wiki/Advanced_Mobile_Phone_System.

[4] Mohammad Ghulam Rahman and Hideki Imai; "Security in Wireless Communication"; Journal of Wireless Personal Communications, Volume 22, Number 2, pages 213 – 228, August 2002; Springer Netherlands; http://www.springerlink.com/content/v52101t23m6r241n/fulltext.pdf.

[5] Wayne Jansen, Rick Ayers, "Guidelines on Cell Phone Forensics"; Recommendations of the National Institute of Standards and Technology; NIST Special Publication 800 – 101; May 2007; Sponsored by the Department of Homeland Security & Technology Administration & U.S. Department of Commerce; http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

[6] Code Division Multiple Access, Wikipedia; http://en.wikipedia.org/wiki/CDMA, IS-95, Wikipedia; http://en.wikipedia.org/wiki/IS-95 and CDMA2000, Wikipedia; http://en.wikipedia.org/wiki/CDMA2000.

[7] GSM, Wikipedia; http://en.wikipedia.org/wiki/GSM and 3G, Wikipedia; http://en.wikipedia.org/wiki/3G.

[8] J. Nicholas Hoover; "Black Hat Conference: Security Researchers Claim To Hack GSM Calls"; February 20, 2008; InformationWeek; http://www.informationweek.com/news/mobility/security/showArticle.jhtml?articleID=206800800&cid=RSSfeed_IWK_All.

[9] Yong Li, Yin Chen and Tie-Jun Ma; "Security in GSM"; GSM Security Papers; http://www.gsm-security.net/papers/securityingsm.pdf.

[10] Priyanka Agrawal; "Security of GSM System"; January 10, 2005; Ezine Articles; http://ezinearticles.com/?Security-of-GSM-System&id=8503.

[11] Levent Ertaul and Basar Kasim; "GSM Security", in Proceedings of the 2005 International Conference on Wireless Networks, ICWN'05, June 2005, Las Vegas; http://www.mcs.csuhayward.edu/~lertaul/ICW3016.pdf.

[12] Alexandre Lun-Yut-Fong and Boris Granovskiy; “Security in Mobile Phone Systems”; October 23, 2006; http://www.it.uu.se/edu/course/homepage/sakdat/ht06/assignments/pm/programme/lung-yut-fong-granovskiy.pdf.

[13] GSM; Wikipedia; http://en.wikipedia.org/wiki/GSM#GSM_security.

[14] Jan Pelzl and Thomas Wollinger; “Security Aspects of Mobile Communication Systems”; March 28, 2006; Springer Berlin Heidelberg; Embedded Security in Cars – Part III; pages 167 – 185; http://www.springerlink.com/content/m252663513v31835/fulltext.pdf.

[15] Daniel Mc Keon, Colm Brewer, James Carter and Mark Mc Taggart; “GSM and UMTS Security”; 4BA2 Technology Survey; http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/index.html.

[16] Tektronix, Technical Brief; “UMTS Security Features”; August 2004; http://www.tek.com/Measurement/App_Notes/2F_17826/eng/2FW_17826_0.pdf.

[17] Abdul Bais, Walter T. Penzhorn and Peter Palensky; “Evaluation of UMTS security architecture and services”; in Proceedings of the 2006 IEEE International Conference on Industrial Informatics; 16 – 18 August, 2006; http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4053451&isnumber=4053336.

[18] K. Boman, G. Horn, P. Howard and V. Niemi; “UMTS Security”; in Electronics and Communication Engineering Journal; October 2002; Volume 14, Issue 5, pages 191 – 204; http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1088436&isnumber=23651.

[19] Runar Langnes, Tom E. Aamodt, Trond Friisø, Geir Køien and Øyvind Eilertsen; “Security in UMTS - Integrity” - Kjeller : Telenor Forskning og Utvikling, 2001. - 24 s. - (Telenor FoU ; N 4/2001); http://www.telenor.com/rd/pub/not01/sec_UMTS.PDF.

[20] Pierre Betouin; “UMTS Security”; June 20, 2006; ESIEA : Ecole Supérieure d'Informatique, Electronique-Automatique; http://securitech.homeunix.org/Projets_ESIEA/3G_nw.pdf.

[21] Femtocell; Wikipedia; http://en.wikipedia.org/wiki/Femtocell.

[22] Kevin Mitchell; “Femtocells: Securing the Core-Internet Border”; November 21, 2008; Wireless Week; http://www.wirelessweek.com/Femtocells-Securing-Core-Internet-Border.aspx.

[23] David Chambers; “Femtocell Security over the Internet”; September 19, 2008; ThinkFemtocell; http://www.thinkfemtocell.com/Technology/Femtocell-Security-over-the-Internet.html.

[24] IMSI-catcher; Wikipedia; http://en.wikipedia.org/wiki/IMSI-catcher.

[25] Ulrike Meyer and Susanne Wetzel; “A Man-in-the-Middle Attack on UMTS”; WiSe’04; October 1, 2004; Philadelphia, Pennsylvania, USA; http://www.cs.stevens.edu/~swetzel/publications/mim.pdf.

[26] Olivier Benoit, Nora Dabbous, Laurent Gauteron, Pierre Girard, Helena Handschuh, David Naccache, Stephane Socie and Claire Whelan; “Mobile Terminal Security”; Cryptology ePrint Archive; http://eprint.iacr.org/2004/158.pdf .

[27] The advertisement of XRY at http://www.mediarecovery.pl/en/content/view/81/60/.

[28] The advertisement of Device Seizure v 2.0 at http://www.agapeinc.in/parabendevicesiezure.htm.

[29] The two-phase manual can be found at http://www.paraben-conferences.com/charts/cell_seizure_rules_1.pdf and http://www.paraben-conferences.com/charts/cell_seizure_rules_2.pdf.

[30] The advertisement of Oygen Forensic Suite 2 at http://www.oxygen-forensic.com/en/ and its manual at http://www.oxygen-forensic.com/download/articles/Oxygen_Forensic_Suite_2_-_Getting_started.pdf.
[31] Julie Creswell; “Wal-Mart Says Worker Taped Reporter’s Calls”; March 6, 2007; The New York Times; http://www.nytimes.com/2007/03/06/business/06walmart.html?_r=1.
[32] Christopher Beam; “How Do You Intercept a Text Message?”; March 7, 2007; Slate; http://www.slate.com/id/2161402.

Chapter 4

Legal Aspects of the Privacy of Mobile Phone Users

In this chapter we discuss the privacy of mobile phone users in Canada from a legal perspective. In the first section we discuss the privacy legislation in Canada. Laws and regulations pertaining to the privacy of mobile phone users are given in Section 4.2. Then, Section 4.3 analyzes the privacy laws and regulations in Canada with a particular emphasis on those applied to mobile phone communication. As a comparative analysis, the privacy laws and regulations in the United Kingdom are discussed in Section 4.4. Finally, Section 4.5 analyzes the impact of the Patriot Act in the United States on the privacy of the mobile phone users in Canada.

4.1 Federal Privacy Legislation in Canada (*Privacy Act, PIPEDA, PIPA*)

Canada has two federal privacy statutes- the *Privacy Act* [1] and the *Personal Information Protection and Electronic Documents Act (PIPEDA)* [2].

1. *Privacy Act*

The *Privacy Act* protects the privacy interests of individuals and provides individuals with a right of access to personal information about themselves held by federal government departments and agencies.

The *Privacy Act* has been in effect since July 1, 1983 and imposes obligations on approximately 150 federal government departments and agencies to respect privacy rights of individuals by limiting the federal government's collection, use and disclosure of personal information. Also, the *Privacy Act* gives individuals the right to access and request the correction of personal information held by federal government departments and agencies.

2. *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)

PIPEDA is relatively new legislation and, unlike the *Privacy Act*, applies only to the Canadian private sector. *PIPEDA* applies to organizations that collect, use or disclose personal information in the course of commercial activities. *PIPEDA* sets out the obligations that must

be satisfied when private sector organizations collect, use or disclose personal information in the course of commercial activities. *PIPEDA* gives individuals the right to access their personal information and to request the correction of their personal information held by these organizations.

PIPEDA was released in a series of three stages, each corresponding with what the Act would cover in terms of personal information. Stage one was implemented on January 1, 2001. Stage two began January 1, 2002 and the final stage occurred on January 1, 2004.

Stage One

Since January 1, 2001, *PIPEDA* has been applicable to personal information collected, used or disclosed in the course of commercial activities involving federal works, undertakings and businesses. Personal information included the collection, use or disclosure of employee personal information collected by federally regulated employers. Personal health information was exempted during this stage. Examples of federally-regulated organizations bound by *PIPEDA* include banks, telecommunications and transportation companies.

Stage Two

Since January 1, 2002 *PIPEDA* has been applicable to personal health information related to an individual's mental or physical health and a person's health services.

Stage Three

Since January 1, 2004, *PIPEDA* has been applicable to provincial organizations that collected, used or disclosed personal information in the course of their commercial activities.

Since January 1, 2004, *PIPEDA* has applied to personal information collected, used or disclosed by the retail sector, publishing companies, the service industry, manufacturers and other provincially regulated organizations. However, unlike federally regulated employers, *PIPEDA* does not apply to employee personal information of these provincially regulated organizations.
The federal government may exempt organizations or activities in provinces that have their own privacy laws if they are substantially similar to the federal law. To date the provinces of British

Columbia, Alberta and Quebec have been exempted from the application of *PIPEDA* on the basis that those provinces have substantially similar legislation.

Administration of the *Privacy Act* and *PIPEDA* is the responsibility of the Privacy Commissioner of Canada who is authorized to receive and investigate complaints.

3. Provincial and Territorial Privacy Laws

Every province and territory has privacy legislation governing the collection, use and disclosure of personal information held by government and government agencies. These acts provide individuals with a general right to access their personal information and with the opportunity to request a correction of their personal information.

Administration of provincial and territorial legislation is performed by either an independent commissioner or ombudsman who is authorized to receive and investigate complaints relating to non-compliance with the legislation.

4. Sector Specific Privacy Legislation (PIPA & PIHPA)

Alberta, Saskatchewan, Manitoba and Ontario have passed legislation to deal specifically with the collection, use and disclosure of personal health information held by health care providers and other health care organizations.

Several federal and provincial sector specific laws include provisions dealing with the protection of personal information. The federal *Bank Act* [3], for example, contains provisions regulating the use and disclosure of personal financial information held by federally regulated financial institutions. Most provinces have legislation dealing with consumer credit reporting. These acts typically impose an obligation on credit reporting agencies to ensure the accuracy of the information, place limits on the disclosure of the information and give consumers the right to have access to and challenge the accuracy of the information. Provincial laws governing credit unions typically have provisions dealing with the confidentiality of information relating to members' transactions.

There are a large number of provincial acts that contain confidentiality provisions concerning personal information collected by professionals. Privacy legislation applicable in the provinces of British Columbia, Quebec, Alberta and Ontario include:

1. *An Act Respecting the Protection of Personal Information in the Private Sector* (Quebec) [4];
2. The *Personal Information Protection Act* - PIPA (British Columbia) [5];
3. The *Personal Information Protection Act* - PIPA (Alberta) [6];
4. The *Personal Health Information Protection Act* - PHIPA (Ontario) [7].

4.2 Privacy of Mobile Phone Users: Laws and Regulations

The regulation of the telecommunications industry is the responsibility of the federal government. Mobile phone service providers are required to comply with the *Telecommunications Act* [8]. The *Telecommunications Act* affirms the essentiality of telecommunications within Canada and sets out in section 7 nine prescribed Canadian telecommunication policy objectives. One of the policy objectives contained in the *Telecommunications Act* is "to contribute to the protection of the privacy of persons" [9].

