Privacy Implications of GSM Network Services

Technical Report

Tracy Ann Kosa
Faculty of Science
University of Ontario Institute of Technology
Oshawa, Canada
tracyann.kosa@uoit.ca

Khalil el-Khatib
Faculty of Business and Information Technology
University of Ontario Institute of Technology
Oshawa, Canada
khalil.el-khatib@uoit.ca

Steve Marsh
Security Trust Group
Communications Research Centre Council
Ottawa, Canada
steve.marsh@crc.gc.ca

Abstract
Current research on GSM does not deal with privacy requirements, or confuses privacy (legislated) with security (standards based). This paper seeks to examine how the applicable privacy legislation in Canada (PIPEDA) would apply to GSM services. Part I provides an overview of the evolution of network communications and how privacy legislation applies, ending with a discussion of GSM functionality and players. An description of the kind of personal information in GSM service delivery is presented in Part 2, while the privacy analysis is conducted in Part 3. Part 4 is a brief inter-disciplinary literature review demonstrating how GSM research is focused respectively on public policy and functionality, while security work focuses on authentication techniques. Various approaches to privacy are described in Part 5, and a short conclusion of the implications is presented in Part 6.

Index Terms – Telecommunications, GSM, privacy, PIPEDA, security.

I. Introduction

The consideration of privacy protection in communications dates back 1865 with the use of the telegraph. Concerns were raised again throughout the fifties and sixties as telecommunications technology advanced and the information society developed. By the mid-1970s, the Internet was a reality, privacy legislation was being passed in North America, and the legal context for considering privacy was based on the idea that technological innovation does have an impact on social values.[5]

The same applies to technologies evolving today. Cellular phone systems offer location independent ubiquitous communication.[31] Networks, the delivery mechanism for these services, are based on the concept of cells, zones that overlap to cover geographic areas.[20] Companies that provide these kinds of services in Canada are subject to a number of regulations in the provision of services to user, including the privacy requirements set out in the *Personal Information Protection of Electronic Documents Act* (PIPEDA).[26]

The requirements in the privacy legislation – PIPEDA – apply to any company involved in the delivery of services. To examine how the privacy requirements apply to the Global System for Mobile communications (GSM), the paper first outlines the evolution of cellular service, leading to a description of GSM functionality and the specific types of organizations involved in the delivery of GSM services.

Cellular networks are based on the use of a central transmitter-receiver in each cell, called a base station (or Base Transceiver Station, BTS).[20] Cell phones always communicate with the closest (geographically) BTS, and are constantly checking for service availability. The BTS will assign different channels either through fixed assignments (a set of frequencies that do not change), fixed assignments with borrowing privileges (before service is restricted, the BTS may try to borrow a frequency from a neighboring BTS), or dynamic assignments allocated on request to the BTS by the Mobile Switching Centre (MSC).[31]

This was not always the case. Cellular telephony, in its infancy, relied on the assignment of frequency spectrum for communication. This method was called Frequency Division Multiple Access (FDMA), but is now more commonly referred to as analog service.[29] The first generation of mobile telephony (1G) operated using analog communications based on three geographically divided standards (US, Advanced Mobile Phone System; Europe, Total Access Communication System; and the UK, Extended Total Access Communication Systems).[20] As long as cellular service relied on circuit switching, it would have to transmit at relatively low speeds.

In the 1990s, new digital cellular technology made it possible to transmit communications more effectively across the spectrum. Two types of technology enabled this transmission: Time Division Multiple Access (TDMA) or Code Division Multiple Access (CDMA) both enable multiple users to share the same radio frequency transmission channel [28] effectively marking the change from analog to digital and making 1G obsolete.[29] With this move to digital packet switching transmission, cell devices were on the verge of becoming an important part of the Internet.

The most widely adopted standard guiding the development of 2G technology was the Global System for Mobile communications (GSM).[20] Work on the GSM standard was initiated by the European Conference of Postal and Telecommunications Administration (CEPT) in 1982, and the standard was issued by the European Telecommunications Standard Institute (ETSI) in 1990. The standard focused on the creation of a digital system for cell phones, primarily for voice services but with a data transmission layer on top.[31]

The functionality of the 2G network allowed for digital data transmission, such as Short Message Service, or SMS messages, and multimedia messages (Multimedia Message Services, or MMS messages). Two extensions to the GSM standard have been made to improve service; the General Packet Radio System (GPRS, or 2.5G) allowed higher rates of data transmission, while the Enhanced Data Rates for Global Evolution (EDGE, or 2.75G) opened the door for multimedia applications.[20]