The Canadian Radio-television and Telecommunications Commission (CRTC) is responsible for regulating and supervising telecommunications throughout Canada. The CRTC, through a number of decisions dating back to 1986 have required service providers to comply with confidentiality and disclosure provisions when dealing with their customers[1]. In particular, telecommunication service providers are required to obtain a customer's express consent to

---

[1] These provisions were first set out in *Review of the general regulations of the federally regulated terrestrial telecommunications common carriers*, Telecom Decision CRTC 86-7, 26 March 1986, and amended in Telecom Order CRTC 86-593, 22 September 1986. For all local exchange carriers, the provisions were further amended in *Provision of subscribers' telecommunications service provider identification information to law enforcement agencies*, Order CRTC 2001-279, 30 March 2001 and in *Provision of subscribers' telecommunications service provider identification to law enforcement agencies*, Telecom Decision CRTC 2002-21, 12 April 2002. In *Confidentiality provisions of Canadian carriers*, Telecom Decision CRTC 2003-33, 30 May 2003 (Decision 2003-33), and amended in Telecom Decision CRTC 2003-33-1, 11 July 2003, the Commission expanded the forms of express consent required by Canadian carriers for the disclosure of confidential customer information. (http://www.crtc.gc.ca/eng/).

disclose customer information that they hold except if the disclosure is made to one of the following:

- the customer;
- an agent of the customer;
- another telecommunication provider;
- a telecommunication service related company;
- an agent of the telecommunication provider for the purposes of evaluating a customer's creditworthiness or to collect a debt owed to the telecommunication provider;
- a public authority in circumstances where there is imminent danger to life or property [10].

Customers may file complaints against telecommunications companies to the CRTC when they are concerned about the service provider's handling or disclosure of their personal information. In addition to the privacy provisions contained in the *Telecommunications Act* and the CRTC decisions and orders made thereunder, telecommunication providers are required to comply with the provisions of *PIPEDA*. The privacy obligations contained in the *Telecommunications Act* and the CRTC decisions are generally less restrictive than the privacy principles contained in *PIPEDA*. In circumstances where the *Telecommunications Act* is contradictory to *PIPEDA*, the provisions of *PIPEDA* will overrule [11].

4.3 Analysis of Privacy Laws and Criminal Laws in Canada

In addition to the sector specific *Telecommunications Act*, there are other general federal statutes in Canada designed to protect the privacy interests of individuals. Federal privacy legislation applicable to telecommunications and the use of mobile phone devices that will be reviewed in this section include: the *Criminal Code* [12]; *PIPEDA*; *Canadian Security Intelligence Service Act* [13]; and the right to privacy that is enshrined in the *Constitution Act* [14] of Canada in the *Charter of Rights and Freedoms* [15].

4.3.1 Criminal Code

The *Criminal Code* prohibits the interception of private communications without authorization. Part VI of the *Criminal Code* governs offences relating to interception. The interception of a

private communication is an indictable offence punishable by a prison term of up to five years. Section 184(1) of the *Criminal Code* states:

> **"**184. (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years" [16] [emphasis added]

The terms "electro-magnetic, acoustic, mechanical or other device", "private communication", and "intercept" referenced in s.184 are defined in section 183 of the C*riminal Code* to mean:

> "electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept a private communication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;
>
> "intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof;
>
> "private communication" means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it." [17]

The *Criminal Code* is applicable to crimes that occur within the jurisdiction of Canada. The application of the *Criminal Code* to the interception of a telephone conversation that involves either the originator or the intended recipient being located in the United States is unclear. Based on the definition of "private communication" it seems as though the offence involves "oral" rather than "written" or "text" communications.

Section 184 appears to be contravened if either party to the private communications is physically located in Canada. However, the location of the person intercepting the private communication is not addressed in this section of the *Criminal Code*.

Section 184(2) of the *Criminal Code* sets out a number of statutory exceptions to the interception offence. The effect of subsections 184(2)(a) through (e) is to list all lawful interception activity that is permissible. Subsection 184(2)(a) exempts consent interceptions when either the originator or the intended recipient of the private communication has either implicitly or expressly consented to the interception. Subsection 184(2)(b) exempts a person who intercepts a private communication when that person has obtained judicial authorization. This section also permits the interception of a private communication by a peace officer when judicial authorization has not been obtained when three conditions have been satisfied. Section 184.4 of the *Criminal Code* describes these conditions as:

1. The peace officer believes on reasonable grounds that the urgency of the situation does not allow for the obtaining of an authorization; and
2. The peace officer believes on reasonable grounds that the interception is necessary for the prevention of an unlawful act that would seriously harm a person or property; and
3. Either the originator or the recipient or intended recipient of the private communication would either cause the harm or be the intended victim of the harm [18].

The provisions under Part VI of the *Criminal Code* relating to the interception of private communications apply to the cell phone communications. In response to the judicial debate regarding the application of the interception provisions of section 184 of the *Criminal Code* to radio based cell phone communications the *Criminal Code* was amended. In 1995, section 184.5 was enacted to emphasize that the interception of private communications was equally applicable to unauthorized cell phone interception. Section 184.5 states:

> "184.5(1) Every person who intercepts, by means of any electro-magnetic, acoustic, mechanical or other device, maliciously or for gain, a radio-based

telephone communication, if the originator of the communication or the person intended by the originator of the communication to receive it is in Canada, is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years." [19]

Lawful Interception

The *Criminal Code* permits the interception of private communications in the circumstances outlined below.

1. Consent Interception – Without Judicial Authorization

Section 184.1 of the *Criminal Code* permits a peace officer and an "agent of the state" (a person acting under the authority of and in cooperation with a peace officer pursuant to s. 184.1(4)) to intercept a private communication without judicial authorization in circumstances where participant consent is obtained. In order to comply with s.184.1, three conditions contained in subsections 184.1(a) through (c) must be satisfied. These conditions are summarized as follows:

1. Either the originator or the recipient of the private communication has consented to the interception; and
2. The peace officer or the agent of the state has reasonable grounds to believe that there is risk of bodily harm to the person consenting to the interception; and
3. The purpose of the interception is to prevent the bodily harm from occurring [20].

2. Consent Interception – With Judicial Authorization

Section 184.2(1) provides for judicially authorized consent interceptions of private communications where there are reasonable grounds for a peace officer or public officer to believe that a *Criminal Code* offence or an offence under another federal statute will be committed. A formal application for judicial authorization must be made by either a peace officer or public officer whose duties include the enforcement of the *Criminal Code* or another federal act. The application must be accompanied by an affidavit. Section 184.2(3) sets out

three conditions that must be met in order for a judge to grant the authorization. According to s. 184.2(3), the judge granting the authorization must be satisfied that there are:

1. Reasonable grounds to believe that an offence against the *Criminal Code* or another federal statute has been or will be committed;
2. Either the originator or the recipient of the private communication has consented to the interception; and
3. Information concerning the offence will be obtained through the interception [21].

3. Conventional (60 day) Interception – With Judicial Authorization

Sections 185 and 186 of the *Criminal Code* prescribe conventional (60 day) authorizations and authorization renewals granted by a judicial authority in relation to the offences enumerated under section 183 of the *Criminal Code*. In addition to *Criminal Code* offences, section 183 offences relate to matters concerning bankruptcy, toxic weapons, competition, illegal drugs, corruption, war crimes against humanity, customs and immigration.

According to section 185, a Provincial Attorney General or the Minister of Public Safety and Emergency Preparedness may file an application for an interception. The application must be accompanied with an affidavit from a peace officer or public officer. Section 186 authorizes a judge to allow an interception provided two conditions are met. First, that it would be in the best interests of administrative justice to authorize the interception. Second, that it is a necessary part of the investigation. According to subsection 186(1.1), interceptions relating to criminal organization offences and terrorism offences under the *Criminal Code* do not require the establishment of investigative necessity to receive judicial authorization [22].

4. Emergency Interception – With Judicial Authorization – (36 hours)

Section 188 of the *Criminal Code* allows for the granting of a judicial authorization in circumstances where the urgency of the situation requires interception of the private communication before a conventional section 186 judicial authorization could be obtained. The authorization is only valid for up to a maximum period of 36 hours.

4.3.2 Canadian Security Intelligence Service Act (CSIS Act)

National Security matters require judicial authorization before an individual's privacy may be invaded. The Canadian Security Intelligence Service (CSIS) is a statutory body established pursuant to the *Canadian Security Intelligence Service Act.* The duties and functions of CSIS are set out in section 12 of the *CSIS Act.* Section 12 states:

> **"**12**.** The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada." [23]

Section 21 of the *CSIS Act* allows for application to a federal court judge to issue a warrant to enable CSIS to investigate a threat to the security of Canada where there are reasonable grounds to believe that a warrant is necessary. Although the authorization provisions of the *CSIS Act* are similar to the *Criminal Code*, s. 26 of the *CSIS Act* explicitly states that the interception of the private communication provisions in Part VI of the *Criminal Code* do not apply in relation to interceptions of private communications made pursuant to investigations of national security.

Section 21(2) of the *CSIS Act* set out the conditions that must be satisfied to in order for a warrant to be granted. The applicant must be able to demonstrate on reasonable grounds through affidavit evidence that a warrant is necessary to enable CSIS to investigate a threat to the national security of Canada. Section 21 also requires evidence that shows that other investigative procedures have been tried or are unlikely to succeed and that the urgency of the matter does not allow for the carrying out of the investigation without a warrant.

4.3.3 Charter of Rights and Freedoms- Section 8

In 1982, the *Canadian Charter of Rights and Freedoms* became constitutionally protected. The *Charter* guarantees certain rights of individuals in Canada from the actions of government and protects individuals against unreasonable intrusions by the government.

An individual's right to privacy is enshrined in the *Charter*. Section 8 of the *Charter* guards against unreasonable invasions of privacy by government. Section 8 states that: "Everyone has the right to be secure against unreasonable search or seizure".

Provincial and federal statutes contain provisions which require individuals to comply with the laws and regulations made thereunder. A failure to comply with a statute or regulation can result in the commission of an offence and with the imposition of a penalty ranging from a fine up to imprisonment. Offences may be characterized as either regulatory or criminal in nature and depending upon the classification will afford an individual with either a higher or lower expectation of privacy [24].

A search or seizure conducted by law enforcement pursuant to legislation that is characterized as criminal, such as the *Criminal Code* will result in greater privacy rights than regulatory offences contained in statutes such the *Competition Act* [25] or the *Income Tax Act* [26]. In order for evidence at a criminal trial to be relied upon by the state, the state must be able to demonstrate that the evidence seized resulted from a reasonable search and seizure and was consistent with section 8 of the *Charte*r. Similarly, evidence sought to be admitted in a regulatory offence matters must also be reasonable under section 8 of the *Charter*. However, in regulatory offences the expectation of privacy that an individual may expect to have is lower.

There is a significant amount of Canadian jurisprudence that describes what is meant by a reasonable expectation of privacy as referenced in section 8 of the *Charter*. In *Hunter v. Southam Inc*. [27], the Supreme Court of Canada held that section 8 refers to a balancing of the rights of the state to enforce laws and the individual's right to privacy. The court also determined that section 8 of the *Charter* does not protect against all invasions of privacy by the state. It protects only against an unreasonable invasion of privacy.

In *R.* v. *Edwards* [28], the Supreme Court of Canada expanded upon *Hunter* v. *Southan* and summarized what was meant by a "reasonable expectation of privacy". Justice Cory stated:

> "A review of the recent decisions of this Court and those of the U.S. Supreme Court, which I find convincing and properly applicable to the situation presented

in the case at bar, indicates that certain principles pertaining to the nature of the s. 8 right to be secure against unreasonable search or seizure can be derived. In my view, they may be summarized in the following manner:

…

Like all Charter rights, s. 8 is a personal right. It protects people and not places.

…

The right to challenge the legality of a search depends upon the accused establishing that his personal rights to privacy have been violated…

As a general rule, two distinct inquiries must be made in relation to s. 8. First, has the accused a reasonable expectation of privacy. Second, if he has such an expectation, was the search by the police conducted reasonably…

A reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances. The factors to be considered in assessing the totality of the circumstances may include, but are not restricted to, the following:

(i) presence at the time of the search;
(ii) possession or control of the property or place searched;
(iii) ownership of the property or place;
(iv) historical use of the property or item;
(v) the ability to regulate access, including the right to admit or exclude others from the place;
(vi) the existence of a subjective expectation of privacy; and
(vii) the objective reasonableness of the expectation. …

If an accused person establishes a reasonable expectation of privacy, the inquiry must proceed to the second stage to determine whether the search was conducted in a reasonable manner." [29]

Criminal Case Law- Reasonable Expectation of Privacy- Telephone Conversations

In *R.* v. *Araujo* [30], the Supreme Court of Canada reaffirmed the high expectation of privacy associated with private communications and the intrusiveness of the state when it intercepts telephone conversations. In this regard, Justice LeBel stated the following:

> "...[W]iretapping is highly intrusive. It may affect human relations in the sphere of very close, if not intimate communications, even in the privacy of the home. La Forest J. was alert to the importance of the societal values involved in wiretapping and the risks to essential privacy interests. Writing for the Court, in Duarte, supra, at p. 44, La Forest J. emphasized the potential danger to privacy rights arising from the use of such modern investigative techniques:
>
> > The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in United States v. White, 401 U.S. 745, supra, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known". If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.
>
> 22 An appropriate balance must be found between the need to safeguard privacy interests and the realities and difficulties of law enforcement." [31]

Criminal Case Law- Reasonable Expectation of Privacy- E-Mail/ Text Messages

There is little criminal law jurisprudence dealing with privacy rights an individual may have in mobile phone text messaging. However, given the similarities of email technology with text messaging is reasonable to assume that mobile phone text messages will be treated by the courts in the same fashion as email messages.

It is difficult to reconcile the varying views concerning the reasonable expectation of privacy associated with email messages that have been made by criminal courts across Canada. A review of case law demonstrates that is unclear whether text messages sent and stored on mobile phone devices will be treated like "private communications" within the meaning of section 186 of the *Criminal Code* or like seized documents. General document search warrant provisions are contained in section 487, Part XV of the *Criminal Code*. The judicial authority requirements for the interception of a private communication under s. 186 [32], Part VI of the *Criminal Code* are much more onerous than the general search warrant provisions contained under s. 487 of the *Criminal Code*. Therefore, judicial authority may be easier to obtain in the case of the state obtaining text messages on mobile phones than intercepting the private oral communications that are made on those very same devices.

In *R. v. Weir* [33], the court examined whether e-mail message should be afforded the same level of protection as first class mail or telephone conversations. The court held that emails carry a reasonable expectation of privacy requiring a warrant before they can be seized by law enforcement. The court also determined that much like a regular mail envelope the header text or cover of the email carries a lower expectation of privacy. In *Weir* the court stated:

> "In summary, I am satisfied e-mail via the Internet ought to carry a reasonable expectation of privacy. Because of the manner in which the technology is managed and repaired that degree of privacy is less than that of first class mail. Yet the vulnerability of e-mail requires legal procedures which will minimize invasion. I am satisfied that the current *Criminal Code* and *Charter of Rights* protections are adequate when applied in the e-mail environment." [34]

In 2002, the Federal Department of Justice produced the *Lawful Access- Consultation Document* [35]. The Document outlined the ambiguity associated with the application of the *Criminal Code* to the interception of email. The Document concludes that emails will be afforded different levels of protection depending upon where the email is located in the chain of transmission. Text messages or emails sent from one device to another but unopened remain "private communications" within the meaning of s. 186 of the *Criminal Code*. Also, emails in transit or waiting to be delivered may constitute "private communications". However, the retrieval of a stored email or text message could constitute a seizure of stored information and may be governed by Part XV, section 487 of the *Criminal Code*.

Criminal Case Law- Reasonable Expectation of Privacy- Mobile Phone Records

Case law relating to whether a privacy interest exists in cell phone records is evolving in criminal law. In the recent 2007 case of *R.* v. *MacInnis (2007)* [36], the Ontario High Court of Justice held that the state could not rely upon cell phone records that were seized from the accused's common law partner pursuant to an unlawful warrant.

The court determined that a person who uses a cell phone with the consent of the subscriber to the cell phone service has a privacy interest in the information collected by the service provider. In this case, the data collected by the service provider consisted of the phone numbers that were called. Also, the time and location of the cell phone at the times the calls were made were referenced in the records seized by the police. The court found that *PIPEDA* created an objective expectation of privacy for the subscriber and for those persons whose personal information is contained in the records relating to the subscriber. The court held that the records contained personal and confidential information and required a judicially authorized warrant pursuant to section 186 of the *Criminal Code.* In coming to this conclusion, the court reviewed the provisions of *PIPEDA* to assist with its interpretation of the privacy rights contained in the *Criminal Code* interception provisions.

Prior to *R.* v. *MacInnis*, it was not uncommon for courts not to recognize privacy rights of a third party in cell phone records. In *R.* v. *Pervez* [37] *and R* v. *Fattah* [38], the courts concluded that a

third party user of a cell phone does not have any privacy interest in the records of another subscriber.

4.3.4 Privacy Act and *PIPEDA*

The *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* are two federal Canadian statutes governing the privacy rights of individuals in Canada.

As stated in the previous section, the *Privacy Act* governs the manner in which the federal government and federal agencies collect, use and disclose personal information and provides individuals with the right to access government held personal information. The *Privacy Act* is not applicable to circumstances involving personal information that is held by telecommunications companies.

PIPEDA applies to federal works, undertakings or business. Telecommunication companies are considered to be federal works, undertakings or business with the meaning of *PIPEDA* [39].
The object of *PIPEDA* is to prescribe rules that will govern the manner in which private sector organizations collect, use and disclose "personal information". Section 3 of *PIPEDA* states the following in relation to its purpose:

> "3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." [40]

Individuals alleging that *PIPEDA* has been violated may file complaints with the Office of the Privacy Commissioner of Canada (OPC). *PIPEDA* complaints made against telecommunication companies tend to involve allegations that an individual's personal information was collected, used or disclosed without the individual's consent and/or that an organization has failed to protect an individual's personal information from unauthorized disclosure.

"Personal Information" is defined in section 2 of *PIPEDA* to mean the following:

> "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." [41]

Principle 4.3, Schedule 1 of *PIPEDA* addresses the requirement to obtain individual consent for the collection, use and disclosure of personal information. Principle 4.3 states:

> "4.3 Principle 3 - Consent
>
> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
>
> Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.
>
> 4.3.1
>
> Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).
>
> 4.3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes.” [42]

Principle 4.7, Schedule 1 of *PIPEDA* requires an organization to implement appropriate safeguards to protect personal information from unauthorized access or disclosure. It states:

“4.7 Principle 7 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include:

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3) [43].

PIPEDA Case Summaries

The Privacy Commissioner of Canada has held that telephone conversations, email messages, and cell phone records [44] are considered to be "personal information" for the purposes of *PIDEDA*. Consequently, mobile phone service providers are required to comply with the provisions of *PIPEDA*. *PIPEDA* cases involving telephone monitoring and disclosure of phone records and the principles involving consent and unauthorized disclosure are reviewed below.

In *PIPEDA Case Summary #51* [45], a customer filed a complaint against his bank when he learned that the telephone conversation he had with his bank representative was recorded. The complainant alleged that Principle 4.3 of Schedule 1 was breached because the bank had not obtained his consent prior to recording the phone call. The Commissioner determined that the complaint was not well founded because the complainant had signed a service agreement that referenced the practice of the bank recording telephone banking transactions. The Commissioner found that the agreement constituted consent within the meaning of 4.3. Also, the bank was able to demonstrate that prior to recording the call, the bank representative informed the complainant that the calls would be recorded.

PIPEDA Case Summary #86 [46] involved another complaint against a bank. In this case, a customer calling in relation to a loan application was not advised that the call was being recorded until the end of the call. The Commissioner examined Principle 4.3 and determined that it would

be reasonable for a customer to be advised at the beginning of the call that the call would be recorded. Prior notification would provide the customer the opportunity to consent to the recording.

In response to this complaint, the OPC developed the *Guidelines for Recording Customer Telephone Calls* [47]. The Guidelines underscore the OPC's position that the monitoring of phone calls constitutes a collection of personal information and except in special circumstances, consent must be provided prior to the collection. Furthermore, the OPC stated that recording of telephone calls should not occur unless it is for a purpose that a reasonable person would consider appropriate in the circumstances.

In a 2003 complaint, the Privacy Commissioner held that a telecommunications company's monitoring of customer calls constituted a collection of information within the meaning of *PIPEDA*, however consent was not required to record the calls. In *PIPEDA Case Summary #160* [48], very little personal information was disclosed during a telephone conversation. This complaint arose from the collection and monitoring of two types of telephone calls. One type of call that was monitored was directory assistance type calls where the customer disclosed the city, name and street address of the person whose listing was being requested. The second type of call involved completing calls for customers where the name and number of the person being called was disclosed by the customer to the operator. The Privacy Commissioner concluded that monitoring live calls when the operator is engaged in side-by-side coaching with a supervisor was collecting personal information within the meaning of *PIPEDA*. The Commissioner found that it did not matter that the personal information disclosed was publicly available information. Notwithstanding that personal information was being collected, the Commissioner determined that consent was not required and that customers did not have to be informed that supervisors were monitoring calls. In dismissing the complaint, the Commissioner determined that the supervisors were focusing their attention on coaching the operators to provide the service and not on what the customer was saying.

In *PIPEDA Case Summary #180* [49], the Commissioner determined that a complaint was well founded when a bank failed to obtain consent prior to taping a telephone conversation as

required by Principle 4.3. The Commissioner also determined that the bank had failed to protect the complaint's personal information with appropriate safeguards when the bank had allowed a third party to overhear the details of his telephone bank transaction. The bank advised the customer that the calls might be recorded for customer quality purposes, however, the customer was not told that the recording could be used for training purposes by bank employees. The Commissioner found that Principle 4.3 was not complied with because the bank had not obtained consent to record the conversation for training purposes.

The Commissioner held that Principle 4.7 relating to adequate safeguards had also been breached since the bank had disclosed the customer's personal information to a third party. The Commissioner determined that notwithstanding the inadvertence of the disclosure, the bank had failed to protect the customer's personal financial information from disclosure to a third party. This inadvertent disclosure was contrary to Principle 4.7.

In *PIPEDA Case Summary #137* [50], the Commissioner determined that a cell phone company had complied with Principle 4.7 notwithstanding an unauthorized access to the complainant's cell phone account records. In this case, the complainant's cell phone account was protected by two passwords. The complainant's estranged husband was able to create a profile and impersonate the complainant without knowing the account passwords. The Commissioner found that the husband likely gained access to an account statement located in the complainant's home and was able to access the account using the account information contained in the statement. The Commissioner held that there was nothing the company could have done to protect the complainant's information in the circumstances.

In a later case involving access to an estranged spouse's cell phone records (*PIPEDA Case Summary # 329)* [51], the Commissioner held that the complaint was well founded and that the company could have done a better job protecting the complainant's personal information. In this case, the complaint was resolved because the company developed a password protection policy on the accounts to prevent a person with sufficient general information from impersonating the actual customer and accessing customer accounts.

In *PIPEDA Case Summary #372* [52], complaints were filed against 3 telecommunications companies- Bell, TELUS Mobility and Fido. This case involved the disclosure of telephone records of telephone calls made by the Privacy Commissioner of Canada, Jennifer Stoddart, from her home telephone, office blackberry and cell phone. The investigation by the OPC showed no evidence that the systems of the companies had been hacked. Social engineering techniques were used by individuals to gain access to personal information through customer service agents of the companies.