A. Functionality

In GSM networks, the user device is called a mobile station. The mobile station includes a card that allows the user to be uniquely identified (Subscriber Identity Module, SIM), and a device (phone). The SIM card also has a unique identification number called the International Mobile Subscriber Identity (IMSI), which can be protected by a 4 digit personal identification number (PIN).[20,31]

Each device is uniquely identified by a 15-digit number called the International Mobile Equipment Identity (IMEI). Mobile devices are typically lightweight and battery powered, and have the same set of basic features: microprocessor, read only memory, random access memory, radio module, digital signal processor, microphone, speaker, hardware keys and interfaces and a liquid crystal display (LCD).[16]

Most information found on the device can be transmitted using GSM technology. Communications starts with the SIM card. The SIM card allows each user to be identified regardless of the terminal used while communicating with the base transceiver station (BTS).[20,31]

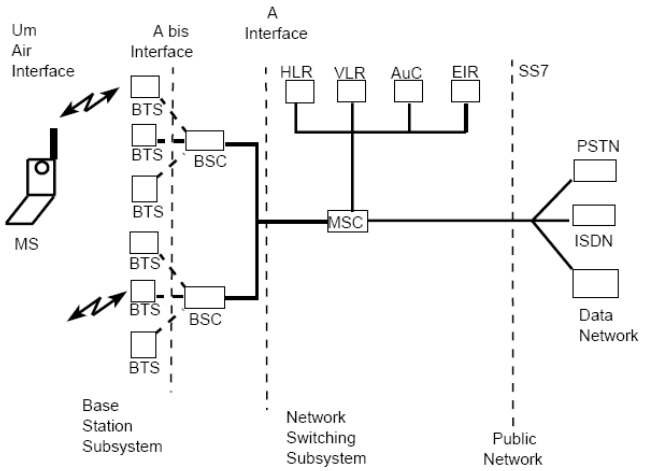

FIGURE I [1]

When the user engages the mobile device, the communication path occurs through a radio link between the mobile station (users' phone) and the base station (network transmitter). Each BTS is assigned a set of channels, and neighboring base stations are assigned different sets to avoid interference.[31] All BTS' in a cellular network are connected to a base station controller (BSC) that determines resource allocations. The BSC and the BTS are together referred to as the Base Station Subsystem (BSS). Each BSC is connected to a MSC, which belongs to a Network Station Subsystem (NSS) responsible for managing user identities, locations and establishing communication with other users. The physical connection between the MSC and the BSC is managed by a telephone network operator, who connects the MSC to the public telephone network and the Internet.[20,31]

GSM also supports roaming; the movement of users from one operator network to another. As users move around, geographically, the mobile will leave the transmission range of one BTS to enter the range of another. This handover process is also known as roaming, and the users' mobile will constantly check the signal levels of surrounding BTS' to obtain service. Mobiles that arrive at a full BTS will get no reception. If a user arrives at a new BTS while in the middle of a call, the handover can be treated as a new call or queued off to allow for other calls to end which makes room for the 'new' user in the 'new' BTS.[31]

B. Players

Under PIPEDA, the user is considered as the data subject, or the individual about whom information in the network relates. In the case of GSM, or any cellular telephony services, the data subject is the user of the mobile device. As such, they have certain rights and obligations afforded under the Act.

The telephone network operator is considered the service provider of mobile phone services. In Canada, there are 17 cell phone providers of GSM technology.[30] The majority of providers use Bell or Rogers networks to provide services. As a service provider, these companies would be statutorily obliged to comply with the requirements set out in PIPEDA for the collection, use and disclosure of personal information.

In a GSM network, the MSC connects with four databases to facilitate GSM service delivery. First, it connects with the Home Location Register (HLR) which contains data on subscriber position in the area of the switch, and coordinates all data changes.[19] HLR functionality is depicted in the figure below.

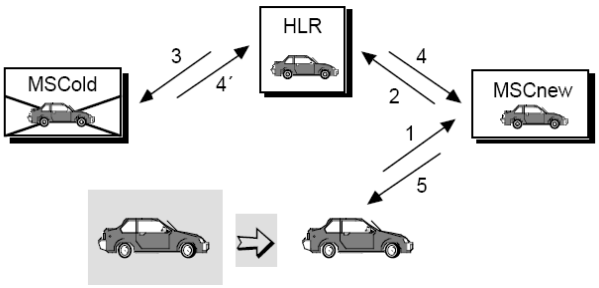

FIGURE II [19]]

Second, it retrieves information on 'new' users through the Visitor Location Register (VLR), which contains data on visiting subscribers to the MSC territory. Third, the MSC connects with the Equipment Identify Register (EIR) to access a database listing all mobile terminals (user phones). Finally, the MSC connects with the Authentication Centre (AUC) to verify user identity.[20,31] .