TELUS argued that the information that was disclosed was not "personal information" within the meaning of *PIPEDA*. The Assistant Commissioner disagreed and held that the cell phone records contained personal information since it showed a calling history. In this regard, the Assistant Commissioner's findings were summarized as follows:

- The Act makes no distinction between personal information and business information. Who an employee chooses to call while at work, including personal calls, is that individual's personal information.
- What was at issue in the complaint is not the employee's cell phone number but her entire calling history.
- An employee's calling history is not the tangible result of his or her work but represents the manner in which that employee does his or her work in order to achieve a work-product. As such, the calling history should be considered personal information "about" that employee.
- The fact that TELUS Mobility did not disclose the personal information of the person requested does not mean that TELUS Mobility did not disclose information about an identifiable individual. Even though the name of the BlackBerry holder was not expressly released together with her call record does not mean that the individual could not be identified. Had Locatecell.com or the journalist (or anyone else for that matter) called everyone on the call record list, there was indeed a serious possibility that they would be able to piece together enough information so as to eventually be able to ascertain the correct identity of the BlackBerry

holder. Therefore, the call record when taken in its entirety in the present context was information about an "identifiable" individual."

- There was no disputing that TELUS Mobility disclosed to Locatecell.com the call records associated with the Office employee's BlackBerry without her knowledge or consent, contrary to Principle 4.3. The disclosure occurred because the CCR did not verify that the caller requesting the information had the authority to obtain the information.
- Furthermore, at the time, TELUS Mobility did not have procedures in place to address the scenario that led to the disclosure, in contravention of Principle 4.7 and 4.7.1. TELUS has since changed its procedures.
- The Assistant Commissioner pointed out that other factors in the disclosure were the inexperience of the CCR and the fact that the tactics employed by information brokers were not covered in her training. CCRS have since been issued several bulletins on tactics used by brokers.
- TELUS Mobility also took a number of other steps to prevent such disclosures from occurring in the future [53].

In concluding, the Assistant Commissioner held that all three complaints were well founded and resolved since the companies had taken measures to guard against future occurrences.

The foregoing *PIPEDA* case summaries support the conclusion that telephone and mobile phone conversations clearly fall within the definition of "personal information" within the meaning of *PIPEDA*. Mobile phone service providers are required to ensure that mobile phone communications are safeguarded against unauthorized interception. Similarly, mobile phone records show a calling history and classify as personal information within the meaning of *PIPEDA*. Mobile phone records can only be disclosed with an individual's consent and must also be protected by service providers against unauthorized disclosure. Therefore, mobile phone customers must be afforded all the protection contained within *PIPEDA*.

Collection, Use, Disclosure of Personal Information - Without Consent

In this section, the provisions of *PIPEDA* dealing with an organization's collection, use and disclosure of personal information without an individual's consent are reviewed.

PIPEDA contains exceptions to the general rule that consent for the collection, use or disclose of personal information must be obtained. Principle 4.3 of Schedule 1 states that consent is not required where obtaining the consent of the individual would be inappropriate. The Note to Principle 4.3 states the following:

> "Principle 4.3 — Consent
>
> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
>
> Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information." [54]

Subsections 7(1) through (3) of *PIPEDA*, elaborate on the meaning of Principle 4.3 by specifying circumstances when an organization's collection, use or disclosure of personal information is permitted without obtaining consent.

Subsection 7(1) [55] permits organizations to collect personal information without consent in the following circumstances:

- the collection is in the interest of the individual and there is insufficient time to obtain consent (s.7(1)(a));
- the collection is reasonably necessary for the investigation of a breach of an agreement or contravention of federal or provincial laws and there are reasonable grounds to believe that knowledge or consent would compromise the information (s.7(1)(b));
- the collection is solely for journalist, artistic or literary purposes (s.7(1)(c));
- information is publicly available and referenced in the regulations to *PIPEDA* (s.7(1)(d));
- the collection is made for national security purposes (s.7(1)(e));
- the collection is required by law (s.7(1)(e)).

According to subsection 7(2) [56] organizations may use personal information without an individual's consent in the following circumstances:

- in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention or potential contravention of provincial laws, federal laws of Canada, or a foreign jurisdiction and the information is used for the purpose of investigating that contravention (s.7(2)(a));
- it is used in an emergency situation that could impact the life, health or security of an individual (s.7(2)(b));
- it is used for statistical, or scholarly study or research purposes that cannot be achieved without using the information (s.7(2)(c));
- information is publicly available and referenced in the regulations to the *PIPEDA* (s.7(2)(c.1));
- the collection is in the interest of the individual and there is insufficient time to obtain consent (s.7(2)(d));
- the collection is reasonably necessary for the investigation of a breach of an agreement or contravention of federal or provincial the laws and there are

reasonable grounds to believe that knowledge or consent would compromise the information (s.7(2)(d));

- the collection is made for national security purposes (s.7(2)(d));
- the collection is required by law (s.7(2)(d)).

Subsection 7(3) [57] states that "an organization may disclose personal information without the knowledge or consent of the individual" in the following circumstances:

- the disclosure is made to a legal representative of the organization (s.7(3)(a));
- the disclosure is made for the purposes of collecting a debt owed by the individual to the organization (s.7(3)(b));
- the disclosure is required to be disclosed pursuant to a subpoena or warrant made by a court or person with the authority to compel the production of information or records (s.7(3)(c));
- the disclosure is made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that:

    - it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;
    - the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
    - the disclosure is requested for the purpose of administering any law of Canada or a province (s.7(3)(c.1)); or
    - the disclosure is made to the government institution pursuant to *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (s.7(3)(c.2));

- the disclosure is made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization;

    - has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
    - suspects that the information relates to national security, the defence of Canada or the conduct of international affairs (s.7(3)(d));

- the disclosure is made an emergency situation that could impact the life, health or security of an individual (s.7(3)(e));
- the disclosure is made for statistical, scholarly study or research (s.7(3)(f));
- the disclosure is made to conserve records of historic or archival importance (s.7(3)(g));
- the disclosure is made the earlier of:

    (i) 100 years after record was created; or
    (ii) 20 years after death of individual the personal information was about (s.7(3)(h));

- the disclosure of information that is publicly available per the regulations (s.7(3)(h.1));
- the disclosure is made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of federal or provincial laws (s.7(3)(h.2)); or
- the disclosure required by law (s.7(3)(i)).

The language relating to an organization's ability to disclose personal information is permissive meaning that an organization has the discretion to determine whether it will disclose the information. For the most part, this is understandable given the clarity surrounding the circumstances that are enumerated in s. 7(3). However, there is some ambiguity associated with the disclosure of information for law enforcement or national security purposes under s. 7(3)(c.1). The discretionary authority afforded to an organization in subsection 7(3)(c.1) places an organization in a position where it is required to consider and weigh the privacy rights of an individual and the interests of a government institution requesting the disclosure of personal information in the absence of a court order or warrant.

Section 29 of *PIPEDA* requires the Committee of the House of Commons to conduct a statutory review of *PIPEDA* every five years. In May 2007, the Committee issued a Report recommending twenty-five changes to *PIPEDA.* Two of those recommendations related to the amendment of s. 7(3)(c.1).

The Committee reported that concerns were raised during the consultation process with respect to the meaning of "government institution" and "lawful authority". The Committee also reported that it was unclear whether the reference to government institutions in s. 7(3)(c.1) was intended to apply to municipal, provincial, territorial, federal and non-Canadian entities. The Committee recommended that these terms be clarified.

Other concerns that were cited in the Report involved the reference to lawful authority and the discretionary power given to organizations to release personal information without consent of the individual. The Committee reported that it was clear that the lawful authority referenced in s. 7(3)(c.1) was less than the judicial authority of a court order or warrant as referenced in s. 7(3)(c). The Committee recommended that in addition to defining what is meant by "lawful authority" the word "may" in the opening part of s. 7(3) be changed to "shall" making disclosure by the organization to a government institution mandatory rather than discretionary.

In July 2007, the Office of the Privacy Commissioner of Canada responded to the Report of the Committee and supported many of the 25 Committee recommendations [58]. In particular, the

OPC supported the defining of the terms “lawful authority” and “government institution”. However, the OPC did not support the Committee’s recommendation that s. 7(3)(c.1) be changed to make disclosure by organizations mandatory rather than discretionary in relation to issues involving national security and law enforcement. Jennifer Stoddart, Privacy Commissioner of Canada, stated in OPC’s response to the Report that to make such a change would represent “a further step backwards from the amendment that was crafted in 2000 to maintain the *status quo* for law enforcement to request “pre-warrant” information from organizations. I believe that the discretion whether or not to disclose should be left with the organization.” [59]

In Government’s response to the Committee’s report, Government adopted the views of the Privacy Commissioner of Canada [60]. Government stated that it recognized the benefits of providing clarity around the terms “lawful authority” and “government institution” and agreed to define these terms. Government did not agree to adopt the Committee’s recommendation that s. 7(3)(c.1) become a mandatory provision. Instead, Government stated that the clarification of the term “lawful authority” would provide organizations and individuals with guidance on the when personal information ought to be disclosed without consent.

The sharing of personal information with law enforcement and the retention of the discretionary power of the organization was considered in a report prepared by the Centre for Innovation Law and Policy in March 2008 [61]. The report recommended that s. 7(3)(c.1) be refined to allow police to request information from organizations without a warrant pursuant to tailored legislative provisions. These tailored provisions would relate to serious crimes and crimes of such a nature that the inability of the state to access the information would foreclose the investigation. Finally, the report recommended that the discretionary power be specific to types of information that has a low expectation of privacy [62].

4.4 Privacy Laws and Regulations of the United Kingdom

In the United Kingdom there is no general protection of privacy at common law, rather the right to privacy in certain personal matters. Protection of personal confidence has been extended to include not only family and domestic matters but also to recreational activities and the right to

avoid unsought publicity [63]. It should be noted that protection will not be provided to conduct that is grossly immoral[2] [64] or otherwise contrary to public policy [65].

Privacy in the United Kingdom is governed primarily by the *Data Protection Act 1998 (DPA)* [66]. It is the main piece of legislation that governs the protection of personal data and provides a way in which an individual can enforce control of information about themselves. The *DPA* in the U.K. is equivalent to Canada's *PIPEDA.*

There is other legislation in the U.K. that impact an individual's right to privacy. These include *The Privacy and Electronic Communications Regulations* [67], the *Interception of Communications Act 1985* [68] and the *Regulation of Investigatory Powers Act 2000* [69].

Data Protection Act (DPA)

The purpose of the *DPA* is to make new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The *DPA* implements the Data Protection Directive [70] whose purpose is to harmonise the data protection legislation through the European Union in an attempt to protect the fundamental rights and freedoms of the individual, with particular emphasis on the right to privacy and the processing of personal information [71]. The *DPA* applies only to information which falls within the definition of 'personal data' defined in s. 1(1) of the *DPA* as data which relate to a living individual who can be identified from data or other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes expressions of opinion about the individual or intentions in respect of the individual.

Contained as a schedule to the *DPA* are eight Data Protection Principles that data controllers must comply with in order to protect the personal information of individuals. These principles

---

[2] The interests of justice may dictate that the disclosure of confidential information is ordered also where illegality is set up as a defence in a civil action, but only if the information is relevant to the issues which need to be tried, and with due regard paid to the interests of parties to the action and of third parties who would be affected by the disclosure: *Toussaint v. Mattis* (22 May 2000) Lexis, CA.

prohibit the processing of personal data except if specific criteria are met and then the processing of that information must be done in accordance with the lawful rights of the individual [72].