Under PIPEDA, any organization that assists in the service provider in supply a service like GSM is subject to the same provisions in the Act. Further, the primary service provider; the telephone network operators, are responsible for ensuring that the privacy requirements have been communicated and implemented to organizations that offer MSC services.

II. GSM DATA

The typical user's mobile device contains a number of types of data, including but not limited to: subscriber and equipment identifiers; date / time, language and other customizable settings; phonebook information; appointment calendar information; text messages; dialed, incoming and missed call logs; electronic mail; photos, audio and video recordings; multi-media messages; instant message and web browsing activities; electronic documents and location information.[16] In addition, the device capacity may be extended by information contained on a smart card, or other type of portable media contained in the device.

Referring back to the legislative requirements, PIPEDA applies to parties as identified in Part I(b) when the information collected, used and disclosed for the purposes of providing the service meets the statutory definition of personal information. Under PIPEDA s.2, personal information is defined as information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.[26] In order to determine what, if any, requirements apply to GSM and which parts of the functionality of the system, at minimum a cursory list of data elements must be examined to determine if the system does actually collect, use and / or disclose personal information as defined by PIPEDA.

Appendix A contains a list of the data elements in a GSM standard mobile telephony network and identified whether each field meets the definition of personal information under PIPEDA. Notably, the mobile devices themselves generate a significant amount of data (as opposed to the user). Under PIPEDA, machine generated data is considered personal information if it can be linked to a user. The purpose of device generated data for GSM is to support functionality and the service delivery model; as a result, the majority can be linked at minimum to an action taken with a given cellular device at a given time, making it identifiable (within a certain probability).

The figure below gives an example of how information listed in Table I (Appendix A) can be used to identify information about a person. Call records, for example, are easily used to identify a person's actions at a given time.

	Who	What	Where	When	Why	How
Subscriber/Device Identifiers	X					
Call Logs	X			X		
Phonebook	X					
Calendar	X	X	X	X	X	X
Messages	X	X	X	X	X	X
Location			X	X		
Web URLs/Content	X	X	X	X	X	X
Images/Video	X	X	X	X		X
Other File Content	X	X	X	X	X	X

FIGURE III [16]

From this table, it is evident that the majority of data collected, used and disclosed in the GSM service delivery process is not only statutorily considered personal information, but can also be used easily to infer specific actions or intentions.

III. Privacy Analysis

The application of PIPEDA is based on two factors: the type of organization and the type of data. Private sector companies that provide GSM services are subject to the Act by virtue of being 'for profit' organizations. Notably, GSM transmission does not work without the communication of data. In particular, providers of GSM services need to collect personal information about users to manage the service delivery process. There are rules, however, that guide how telecommunications companies collect, use and disclose information about users, including the need to obtain informed consent. The collection of personal information must be reasonable, e.g. not excessive or beyond that required to provide the cellular telephone service. GSM providers must have privacy policies in place, and also have a responsibility to secure and protect information. All of these rules are set out in detail in PIPEDA, which is consent-based legislation intended to enable the user to understand how their information will be used in the service delivery process.

The consent-based mechanism means that GSM users have a right to expect to be informed of the information management practices used to support the delivery of services. Further, users have a right to see any information about them, which should be accurate and complete. The enforcement mechanism for PIPEDA is complaint-based; the user has a right to complain to the Office of the Privacy Commissioner of Canada when they believe a GSM provider is not complying with PIPEDA.

The application of PIPEDA becomes more difficult the more complex the service offering. To start, identifying all the personal information data elements can be an extraordinarily detailed and onerous task, yet is required to implement even the most basic compliance requirements under the Act. An attempt is provided in Section IV. Without even a basic data inventory, the minimum requirement under PIPEDA to obtain informed consent from the user is suspect, and providers of GSM services are in a position of non-compliance. Additionally, how can a user obtain an accurate list of their own information without knowledge of system functionality? Further, a user cannot exercise their right to formal redress without knowing the role of each company in the GSM service delivery model.

Referring back to the specific provisions in PIPEDA, there are 10 key components of privacy protection, each with several sub-provisions.