The *DPA* accords certain rights to the individuals which include the right to access their personal information, the right to prevent processing of that information if there is a likelihood that doing so may cause damage or distress to them, the right to prevent the use of that personal information for direct marketing purposes and the *DPA* provides remedies in the event of a breach of an individual's rights under the *DPA* [73]. Remedies can include the right to request an assessment to ensure the personal information is being used appropriately and in compliance with the *DPA*, compensation for non-compliance, rectification on the process, blocking of the personal information and the erasure and destruction of the personal information [74].

There are certain notable exemptions, s. 28 National security; s. 55 Unlawful obtaining of personal data; s. 29 Crime and taxation; and s. 36 Domestic purposes.

The *DPA* establishes an office of Data Protection Registrar that is required to maintain a register of all data users and is given the power to review and if appropriate reject applications for registration. The Registrar also has the authority to monitor and enforce compliance of the Data Protection Principles and in the event of non-compliance criminally prosecute [75].

It is an offence under the *DPA f*or any unregistered person to hold personal data and as a result strict liability is imposed. Personal liability can also be imposed on directors or managers or any person acting in that capacity for any offence committed under the *DPA* [76].

It is an offence to unlawfully obtain personal date (s. 55) and it is a criminal offence to require an individual to make a Subject Access Request relating to cautions or convictions for the purposes of recruitment, continued employment of the provision of services, (s. 56).

Privacy and Electronic Communications (EC Directive) Regulations 2003

This legislation sets out rules for people who wish to send electronic communication for direct marketing purposes, for example, email and text messages. This legislation has made it unlawful

to transmit an automated recorded message for direct marketing purposes via telephone, without the prior consent of the subscriber and the identity of the caller must be provided. Unsolicited marketing material sent by electronic mail, which includes texts, picture message and emails, must only be sent if the individual has asked to receive them. The individual must always be given the opportunity to decline receiving electronic mail.

The Information Commissioner's Office in the U.K. has the legal authority to ensure compliance with the regulations by all organizations in the U.K. The Provider of a public electronic communications service must take appropriate technical and organizations measures to safeguard the security of its service [77] and any individual that suffers damage by way of non-compliance with the Regulations is entitled to bring proceedings for compensation against the person that has caused the damage [78].

A Directive of the European Parliament concerning the processing of personal data and the protection of privacy in the electronic communications sector has recognized the advancement of digital technologies that give rise to specific requirements concerning the protection of personal information of its users. Today, access to digital mobile networks has become available and largely affordable for the public. These networks have the large capacity to process personal information and the confidence of the users that their privacy is not at risk will determine the success of the cross-border development of these services [79].

This Directive does not address the protection of an individual's fundamental rights and freedoms, as a result it does not interfere with the existing balance between an individual's rights to privacy and the possibility of the State having to take measures necessary to protect public security, defence, the economic well-being of the State and the enforcement of criminal law [80]. The caveat being that "measures taken must be appropriate and strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to the safeguards in accordance with the European Convention for the protection of Human Rights and Fundamental Freedoms." [81]

Finally, this Directive holds that all member States must ensure the confidentiality of communications by way of a public communications network and public ally available communications services, through national legislation. This would entail the prohibition of "listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned." [82]

Interception of Communications Act (ICA)

The *Interception of Communications Act (ICA)* [83] created a new provision for and in connection with the interception of communications sent by post or by means of public telecommunication systems and to amend s. 45 of the Telecommunications Act. It is very simplistic in that the following are the only applicable provisions to communications sent by post or by means of a public telecommunications system, as described in the section directly above.

Prohibition on interception

1.-(1) Subject to the following provisions of this section, a person who intentionally intercepts a communication in the course of its transmission by post or by means of a public telecommunication system shall be guilty of an offence and liable

a. on summary conviction, to a fine not exceeding the statutory maximum;
b. on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

(2) A person shall not be guilty of an offence under this section if-

a. the communication is intercepted in obedience to a warrant issued by the Secretary of State under section 2 below; or
b. that person has reasonable grounds for believing that the person to whom, or the person by whom, the communication is sent has consented to the interception.

(3) A person shall not be guilty of an offence under this section if-

a. the communication is intercepted for purposes connected with the provision of postal or public telecommunication services or with the enforcement of any enactment relating to the user of those services; or

b. the communication is being transmitted by wireless telegraphy and is intercepted, with the authority of the Secretary of State,

for purposes connected with the issue of licences under the Wireless Telegraphy Act 1949 or the prevention or detection of interference with wireless telegraphy.

Regulation of Investigatory Powers Act (RIPA)

The *Regulation of Investigatory Powers Act 2000 (RIPA)* [84] puts a regulatory framework around a range of investigatory powers in the United Kingdom. This is done to ensure the powers are used lawfully and in a way that is compatible with the European Convention on Human Rights. It also requires, in particular, those authorising the use of covert techniques to give proper consideration to whether their use is necessary and proportionate. This legislation appears to share characteristics of the *Canadian Security Intelligence Service Act* in its purpose. The difference in *RIPA* is that is does not draw a distinction between private and public communication.

According to the Office for Security and Counter Terrorism, RIPA *regulates the following areas:*

- The interception of communications (for instance, the content of telephone calls, e-mails or postal letters)
- The acquisition and disclosure of communications data (information from communications service providers relating to communications)
- The carrying out of covert surveillance
    - in private premises or vehicles (‘intrusive surveillance’) or
    - in public places but likely to obtain private information about a particular person (‘directed surveillance’)
- The use of covert human intelligence sources (such as informants or undercover officers)
- Access to electronic data protected by encryption or passwords.

RIPA provides a number of important safeguards as it strictly limits the people who can lawfully use covert techniques, the purposes for and conditions in which they can be used and how the material obtained must be handled; it reserves the more intrusive techniques for intelligence and law enforcement agencies acting against only the most serious crimes, including in the interests of national security; and it provides for the appointment of independent oversight Commissioners and the establishment of an independent tribunal to hear complaints from individuals who believe the techniques have been used inappropriately. [85]

These Regulations authorize certain interceptions of telecommunication communications which would otherwise be prohibited by s. 1 of *RIPA*. The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions) for purposes relevant to that person's business and using that business's own telecommunication system.

Interceptions are authorised for monitoring or recording communications - to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training), in the interests of national security (in which case only certain specified public officials may make the interception), to prevent or detect crime, to investigate or detect unauthorised use of telecommunication systems or, to secure, or as an inherent part of, effective system operation; monitoring received communications to determine whether they are business or personal communications; monitoring communications made to anonymous telephone help lines.

Interceptions are authorised only if the controller of the telecommunications system on which they are affected has made all reasonable efforts to inform potential users that interceptions may be made. The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented: they are not prohibited by the Act.

In a news release on October 20, 2008, the UK's Regulation of Investigatory Powers Act did not receive a formidable review. In fact, the article was entitled, "Your Privacy is an illusion: UK

attacks civil liberties". To quote journalist, Peter Bright, "the UK government continues to undermine its citizens' civil liberties, using everyone's favourite bogeyman, the threat of terrorism, to justify its actions." [86]

This article criticizes the legislation stating that it has made it a "criminal offence to refuse to decrypt almost any encrypted data residing within the UK if demanded by authorities as part of a criminal investigation." [87]

Finally, the article reports that even within Parliamentary Home Office there has been backlash. A memo leaked to the Sunday Times expressed grave misgivings about the plans among senior Home Office officials; the database was decried as "impractical, disproportionate, politically unattractive and possibly unlawful from a human rights perspective". [88]

U.K. Privacy Law and Mobile Phone Users

There is no specific piece of legislation in the U.K. that speaks directly to the use of mobile phones and private communications. The *DPA* being the *PIPEDA* equivalent in the U.K. does its part to ensure the protection of personal information, provide access to personal information and limit the use of personal information. There are both civil and criminal sanctions for non-compliance with the *DPA*, as there are with *PIPEDA* and the *Criminal Code* respectively, in Canada.

The *Privacy and Electronic Communications Regulation* along with the *ICA* govern specifically the sending of electronic communications for direct marketing purposes in the U.K., which would be covered by *PIPEDA* in Canada. There are no specific provisions in either of the U.K. legislation for mobile phone usage or private communications. Distinctions are drawn between public communications systems and private communications systems, but again with specific reference to the receipt of direct marketing.

The major difference in the governing law of privacy in the U.K. as opposed to Canada is the broad scope of *RIPA.* Based on a review of the legislation is appears that Government Bodies will be able to access any information or communications, whether over a public or private

communications system, with very little trouble. This is different than the onerous conditions imposed on Government Bodies in Canada as can be seen in both the *PIPEDA* and *Criminal Code* provisions.

4.5 *USA Patriot Act* and its Impact on the Privacy of Mobile Phone Users In Canada

In response to the events of September 11, 2001, the United States enacted legislation entitled the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001 (USA Patriot Act)* [89].

The passage of the *USA Patriot Act* reduced the procedural hurdles that US law enforcement agencies and government had to overcome to obtain access to personal information held by organizations in the United States.

In Canada, it is not uncommon for organizations to outsource processing services to an American firm. To date, the Privacy Commissioner of Canada has addressed three privacy complaints relating to the *USA Patriot Act*. In all three cases, the Privacy Commissioner of Canada determined that the complaints were unfounded. A summary of these cases are provided in this section.

In *PIPEDA Case Summary #313* [90], the Office of the Privacy Commissioner received a number of complaints against CIBC when CIBC had notified its customers that VISA accounts would be processed and stored in the United States and that personal information could be accessed by US law enforcement, US Government, and/or law enforcement and regulatory agencies through the laws of the United States. The complainants alleged that the transfer of this personal information breached Principles 4.1.3 and 4.8, Schedule 1 of *PIPEDA*. Principle 4.1.3 states:

> "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party." [91]

Principle 4.8 of *PIPEDA* states:

> "4.8 Principle 8 – Openness
>
> An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
>
> 4.8.1
>
> Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.
>
> 4.8.2
>
> The information made available shall include
>
> (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
>
> (b) the means of gaining access to personal information held by the organization;
>
> (c) a description of the type of personal information held by the organization, including a general account of its use;
>
> (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
>
> (e) what personal information is made available to related organizations (e.g., subsidiaries).
>
> 4.8.3
>
> An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number." [92]

The Assistant Commissioner found that *PIPEDA* does not prohibit the transfer of personal information to service providers outside of Canada since *PIPEDA* contains provisions that address the protection of the personal information while being held by that third party. In *PIPEDA Case Summary #394* [93], the following findings concerning the transfer of personal information to a third party outside Canada were summarized:

- While the Act does not prohibit the use of foreign-based third-party service providers, it does oblige Canadian-based organizations to have provisions in place, when using third-party service providers, to ensure a comparable level of protection;
- In keeping with its obligations under Principle 4.1.3 of the Act and in accordance with OSFI's guidelines (which are also consistent with this Principle), CIBC has in place a contract with its third-party service provider that provides guarantees of confidentiality and security of personal information;
- The contract allows for oversight, monitoring, and an audit of the services being provided. CIBC maintains custody and control of the information that is processed by the third-party service provider;
- The Assistant Commissioner noted, however, that while customer personal information is in the hands of a foreign third-party service provider, it is subject to the laws of that country and no contract or contractual provision can override those laws;
- In short, an organization with a presence in Canada that outsources the processing of personal information to a U.S. firm cannot prevent its customers' personal information from being lawfully accessed by U.S. authorities;
- Furthermore, even if one were to consider the issue of "comparable protection" from the perspective of U.S. versus Canadian anti-terrorism legislation, it was clear to the Assistant Commissioner that there is a comparable legal risk that the personal information of Canadians held by any organization and its service provider — be it Canadian or American

— can be obtained by government agencies, whether through the provisions of U.S. law or Canadian law;

- The Assistant Commissioner therefore determined that CIBC was in compliance with Principle 4.1.3;
- She went on to reaffirm this Office's publicly stated position: that, at the very least, a company in Canada that outsources information processing to the United States should notify its customers that the information may be available to the U.S. government or its agencies under a lawful order made in that country;
- In keeping with this direction, CIBC notified its customers of the risk that their personal information might be accessed under the provisions of the *USA PATRIOT Act* whilst in the hands of a U.S.-based third-party service provider;
- Thus, by providing such information, the bank was informing its customers about its policies and practices related to the management of their personal information, in accordance with Principle 4.8;
- In the Assistant Commissioner's view, the real concern underlying these complaints is the prospect of a foreign government accessing Canadians' personal information;
- She concluded, however, that the Act cannot prevent U.S. authorities from lawfully accessing the personal information of Canadians held by organizations in Canada or in the United States, nor can it force Canadian companies to stop outsourcing to foreign-based service providers. What the Act does demand is that organizations be transparent about their personal information handling practices and protect customer personal information in the hands of foreign-based third-party service providers to the extent possible by contractual means. This Office's role is to ensure that organizations meet these requirements. In the case of these complaints, these requirements have been met [94].

In 2007, the OPC investigated a complaint involving personal information that was transferred to the United States for the processing of money orders. In *PIPEDA Case Summary 365* [95], the Assistant Privacy Commissioner held that the complaints were not founded. The Assistant Privacy Commissioner reviewed the contract between the Canadian banks and the US process company and concluded that principle 4.1.3 was complied with because the US company offered a comparable level of protection to that of its Canadian counterparts. The Assistant Privacy Commissioner re-stated the earlier findings of the Office of the Privacy Commissioner in *PIPEDA Case Summary #313* and that Canadian companies that outsource services cannot shield Canadian customers from the laws of the country where the information is held. Consequently, privacy information of Canadians that is held in the United States for processing is subject to interception by US Government and law enforcement agencies in accordance with the laws of that country.

In 2008, in *PIPEDA Case Summary #394* [96], the Privacy Commissioner investigated a complaint concerning the outsourcing of email services to a US based firm. The complainants alleged that they did not have the opportunity to consent to the transfer of the information to the US service provide and that appropriate safeguards were not put in place to protect personal information held by the US firm.

The Assistant Privacy Commissioner dismissed the complaint and held that the subscribers were informed in advance that the services were being transferred to the US and were provided with the opportunity to accept or reject the terms of service. With respect to the allegation that comparable protection was not provided, the Assistant Privacy Commissioner held that a contractual review demonstrated that the US firm was obligated to provide a level of protection that was contained in *PIPEDA*.

In January, 2009, the Office of the Privacy Commissioner released Guidelines to explain how *PIPEDA* applied to the transfer of personal information to a third party operating outside Canada [97].

In the Guidelines, the OPC clarified the meaning of Principle 4.1.3, Schedule 1 of *PIPEDA*. The Office of the Privacy Commissioner stated that Principle 4.1.3 does not distinguish between domestic and international transfer of personal information. The Office of the Privacy Commissioner states that "transfer" is a use by the organization and that *PIPEDA* is applicable. According to the Guidelines, an example of transfer of information is the outsourcing of a process to a third party such as IT support for processing payments to customers.

According to the Guidelines, "processing" under *PIPEDA* is interpreted to include any use of the information by the third party processor for a purpose for which the transfer organization can use it. Finally, the Guidelines state "a comparable level of protection requires the third party processor to provide protection that can be comparable to a level of personal information that would be received if it had not been transferred [98]." The Office of the Privacy Commissioner states that organizations must ensure that personal information is protected through contract and that the organization must be satisfied that effective security measures are in place to protect personal information from unauthorized use and disclosure.

The Guidelines re-state the previous findings of the OPC that the organization cannot override the laws of foreign jurisdictions. Finally, the Office of the Privacy Commissioner states that organizations need to make it plain to individuals that their information may be processed in a foreign country and that it may be assessable to law enforcement and national securities of that jurisdiction to comply with the openness requirement referenced in Principle 4.8.

The *USA Patriot Act* has implications for Canadian mobile phone users and service providers since "personal information" is processed in the United States. Mobile phone users in Canadian cities close to American borders (such as Windsor, Ontario and Vancouver, British Columbia) are at risk of having their signals intercepted on the American side of the border from a technical viewpoint. Mobile phone private communications are susceptible to interception by law enforcement in the United States in accordance with the laws of the United States.

Similarly, Canadians using their mobile phones while visiting the United States are creating data history records with American service providers that are "processing" their mobile phone calls.

These records are subject to disclosure in accordance with American laws. An interesting situation arises when one mobile phone user is situated in the United States and the other is situated in Canada since the privacy laws of both countries are potentially applicable.

References

[1] Privacy Act, R.S.C. 1985, c. P-21.

[2] Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5.

[3] Bank Act, S.C. 1991, c. 46.

[4] An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. Chapter P-39.1.

[5] Personal Information Protection Act, S.B.C. 2003, c. 63.

[6] Personal Information Protection Act, S.A. 2003, c. P-65.

[7] Personal Health Information Protection Act, 2004, S.O. 2004, c. 3.

[8] Telecommunications Act, S.C. 1993, c. 38.

[9] Ibid., s.7(i).

[10] Telus Service Terms and Conditions (http://www.telusmobility.com/nf/webactivation/terms_conditions_post.shtml); Also see: Aliant Telephone Book - White Pages, p. 37 clause 11- Confidentiality of Customer Records- Terms of Service.

[11] Englander v. TELUS Communication Inc. [2005] 2 F.C.R. 572 at para. 83.

[12] Criminal Code, R.S.C. 1985 c.34.

[13] Canadian Security Intelligence Service Act, R.S.C. 1985, c.C-23.

[14] Constitution Act, being Schedule B to the Canada Act, 1982 (U.K.) c.11.

[15] Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act 1982, being Schedule B to the Canada Act, 1982 (U.K.) c.11.

[16] Supra, note 13 at s.184.

[17] Ibid., s. 184.

[18] Ibid., s. 184.4.

[19] Ibid., s. 184.5.

[20] Ibid., s. 184.1.

[21] Ibid., s. 184.2(3).

[22] Ibid., s. 186(1.1).

[23] Supra, note 14, s.12.

[24] Thompson Newspapers Ltd. v. Canada (Director of Investigation & Research), [1990] 1 S.C.R. 425; R. v. McKinlay Transport Ltd. [1990] 1 S.C.R. 627.

[25] Competition Act, R.S.C. 1985, c.C-34.

[26] Income Tax Act, R.S.C. 1985, c.1.

[27] Hunter v. Southam Inc. [1984] 2. S.C.R. 145.

[28] R. v. Edwards [1996] 1 S.C.R. 128.

[29] Supra, at para. 45.

[30] R. v. Araujo 2 [2000] S.C.R. 992.

[31] Ibid, paras. 21 to 22.

[32] Supra, note 13, s. 487.

[33] R. v. Weir (1998), 59 Alta. L.R. (3d) 319 (Q.B.).

[34] Ibid, at para. 77.

[35] Lawful Access- Consultation Document, Department of Justice Canada, August 25, 2002, (http://www.justice.gc.ca/eng/cons/la-al/la-al.pdf). Also see- Summary of Submissions to the Lawful Access Consultations, Nevis Consulting Group Inc., April 28, 2003 (http://www.justice.gc.ca/eng/cons/la-al/sum-res/sum-res.pdf).

[36] R. v. MacInnis (2007), [2007] O.J. No 2930 (Ont. S.C.J.).

[37] R. v. Pervez (2005) 367 A.R. 165 (ABCA).

[38] R. v. Fattah (2006), 395 A.R. 223 (Alta. Q.B.).

[39] PIPEDA Case Summary #8 - Use and disclosure of personal information in telephone directories (http://www.privcom.gc.ca/cf-dc/2001/cf-dc_010814_01_e.asp); PIPEDA Case Summary #210 - Telecommunications company used and disclosed customer's personal information (http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030801_05_e.asp).

[40] Supra, note 2.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] PIDEDA Case Summary #61, Customer alleges company used his phone records to trace debtor (http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020719_2_e.asp) Office of the Privacy Commissioner of Canada found that a complaint was well founded where the telephone company had improperly used his telephone records without his knowledge or consent, for the purposes of tracking down a third party debtor. PIPEDA Case Summary #54, Couple alleges improper disclosure of telephone records to a third party (http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020628_2_e.asp). Also see R v. McInnis [2007] O.J. No. 2937 whereby the Ontario High Court of Justice held that cell phone records contain personal information. PIPEDA Case Summary #372- Disclosure to data brokers expose weakness in telecom's safeguards(http://www.privcom.gc.ca/cf-dc/2007/372_20070709_e.asp).

[45] PIPEDA Case Summary #51 - Bank accused of non-consensual recording and disclosure of telephone conversation (http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020516_e.asp).

[46] PIPEDA Case Summary #86 - Bank failed to inform customer of taped telephone call (http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021022_2_e.asp).

[47] Guidelines for Recording Customer Telephone Calls, Office of the Privacy Commissioner, 2002-11-27 (http://www.privcom.gc.ca/fs-fi/02_05_d_14_e.asp).

[48] PIPEDA Case Summary #160 – Telecommunications company monitors customer calls (http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030416_5_e.asp).

[49] PIPEDA Case Summary #180 - Bank uses tape-recording of customer's call for unidentified training purpose; connects another customer to the recording (http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030710_02_e.asp).

[50] PIPEDA Case Summary #137 - Telecommunications company accused of not protecting account against unauthorized access (http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030306_6_e.asp).

[51] PIPEDA Case Summary #329 - Wireless phone company improves safeguards for estranged spouses (http://www.privcom.gc.ca/cf-dc/2006/329_20060201_e.asp).

[52] PIPEDA Case Summary #372 - Disclosures to data brokers expose weaknesses in telecoms' safeguards (http://www.privcom.gc.ca/cf-dc/2007/372_20070709_e.asp).

[53] Ibid.

[54] Supra, note 2.

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] Letter to the Minister of Industry regarding the 5 year statutory review of the Personal Information Protection and Electronics Document Act (PIPEDA), July 13, 2007 (http:/www.provcom.gc.ca/parl/2007/let_070713_e.asp).

[59] Ibid.

[60] Industry Canada- Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics (http://www.ic.gc.ca/eic/site/ic1.nsf/eng/h_02861.html).

[61] Personal Information Protection in the Face of Crime and Terror: Information Sharing by Private Enterprises for National Security and Law Enforcement Purposes. Centre for Innovation Law and Policy, March 2008 (http://www.innovationlaw.org/Assets/Privacy+report.pdf).

[62] Ibid., p. 45

[63] Halsbury's Laws of England, Fourth Ed., 2003 reissue of vol. 8(1), para. 433.

[64] Stephens v. Avery [1988] Ch. 449 at 453, [1988] 2 All ER 477 at 481.

[65] Lion Labratories Ltd. V. Evans [1985] QB 526, [1984] 2 All ER 417, CA.

[66] Data Protection Act 1998 (c.29) [DPA].

[67] The Privacy and Electronic Communications (EC Directive) Regulations 2003, Statutory Instrument 2003, No. 2426 [Regulations].

[68] Interception of Communications Act 1985 (c. 56) [ICA].

[69] Regulation of Investigatory Powers Act 2000 (c. 23) [RIPA].

[70] Ie EC Council Directive 95/46 (OJ L281, 23.11.95, p.31)on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[71] Supra note 64 at para 503.

[72] McIsaac, Shields & Klein, The Law of Privacy in Canada, looseleaf (Toronto, ON: Thomson Canada Limited, 2000).

[73] Ibid.

[74] Ibid.

[75] Kyer, C. Ian, Fasken & Calvin, “The U.K. Data Protection Act: A model for Canada?”, Can. Computer L.R., Vol. 2, Issue 12, October 1985, 225-230.