The first is accountability (PIPEDA s.4.1). In GSM, each company is responsible for identifying a privacy accountable party in the organization, who must implement policies and practices to reflect the requirements in PIPEDA. This provision sets out that the GSM provide is responsible for all personal information in its possession, but also extends the requirement to include any personal information transferred to a third party for processing. Each telephone network operator is accountable for the privacy practices of each MSC, and other telephone network operators as signals roam.

The second requirement speaks to identifying purpose (PIPEDA s.4.2), a requirement for the GSM provider to identify the purpose for which personal information is collected prior to the collection. There are provisions under this requirement that restrict extending the use of personal information for any other purpose that the one initially identified; so the GSM provider may not collect information for billing and then use it for research or analysis purposes.

Consent (PIPEDA s.4.3) is perhaps the most critical requirement under PIPEDA. GSM providers are required to explain how information is transmitted in a way that is meaningful and reasonably understandable by the user. The form of the consent (e.g. check off box, application form) is not as important as meeting the expectations of the user. The successful implementation of this requirement, like the others under PIPEDA, hinges on informed and open communications with the GSM provider in particular about mechanisms like lawful access to subscriber data.

Requirements in PIPEDA also limit collection to that which is reasonably necessary to provide the specific GSM service (PIPEDA s.4.4). They also limit use, disclosure and retention (PIPEDA s.4.5) which, in particular, limit the retention of user information beyond a time necessary to complete a specific transaction, for example, a phone call from start to finish. Arguably, this provision could require GSM providers to significantly scale back the retention schedules of subscriber data closer to the time frame of the specific communication task request by the user.

GSM users are entitled under the accuracy requirement (PIPEDA s.4.6) to have complete and accurate information held about them by the GSM provider (and by extension any other organization that holds data about the user).

Section 4.7 of PIPEDA is where security and privacy overlap; these requirements call for GSM providers to have administrative, technological and physical safeguards in place to protect the user's personal information as it is collected, used and disclosed in the service delivery process. Training requirements are also set out in this section.

Requirements for openness, in particular about information management practices within the GSM provider, are also set out in PIPEDA (s.4.8).

Users are entitled to access their own information held by the GSM provider (PIPEDA s.4.9) except in very limited and specific circumstances (such as litigation privilege). GSM users are also entitled to know what specific third parties have had access to their data, for example any MSCs, and to correct it where necessary.

Finally, GSM users are entitled to complain to the GSM provider about non-compliance with privacy requirements set out PIPEDA, and the organization is obligated to respond.

Although these requirements can be interpreted as largely business process ones, they bleed into architecture specifications, in particular during the GSM roaming process. The purpose of cellular telephony was to enable mobile communications, in effect, making it ubiquitous. As person information roams, so does the obligations of the initial GSM provider in ensuring compliance with PIPEDA. Further, each of these requirements apply to any personal information data element contained in the GSM service, no matter the format, e.g. call logs versus server logs.

Non-compliance with PIPEDA presents two risks to GSM providers: harm to the user, and harm to the organization. There is no right of tort action in PIPEDA; complaints are directed to the Office of the Privacy Commissioner of Canada (OPC). The OPC is obligated to investigate all complaints and issue orders. If the GSM provider does not comply with the initial order, the user has a right to take the matter to Federal Court, which does have the power to name a provider publicly, award damages and make them comply with the Act. Non-compliance with PIPEDA can pose a reputation and monetary risk to the GSM provider; trust is an essential part of the cellular telephony system [5] and users have a choice of service providers. On an impact scale, at minimum, non-compliance with PIPEDA could result in an internal loss of reputation among staff. More significant instances of non-compliance could result in a minor to serious adverse attention from the media or the public. Very significant instances could result in a reduction or elimination of a specific line of services altogether.

User harm as a result of non-compliance is more difficult to quantify. On a minor scale, it is conceivable that a GSM provider's non-compliance with PIPEDA does not result in any harm or injury to the individual. More significantly or substantive breaches of personal information in a GSM system could cause personal injury, damage to relationships or personal reputation. At the most significant level, a breach in GSM communications between users could cause a loss to public safety, significant financial or social hardship, or even loss of life depending on the nature of the communications.

IV. Literature Review

Literature on GSM and privacy is diverse and interdisciplinary. It can be loosely classified by strategic and operational domains. The first set of literature focuses on exploring and explaining the architecture and functionality of networks, network security and how GSM has evolved.[5,12,13,16,20,29,31] Although much of this research cites privacy in some way, none of it deals with the explicit requirements of PIPEDA. For background purposes, of some interest in this body of research is a review of how privacy issues were dealt with during the creation of the modern Internet. During the basic Internet design process, privacy issues were considered at three different levels: the network, individual hosts and the user. At the network level, contributors to the Request for Comments (RFC) process presented four different arguments for privacy protection. First, network integrity required trust, which in turn required both privacy and security for both users and computing processes (daemons). Second, privacy was identified as key to enabling resource sharing across networked databases. Second, billing for resources used for ARPA funded sites created the need for user identification protocols (passwords). Finally, privacy was seen as a tool for ensuring professionalism by those who participated in the development of the network. At the host level, privacy protections were a component of ensuring service integrity, while user verification (usernames and password passwords) were used as the mechanism. Generally, at the host level, privacy was dealt with inconsistently throughout the RFC process. At the user level, data privacy was linked with the issue of data integrity. The RFCs demonstrate an understanding of the differences in data types when it comes to privacy concerns. Notably, it was understood that privacy protections apply throughout the data transmission process, although it was often limited to access controls.[5]

Similarly, there is a small body of work that is focused on the evolution of the GSM standard, and associated issues like intellectual property rights.[2,25] This work does not address privacy considerations in the implementation of GSM.

From the policy perspective, there are a few papers that focus on the application of privacy policy to the telecommunications industry.[14,17] Katz makes some interesting points on how the historical design of telecommunications systems can actually protect privacy: the introduction of automatic switching restricted the local operator from overhearing phone calls, public key-coding procedures can allow users to communicate with each other in relative secrecy; and social networks created by ubiquitous computing can enable users to work together to combat privacy invasions. Hiramatsu examines how the Japanese right of privacy in enshrined in the constitution, and how this balanced in the telecommunications industry. The approach, Hiramatsu notes, is based largely on the claim of communications privacy in support of the right to freedom of expression. Private telecommunications companies, such as the Nippon Telegraph and Telephone Company (NTT) and the Kokusai Denshin Denwa (KDD) struggle with the issue of employee privacy rights. There is also a cultural distinction of how the more publicly associated telecommunications company (NTT, still privately held) handles privacy, versus the more private company (KDD).

Some papers focus on the application of telecommunications policy in a specific geography, which others are comparative in nature.[27] Schwartz presents an interesting comparative analysis of telecommunications surveillance patterns in German versus the United States considering both constitutional and statutory laws. Of particular interest, he notes that data erasure and data retention are the most distinct areas of comparison; while German telecommunications laws require fixed erasure times (e.g. connection data must be retained no longer than six months), American law has no such requirement. In addition, the US government has become an international lobbyist for mandatory data retention requirements, although most European Union countries have no such requirement (although Switzerland enacted a requirement for Internet Service Providers (ISPs) to record and store traffic and email data for at least 6 months).[27]

More recently, research papers focus on the application of the US Patriot Act to the telecommunications industry, generally highly critical of the ensuing privacy invasion of telecommunications.[23] Lee notes that many telecommunications carriers have already turned over user data to law enforcement agents without notice to subscribers, and the Congress failed to consider that law enforcement might use electronic surveillance to monitor activities unrelated to terrorism. In detail, Lee examines how provisions extending the right and ease of searches, subpoenas, and wiretaps have violated the privacy of ISP subscriber records and voicemail in particular. Law enforcement authorities have also benefited, Lee states, from the extension of authority of pen registers (records of telephone number of outgoing calls) to the Internet and other computer networks.

In the security realm, there is a significantly larger body of research work that relates to GSM network protocols, and tends to focus on securing authentication mechanisms. [1,3,6,7,21,22,24] Al-Tawil et al propose a new authentication protocol for GSM with a goal towards lightening signaling traffic and decreasing the call set up time.[1] Lee et al also propose a new authentication scheme to improve GSM to support communication between the MS and VLR within the existing architecture and reducing bandwidth and store space at the VLR at the same time. This technique would also eliminate the need for the HLR to be involved in the authentication process.[21] Lee et al [22] propose not only a new authentication protocol, but also a location and data confidentiality protocol based on the assumption that the HLR is trusted but in reality, the VLR might not be trusted. Peinado used this scheme proposed by Lee et al [22] and added the anonymous channel protocol (modeled in a scenario where users want to communicate from visiting networks, but they do not want location and identification information known) to create an enhanced version of [22]. The addition of the anonymity protocol allowed for any user to access the GSM service without disclosing their identity to the VLR.[24]

Brown compares GSM authentication mechanisms and concludes that hybrid method is likely the best mechanism for protecting user identity information.[6] Similarly, Beller et al compare the use of different public-key techniques in protecting mobile conversations, concluding that any of them protect privacy using specific cipher functions, but still require authentication and key-agreements.[3] In response, Carlsen provides an improved protocol to obtain a higher assurance of authentication and key distribution, commenting that such a protocol provides end-to-end privacy.[7]

While many of these papers reference privacy, the substantive majority do not actually address legislated privacy rights as outlined in PIPEDA. As a preliminary step towards that analysis, a GSM data analysis is presented in the next section.