[76] Ibid.

[77] Supra note 68 at s. 5.

[78] Supra note 68 at s. 30.

[79] “Directive 2002/58/EC Of The European Parliament And Of the Council of 12 July 2002”, Official Journal of the European Communities, L 201/37 at Article 1, para. 5.

[80] Ibid. at Article 1, para. 11.

[81] Ibid.

[82] Ibid. at Article 5, para.1.

[83] Interception of Communications act 1985 (c. 56) [ICA].

[84] Regulation of Investigatory Powers Act 2000 (c. 23) [RIPA].

[85] Office for Security and Counter Terrorism, “About RIPA”, <http://security.homeoffice.gov.uk/ripa/about-ripa/>.

[86] “Your Privacy is an illusion: UK attacks civil liberties”, October 2008, http://arstechnia.com/security/news/2008/10/your-privacy-is-an-illusion-uk-attacks-civil-liberties.ars>.

[87] Ibid.

[88] Ibid.

[89] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001 (USA Patriot Act).

[90] PIPEDA Case Summary #313, Bank’s notification to customers triggers Patriot Act concerns (http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp).

[91] Supra, note 2.

[92] Ibid.

[93] PIPEDA Case Summary #394 - Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers (http://www.privcom.gc.ca/cf-dc/2008/394_20080807_e.asp).

[94] Ibid.

[95] PIPEDA Case Summary #365 - Responsibility of Canadian financial institutions in SWIFT’s disclosure of personal information to US authorities considered (http://www.privcom.gc.ca/cf-dc/2007/365_20070402_e.asp).

[96] Supra, note 66.

[97] Guidelines for Processing Personal Data Across Borders, Office of the Privacy Commissioner of Canada, January, 2009 (http://www.privcom.gc.ca/information/guide/2009/gl_dab_090127_e.asp).

[98] Ibid.

Chapter 5

Mobile Phone Users' Privacy Surveys

The project team designed two questionnaires as a part of this study. These two surveys were intended to seek the feedback of mobile phone users as well as major mobile phone operators in Canada concerning the privacy of mobile phone users. This chapter discusses these two surveys, the obtained responses, the indicators that can be observed from the responses and the explanation of some of these indicators.

5.1 Mobile Phone Users' Survey

This survey is designed to explore the mobile users' privacy from the users' perspective. This survey was not intended to be a comprehensive one but rather a pilot study to explore the main concerns, expectations and awareness of mobile phone users regarding the privacy their privacy. This might explain the relatively small number of participants (forty eight). The questionnaire is filled online to keep the anonymity and privacy of the participants. A copy of the questions included in the questionnaire is given in Appendix I. The first part of the questionnaire is about the participant background (gender, age group, education level, and service provider (for hi/her mobile phone)). This background is included to test if there is any influence of the background information (e.g., age) on the measured indicators. As for the gender, 53% of the participants are female, 48% are male and 2% preferred not to disclose. Regarding the age group, 28% of the participants are between 18 and 24, 55% are between 25 and 44, and 15% are between 45 and 64. 9% of the participants have high school education, 6% have college diplomas, 30% have university degrees while 55% have postgraduate degrees.

The remaining questions can be grouped into three classes. One class (including questions 1, 3b, 4a, 6, 7, 11 and 12b) measures the expectations and views of the participants in their privacy issues as users of mobile phones. The second class (including questions 2, 3, 4, 8, 9, 12 and 13) evaluates the practices (of the participants) as mobile phones users and how this affects their privacy. Finally, the third class (including questions 5 and 10) tests the awareness of the participants with the privacy legislations and organizations in Canada.

The first question was inquiring about the user's expectation of the confidentiality of the information transmitted/received over the mobile phone. It has been found that users have high expectations for the confidentiality of the transmitted/received information. 30% have very high expectations, 26% have high expectation, 30% have medium expectations, 11 % have low expectations while 2% have very low expectations.

The next question was related to the frequency of sending/receiving confidential information by the users. Answers indicated that users generally send/receive confidential information over mobile phones in a regular basis. The responses show that 7% send/receive confidential information very often, 26% often, 28% sometimes, 25% rarely while 15% never send/receive confidential information over their mobile phones. This means that 85% of surveyed users send/receive (with different degrees of frequency) confidential information over their mobile phones.

Whether (or not) users save confidential information in their mobile phone was the following question. The trend changed this time and it was found that majority of surveyed users (68%) do not save information in their mobile phones. When users (who don't save confidential information in their mobile phones) were asked why they don not do, it was found that only 35% of them are concerned about the confidentiality of the stored information (in case the mobile phone is lost or stolen), while 71% indicate no need for that. Users who save information were found to save mainly personal photos (83%), business information (48%), personal information (39%), credit card number (13%), and other information is (13%). This indicates that sensitive information like personal photos, business information, and credit card numbers are saved by some mobile phone users.

The alarming response was that 84% of users never read the privacy statements provided to them by the mobile phone operator. 23% of those who never read the privacy statements indicated that it is too difficult to read, 37% did not do because they consider that not important!, while 46% of users did not do for other reasons such as "the user did not know that there is a privacy statement" or because "he can not change it". From the 16% percent who have read the privacy statement, 30% are highly satisfied and 70% are satisfied. This indicates high satisfaction with the privacy statement.

In the responses to questions 6 & 7, participants showed very serious concerns if they would find that their personal records (at the mobile phone operator) is made available to a third party or if they find that their text message is saved by their mobile phone operator. For the first case, 69% showed very high concern, 24% high concern and 7% medium concern, while for the second case, 74% showed very high concern, 13% high concern and 11% medium concern.

Despite these serious concerns showed in the previous two questions, the next question indicated that only 14% use password to protect stored information on their mobile phones.

The participants who use their mobile phones outside Canada were found to be 26% of the total number of participants. The list of countries where some participants use their mobile phones includes U.S.A, U.K., France, Spain, Italy, Germany, Japan, China, Singapore, India, Egypt, Greece, Netherlands, Taiwan, Saudi Arabia and U.A.E. The participants showed differed expectation of their privacy as mobile users outside Canada. While 29% expects the same level of privacy, 30% expects higher levels of privacy and 41% expects lower levels of privacy. It is alarming that 30% of the participants expect better privacy levels when they use their mobile phones outside Canada. This point requires further investigations and comparative studies to find the reasons of this finding.

Regarding the awareness with the privacy legislations and organizations in Canada, 89% indicated that they are not aware with them. What is even more alarming is that 95% of participants did not know what organizations or agencies can offer help if they have concerns regarding the privacy of their mobile phones. Even among the 5% who answered yes, two mentioned CRTC and one mentioned the name of one of the mobile phone operators as the organization/agency that can help them with their privacy problems, while no one mentioned the privacy commissioner office. However, 62% (of those who do not know which organization/agencies can help) showed their interest to know more information about such organizations/agencies.

The participants expressed their concerns from viruses or spyware that can attack their mobile phones. While 4% only had some previous experiences with viruses or spyware, 62% think that these viruses or spyware can compromise their privacy.

We also checked the influence of the background on the obtained indicators. For instance, it was found that 62% of male participants save confidential information in their mobile phones while 25% only of female participants do the same. Also, it was shown that 42% of male participants have read the privacy statement provided by their mobile phone operator while 4% only of female participant did. Regarding the awareness, 20% of male participants indicated that they know organizations/agencies can offer help with privacy problems, while 0% of female participants do. In addition, 70% of male participants showed their interest to know more about such organizations/agencies, while 50% only of female participants who have the same interest. The age also showed some influence on some indicators. For example, the 25-44 age group showed 72% high or very high expectations of their privacy as mobile phone users, while the 18-24 and 45-64 groups showed 33% and 28% high or very high expectations, respectively. The age also showed interesting influence on the tendency to save information in mobile phones. While 41% in the 18-24 age group save information in their mobile phones, 70% do in the 25-44 age group and 86% do in the 45-64 age group.

Finally it should be kept in mind that the number of participants in this survey was not large enough and the participants might represent a biased sample (with some emphasis on some age groups or education levels). Hence, the obtained statistics should be dealt with as just indicators rather than statistical measures of all mobile phone users in Canada.

5.2 Mobile Phone Operators' Survey

The second questionnaire was intended to analyze the privacy of mobile phone users from the operators' perspective. This questionnaire is given in Appendix II. The project team contacted most of the major mobile phone operators in Canada and provided them with a copy of the questionnaire. Three operators only (Bell mobility, Rogers and SaskTel) replied by declining to fill the questionnaire and they chose to direct us to their web sites which include their privacy agreements with the users. Other mobile phone operators never responded to our request. Hence, we could not get any response to our survey, which could have helped us in analyzing more aspects of the privacy of mobile phone users.

Chapter 6

Conclusions, Recommendations and Future Work

In the previous chapters, we have analyzed the problem of privacy of mobile phone users from technical and legal perspectives. In this chapter, we conclude the report by briefly discussing some general conclusions and recommendations that can improve the privacy of mobile phone users. Section 6.1 includes general conclusions of this study. Technical recommendations are discussed first in Sections 6.2. Legal recommendations are then given in Section 6.3. Then, Section 6.4 includes other recommendations. Finally, future work is given in Section 6.5.

6.1 General Conclusions

This report addressed several issues related to the privacy of mobile phone users from technical and legal perspective. The report also studied some indicators of the users' awareness and practices towards their privacy as mobile phone users. The main conclusion of this report is that there are various issues that can constitute serious risks to the privacy of mobile phone users. These issues include technical and legal issues. Technically speaking, the four addressed threats (signal interception, access to text message, access to users' records and access to stored information) are challenging but feasible. Furthermore, the legal study indicated some cases where the privacy of mobile phone operators is not protected under Canadian legislations (e.g., mobile phone calls intercepted across the borders). Also, the study shows that better awareness and more cautious practices should be adopted by mobile phone users. In addition, the results indicated that the privacy statements provided to users by the operators are not easily accessible to the average user perhaps because of their large size and difficult wording.

6.2 Technical Recommendations

i. Network Authentication: As shown in Chapter 3, some devices such as IMSI catcher and femotcells can be utilized as faked base stations and allow others to get access to the mobile phone users' information. The solution for this problem is introducing network authentication to the mobile phones as mobile phones are authenticated by the network. This can eliminate the

faked base station problem but it requires new protocols and software upgrading for by the mobile phone network operator and in mobile phone sets as well.

ii. Additional Encryption: In order for mobile phone users to guarantee higher security and more privacy on their phone calls, users can always use external voice encryption devices such as TopSec Mobile from Rohde and Schwartz [1]. Such devices ensure that additional stronger encryption on top of the encryption offered by the wireless system (e.g., GSM or UMTS). The additional encryption can be utilized as a separate device which can be connected to the mobile phone using Bluetooth technology or integrated in the mobile phone handsets as in TopSec GSM mobile phone handsets. Hence, it is recommended for users who usually exchange confidential information over their mobile phones to use additional encryption.

iii. Password/Fingerprint Sensor: In Chapter 5, it was shown that the majority of mobile phone users do not use passwords to protect the stored information on their mobile phones despite the fact that a considerable percentage of users save personal and confidential information on their mobile phones. What is even more effective (than passwords) is the fingerprint sensor (available in some new models of mobile phones). Users, who store sensitive information in their mobile phones, should consider adopting such protection measures.

iv. Protection against Viruses/Spyware: Mobile phone viruses or spyware can be very harmful to the mobile phone users as discussed in Chapter 2. Antivirus and spyware-aware software will become soon essential to protect mobile phone users from many serious problems including privacy threats. Also, mobile phone users are encouraged to be cautious before downloading any files or software to their mobile phones unless they are obtained from reliable source.

v. Regular Tests by Operators: As mentioned in Chapter 2, the “Athens Affair” mobile phone spying scandal was discovered by chance during software upgrade by the mobile phone operator few months after inserting the malicious software (or more accurately modifying the software) at the operators equipment. Hence, mobile phone network operators are encouraged to perform (if they don’t already do) regular tests and checks for their equipment (switches, servers, computers,

etc.) and software (either embedded or application) to ensure the integrity and security performance.