V. APPROACHES

Some of the techniques for protecting network privacy predate PIPEDA. They were proposed through the development of ARPA and impact GSM functionality today. Specifically, four network level techniques were identified. First, private networking allowed for the creation of a subspace where communications could occur privately (originally for national security reasons). Termination of activity features allowed for serving hosts to shut down all processes upon receipt of an error message from a remote host, e.g. incorrect username or password. Thirdly, messages were designed such that content was packetized (broken up). Finally, computers were assigned identities for authentication purposes, specifically related to trusting the transmission of data. From the data perspective, decisions on information architecture (e.g. storing metadata separately from content data) and the ability to implement encryption were also included.[5] Together, these design features address a few privacy requirements, including safeguards, limiting collection, limiting use, disclosure and retention (PIPEDA s4.7, s.4.4, s.4.5).

The European Telecommunications Standards Institute issued a number of standards on GSM, of particular interest is the Specification of the Subscriber Identity Module for the Mobile Equipment interface.[13] This standard sets out a number of security requirements with the goal of securing authentication of the subscriber identity to the network, data confidentiality during transmission and access controls.[13] These design features speak to the requirement under PIPEDA for securing the transmission of personal information, however, to what extent they are implemented and successful in providing protection is unknown (meeting s.4.7).

Authentication, anonymity and encryption are also used on the GSM service. Authentication procedures focus on checking the validity of SIM cards, and / or permissions of a given mobile station for a given network, as depicted in the figure below.

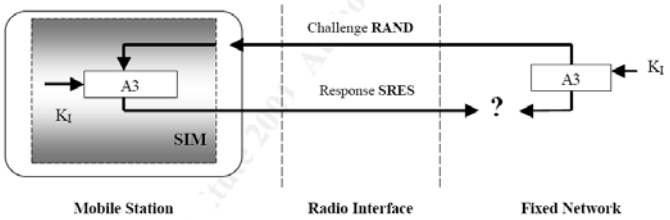

FIGURE IV [15]

Anonymity techniques include discussions of design features inherent in GSM, for example, restrictions on IMSI transmissions on the network to protect users from identification by using a TMSI instead. GSM uses a cipher key to protect user data and signal data, as depicted in the figure below.[15]

FIGURE V [15]

Willig acknowledges that significant effort is made in GSM to protect speech transmission against eavesdropping.[31] These include: authentication of registered subscribers only, encrypted data transfer, subscriber identity services, requirements for SIM cards, and elimination of duplicate SIM cards on the same network (meeting PIPEDA s4.7).[15]

The design of the SIM card also offers some privacy to users; who are allowed to "port their identity, personal information and services between devices." The SIM card operates system controls for the mobile device, including access rights through the use of a Personal Identification Number (PIN) modifiable by the user (meeting PIPEDA s.4.9). The correct PIN Unblocking Key (PUK) must be entered within a default set of attempts or the SIM becomes permanently locked (PIPEDA s.4.7). PUKs are set by the service provider.[16]

In the few research papers that address privacy specific issues in GSM, the content focuses on architecture requirements to support anonymity and pseudonymity [19] in terms of identifying location of the user (generally meeting PIPEDA s.4.4).[4,19] Kesdogan et al present a location management strategy targeted at restructuring the HLR to enable user privacy to such a degree that even the GSM provider would be unable to trace the roaming patterns of users. These techniques support user privacy by support limiting collection, use, disclosure and (presumably upon implementation) retention. It also enables stronger user control over their own data, meeting

access requirements (PIPEDA s4.9).[19] Bilogrevic evaluated a mobile network architecture with an untrusted connection between the cell site and operator, but a user installed and operator controlled equipment called a femtocell. The privacy analysis builds on existing de-anonymization and 3-way authentication protocols, concluding that the UTMS (3G) network still has privacy and security concerns, but did provide some user anonymity in terms of location.[4]

In industry news, earlier this year, AT&T announced they were offering new mobile services, including encrypted mobile device products.[32] Such services may adequately address portions of the safeguards requirements under PIPEDA s.4.7.