6.3 Legal Recommendations

i. *Criminal Code* – Amend definition of "private communication" to explicitly reference "text messages": Text messages and telephone calls are two types of communications that may be transmitted from a mobile phone device. The expectation of privacy that a mobile phone user has when communicating through text messaging should not be any different than when the user is communicating orally using the very same mobile device.

Prior to the introduction of section 184.5 to the *Criminal Code* it was not clear that the prohibition against the interception of private communications applied to radio-based telephone communications such as mobile phones communications. In 1995, the *Criminal Code* was amended to end the debate associated with the application of the private communication interception offence in section 184 to wireless communications. Since 1995, mobile phone users have been protected by the *Criminal Code.* The interception of their "oral" private communications require judicial authorization pursuant to Part VI of the *Criminal Code*.

The legal debate that exists today surrounding email/text messages in various stages of transmission should be resolved and all such activity ought to be treated like "private communications" and afforded the protection of Part VI of the *Criminal Code* rather than like "records" under Part XV of the *Criminal Code*. Part VI, judicial authorization preconditions are more onerous provisions than Part XV authorizations.

It is important that legislation such as the *Criminal Code* be reflective of the expectations of privacy that individuals feel they have when the use their wireless devices. Given this reasonable expectation of privacy, it is recommended that the level of protection against interception not be different for text messages than it is for oral communications. The definition section of Part VI of the *Criminal Code* should be amended to ensure that the definition of "private communications" includes both "text" and "oral" communications.

Hence, we recommend that the *Criminal Code* should be amended to define "private communication" to include oral and text messages to ensure that the interception of text messages requires Part VI, *Criminal Code* judicial authorization.

ii. PIPEDA- Amend *PIPEDA* to define what is meant by "lawful authority" and "government institution" under section 7(3)(c.1) and draft prescriptive Guidelines outlining when an organization ought to exercise its discretion to disclose personal information to a government institution: The present wording of section 7(3)(c.1) of *PIPEDA* provides significant organizational discretion with respect to the disclosure of personal information to a government institution in the absence of a warrant or court order. In 2007, Government indicated in its response to the five year statutory review produced by the House of Commons Standing Committee that it does not intend to remove the discretionary authority of an organization to determine whether to release personal information to a government institution. Government's intention to clarify the meaning of "lawful authority" and "government institution" through legislative amendment and the issuance of guidelines to assist an organization in its deliberations of deciding whether to release personal information to assist law enforcement during the pre-warrant stage of an investigation is encouraging.

However, it is essential that drafted guidelines describe the types of offences that are considered to be serious enough that an organization may release the personal information without the government institution producing a warrant or court order. Also, disclosure of personal information without a warrant or court order should be discouraged unless the personal information sought would not be afforded a high expectation of privacy by an individual.

Therefore, we recommend that the *PIPEDA* and/or the Regulations should be amended to define what is meant by "lawful authority" and "government institution" under section 7(3)(c.1). Also, regulate or draft prescriptive guidelines outlining the specific offences and the circumstances when an organization ought to exercise its discretion to disclose personal information to a government institution without consent of the individual.

6.4 Other Recommendations

i. Increasing the Awareness: The most effective way to improve the privacy of mobile phone users is to increase the awareness among mobile phone users with the various threats that can compromise their privacy. This report is one step towards this direction. However, much more steps and efforts are needed from all people involved in this business including mobile phone operators, mobile phone users, federal and provincial governmental institutes, media, and academia.

ii. More Accessible Privacy Regulations: Operators are encouraged to make their privacy regulations are easier to be accessed by the average user. For instance, the wording and size of the privacy statements need more work to make them less challenging for the regular user.

6.5 Future Work

Some of the addressed issues in this report still need further and more rigorous investigation. For instance, at the technical side, the design of robust and efficient network authentication protocols that have backward compatibility of existing systems is an open topic for future research. On the other hand, gaining deeper insight into users expectations, attitude and towards their privacy as mobile phone users is vital. Furthermore, effective ways to influence mobile phone users to increase the awareness and improve the privacy protection need inter-disciplinary studies by psychological, sociological and technical research teams. The privacy of users of other wireless communication systems such as wireless local area networks is also a good candidate for future work.

References

[1] TopSec Mobile Voice encryption for mobile phones;
http://www2.rohde-schwarz.com/file_10992/TopSec-mobile_dat_en.pdf

Appendixes

Appendix I

Mobile Phone Privacy Questionnaire (users)

This questionnaire is part of a research project studying the privacy of mobile phone users in Canada. This project is funded by the Office of the Privacy Commissioner of Canada. The questionnaire includes 15 questions and should take 10-15 minutes to complete. Please answer these questions to the best of your knowledge. The project team appreciates your help with this study. For more information about the project, please contact the project leader (Dr. Mohamed H. Ahmed, Memorial University of Newfoundland) using the email address given above, or follow the following links:

http://www.engr.mun.ca/~mhahmed/privacy.html
http://www.privcom.gc.ca/resource/cp/2008-2009/cp_background_e.asp

1-Personal Information

Age: _____ City: _____
Gender: _____ Province: _____
Mobile phone/device (e.g., Blackberry) service provider: _____

2-How do you rate your expectations of the confidentiality of the information you send/receive over your mobile phone/device?

☐ Very High ☐ High ☐ Medium ☐ Low ☐ Very Low

3-How often do you send/receive confidential information over mobile phone/device?

☐ Very Often ☐ Often ☐ Sometimes ☐ Rarely ☐ Never

4-Do you save confidential information in your mobile phone/device?

☐ Yes ☐ No

4a-If yes, what type of information do you save in your mobile phone/device?

☐ Personal information (Date of birth, SIN number, etc.) ☐ Personal photo(s)
☐ Business information ☐ Credit card number(s) ☐ Others: _____

4b-If no, please provide reasons

☐ Concerned about the information privacy if the mobile phone/device is lost/stolen
☐ No need ☐ Others: _____

5-Did you read the *Privacy Statement* provided by the mobile phone/device service provider?

☐ Yes ☐ No

5a-If yes, how do you rate your satisfaction with the *Privacy Statement*?

☐ Very High ☐ High ☐ Medium ☐ Low ☐ Very Low

5b-If no, please provide reasons

☐ Too difficult to read
☐ Not important
☐ Others: _____

6-Are you aware with the privacy laws and regulations related to the mobile phone/device?

☐ Yes ☐ No

6a-If yes, how do you rate your satisfaction with these privacy laws and regulations?

☐ Very High ☐ High ☐ Medium ☐ Low ☐ Very Low

7-How would be your concern IF you find out that your mobile phone/device service provider makes your personal records available to a third party?

☐ Very High ☐ High ☐ Medium ☐ Low ☐ Very Low

8-How would be your concern IF you find out that your mobile phone/device service provider keep records of the text message you send/receive?

☐ Very High ☐ High ☐ Medium ☐ Low ☐ Very Low

9-Do you use a password to protect your stored information on your mobile phone/device?

☐ Yes ☐ No

10-Do you have embedded fingerprint sensor in your mobile phone/device?

☐ Yes ☐ No

11-Do you know what agencies to contact regarding your concerns/questions related to the privacy of your mobile phone/device service?

☐ Yes ☐ No

11a-If yes, please mention these agencies:

i) _____
ii) _____
iii) _____

11b-If no, would you like to receive more information about such agencies?

☐ Yes ☐ No

12-Do you support the monitoring (tapping) of mobile phone/device by governmental or law enforcement agencies?

☐ Yes, with a court order ☐ Yes, with or without a court order
☐ No, even with a court order

13-Do you use your mobile phone/device outside Canada?

☐ Yes ☐ No

13a-If yes, in what countries (in addition to Canada) you use your mobile phone/device?

i) _____
ii) _____
iii) _____
iv) _____

13b-In this case, how do you rate your expectations for the privacy of your mobile phone/device (compared with that in Canada)?

☐ Same ☐ Worse ☐ Better

14-Have you ever had any problem with viruses or spyware software on your mobile phone/device?

☐ Yes ☐ No

14a-If yes, do you think this virus or spyware software affected the privacy of your mobile phone/device service?

☐ Yes ☐ No

15-Do you have any additional information, suggestions or concerns regarding the privacy of mobile phone/device service?

_____
_____
_____
_____

Appendix II

Mobile Phone Privacy Questionnaire (operators)

This questionnaire is part of a research project studying the privacy of mobile phone users in Canada. This project is funded by the Office of the Privacy Commissioner of Canada. The questionnaire includes 14 questions and should take about 15 minutes to complete. Please answer these questions to the best of your knowledge and return the completed questionnaire by email to mhahmed@engr.mun.ca by January 31st, 2009. The project team appreciates your help with this study. For more information about the project, please contact the project leader (Dr. Mohamed H. Ahmed, Memorial University of Newfoundland) using the email address given above, or follow the following links:

http://www.engr.mun.ca/~mhahmed/privacy.html
http://www.privcom.gc.ca/resource/cp/2008-2009/cp_background_e.asp

Note: In MCQ questions, please highlight the most suitable answer(s) and underline it/them

1-Background

Compnay's name: _____
City: _____
Province: _____

2-What is the wireless technology your company uses?

a) GSM/GPRS b) CDMA (IS95) c) CDMA (cdma2000)
d) CDMA (W-CDMA) e) TDMA (IS-136/54) f)
Other:_____

3-What types of security measures does your company use to protect the users' records on its databases?

a) Firewalls b) Encryption software c) Passwords
d) Others:
_____

4-Does the privacy agreement with the customers allow your company to provide a third party with some of the customers' information?

a) Yes b) Yes after obtaining cutomer's consent c) No

4a-If yes, what kind of information your company can provide to the third party?
_____

_____

5- Does your company keep copies of text messages that customers send/receive?

a) Yes b) Sometimes c) Rarely d) No

5a- If yes, how long does your company keep the text messages?

a) Days b) Weeks c) Months d) Years

6- Does your company have a formal procedure to facilitate phone tapping by law enforcement?

a) Yes b) No

6a- If yes, what are the main guidelines and regulations of this procedure?

_____
_____
_____
_____
_____

7- Does your company perform routine checks to test the security of its databases?

a) Yes b) Sometimes c) Rarely d) No

7a-If yes, what type of tests does your company perform?

_____

7b-If yes, how frequently these tests are performed?

_____

8-Does your company keep hardcopies of the customers' information?

a) Yes b) No

8a-If yes, what measures are used to protect these hardcopies?

_____
_____
_____

8b-If yes, how long your company keep these hardcopies?

_____

8c-If yes, what is the process your company uses to discard these hardcopies?

_____
_____

9-What is the process your company uses to discard old computers/storage devices used for databases?

_____
___
_____
___
_____
___
_____
___

10-Is there any formal agreements your company has with its employees regarding the privacy and confidentiality of the customers' information they are handling?

a) Yes b) No

11-How does your company verify the identity of the customer requesting some of his/her personal information?

a) Questions regarding some personal information
b) ID document
c) Some shared secret (e.g., password, PIN, etc.)
d) Others:
_____

12-Does your company offer roaming service to its customers?

a) Yes b) No

12a-If yes, what information about roaming customers your company sends to other operators?
_____
_____
_____
_____

13-Does your company allow customers to upload their files (stored on their mobile phones/devices) on the company's servers?

a) Yes b) No

14-Do you have any additional information, suggestions or concerns regarding the privacy of mobile phone/device service?
_____
_____
_____
_____