VI. Conclusion

The majority of existing privacy research work on GSM focuses on technical and some administrative security concerns, some of it on limits to collection, use, disclosure and retention. Optimistically, this represents a possible 30% of the requirements under PIPEDA; although it is unknown whether the physical safeguards requirements are met to support the administrative and technical requirements under s.4.7. Additional components of privacy protection that are unmentioned in research include: accountability; identifying purpose; consent; accuracy, openness; individual access and challenging compliance. While some of these provisions are dealt with primarily administratively, even consent has a technical component in terms of tracking and updating user preferences at the network, application and device layers. GSM system design appears to lack the ability to comply with the existing legislation in Canada; this non-compliance with the Act violates user privacy at the most basic level at best.

Acknowledgment

The author gratefully acknowledges the assistance of Dr. Shahram Heydari, Dr. Steve Marsh and Dr. Khalil el-Khatib.

Appendix A

The table below summarizes at a high level the type of data that can and does flows in a GSM standard mobile telephony network, and identifies whether each field meets the definition of personal information under PIPEDA (Y = yes, N = no, P = possibly when combined with other data fields).

TABLE I [20,13,16,1]

Party	Field	Description	PI
User device hardware	IMEI	International Mobile Equipment Identity; indicates manufacturer, model type and country of approval	Y
User device hardware	TAC	Type Allocation Code, gives model and origin of device	N
User device hardware	ESN	32-bit identifier recorded on a secure chip	Y
User device hardware	IMSI	International Mobile Subscriber Identifier	Y
User device software	IM	Instant messaging	Y
User device software	Email	Messages sent and received through network operator's service gateway	Y
User device software	Web	Access to the Internet via WAP gateway	Y
User device software	Wireless	IrDA, Bluetooth	N
User device software	PIM	Phonebook, or address book	Y
User device software	Mp3	Music player application	P
User device software	Email	Messages sent and received through network operator's service gateway	Y
User device software	Wed	Access to the Internet via WAP gateway	P
User device software	Wireless	IrDA, Bluetooth	N
SIM card	PUK	Personal unlock code	P
SIM card	ADN	Abbreviated Dialing Numbers (ADN)	Y
SIM card	LDN	Last Numbers Dialed (LDN)	Y
SIM card	SMS	Simple Messaging Standard	Y
SIM card	MMS	Multimedia messaging standard	Y
SIM card	LAI	Location Area Information for voice communications	Y
SIM card	RAI	Routing area information for data communications	Y
Telephone operator	Unknown	Connect MSC and BSC	P
Telephone operator	Service	Customer name and address	Y

Party	Field	Description	PI
	records		
Telephone operator	Billing	Account details of customer paying the bill, e.g. financial data	Y
Telephone operator	PUK	Personal unlock code	P
Telephone operator	Services	List of services allowed	N
Telephone operator	ICCID	SIM serial number	Y
Telephone operator	Call record	IMEI of calling ME	Y
Telephone operator	Call record	Served MSISDN, Primary MSISDN of the calling party	P
Telephone operator	Call record	Called Number, Address of the called party	P
Telephone operator	Call record	Translated number, The called number after digit translation with the MSC	P
Telephone operator	Call record	Connected number, the number of the connected party if different from the Called Number	P
Telephone operator	Call record	Roaming number, Mobile Station Roaming Number employed to route the connection	P
Telephone operator	Call record	Recording entity, The E.164 number of the visited MSC producing the record	P
Telephone operator	Call record	Incoming TKGP, The MSC trunk group on which the call originated usually the BSS	P
Telephone operator	Call record	Outgoing TKGP, The trunk group on which the call left the MSC	P
Telephone operator	Call record	The identity of the cell in which the call originated including the location area code	P
Telephone operator	Call record	A list of changes in the Location Area Code / Cell ID each time stamped	P
Telephone operator	Call record	Bearer or teleservice employed	P
Telephone operator	Call record	Transparency Indicator Only provided for those teleservices which may be employed in both transparent and on-transparent mode	P
Telephone operator	Call record	A list of changes of basic service during a connection each time stamped	P
Telephone operator	Call record	Supplementary services invoked as a result of this connection	P
Telephone operator	Call record	The change advice parameters sent to the MS on call setup	P
Telephone operator	Call record	Change of AOC Parameters New AOC parameters sent to the MS, e.g. as a result of a tariff switch over, including the time	P
Telephone operator	Call record	The mobile station classmark employed on call setup	P
Telephone operator	Call record	A list of changes to the classmark during the connection, each time stamped	P
Telephone operator	Call record	Seizure of incoming traffic channel (for unsuccessful call attempts), answer (for successful attempts), release of traffic channel	P
Telephone operator	Call record	The chargeable duration for the connection for successful calls, the holding time for call attempts	P
Telephone operator	Call record	The type of radio traffic channel requested by the MS	P
Telephone operator	Call record	Radio channel used The type of radio channel actually used (full or half)	P
Telephone operator	Call record	Change of radio channel A list of changes, timestamped	P
Telephone operator	Call record	The reason for the release of the connection	P
Telephone operator	Call record	A more detailed reason for the release of the connection	P
Telephone operator	Call record	The number of data segments transmitted, if available	P
Telephone operator	Call record	Partial record sequence number, only present in case of partial records	P
Telephone operator	Call record	Call reference, A local identifier distinguishing between transactions on the same MS	P
Telephone operator	Call record	Charge / no charge indicator and additional charging parameters	P

Party	Field	Description	PI
Telephone operator	Call record	Record extensions, A set of network / manufacturer specific extensions to the record	P
Telephone operator	Call record	gsmSCF address, Identifies the CAMEL server serving the subscriber	P
Telephone operator	Call record	Service key, The CAMEL service logic to be applied	P
Telephone operator	Call record	Network call reference, An identifier to correleate transactions on the same call taking place in different network nodes	P
Telephone operator	Call record	MSC address, Contains the e.164 number assigned to the MSC that generated the call reference	P
Telephone operator	Call record	Indicates whether or not a CAMEL call encountered default call handling	P
Telephone operator	Call record	The max number of HSCSD channels requested as received from the MS at call set-up	P
Telephone operator	Call record	The max number of HSCSD channels allocated as received from the MS at call set-up	P
Telephone operator	Call record	A list of network or user initiated changes of number of NSCSD channels during a connection, each timestamped	P
Telephone operator	Call record	Fixed network user rate May be present for HSCSD connection	P
Telephone operator	Call record	Air interface user rate requested The total Air Interface User Rate Requested by the MS at the call setup	P
Telephone operator	Call record	Channel coding accepted A list of the traffic channels coding accepted by the MS	P
Telephone operator	Call record	The traffic channel codings negotiated between the MS and the network at call setup	P
Telephone operator	Call record	Speech version used for the call	P
Telephone operator	Call record	Speech version supported supported by the MS with highest priority indicated by MS	P
Telephone operator	Call record	Number that counts how often armed detection points were encountered	P
Telephone operator	Call record	Indicator for the complexity of the CAMEL feature used	P
Telephone operator	Call record	This field contains data sent by the gsmSCF in the FCI message	P
Telephone operator	Call record	Set of CAMEL information IEs related to logs	P
MSC provider	VLR database	Data on any users not from the HLR	Y
MSC provider	HLR database	Home Location Register used to obtain information on subscribers	Y
MSC provider	NSS	Manages user identified, locations and establishes communications among users	Y
MSC provider	AuC database	Authentication Centre; authentication and encryption information every mobile user, shared with the HLR and VLR	Y
MSC provider	EIR	Equipment Identity Registrar; used to prevent the use of stolen or fraudulent MS equipment	Y

References

[1] Al-Tawil, Khalid, Ali Akrami and Habib Youssef. *A New Authentication Protocol for GSM Networks*, Department of Computer Engineering, King Fahd University of Petroleum and Minerals. Proceedings of the 23rd Annual Conference on Local Computer Networks. 11-14 October 1998. Page 11-14. Available at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=727643&tag=1.

[2] Bekkers, Rudi, Bart Verspagen and Jan Smits. *Intellectual Property Rights and Standardization: the case of GSM*. Telecommunications Policy, Volume 26. 2002. Page 171-188. Available at https://atmire.com/labs/bitstream/handle/123456789/6805/file14424.pdf?sequence=1.

[3] Beller, Michael J, Li-Fung Chang and Yacov Yacobi. *Privacy and Authentication on a Portable Communications System*. IEEE Journal on Selected Areas in Communications, Volume 11, Number 6. August 1993. Page 821- 829. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00232291.

[4] Bilogrevic, Igor. *Security and Privacy in Next Generation Mobile Networks: Long Term Evolution and Femotocells*. Security and Cooperation in Wireless Networks / EPFL. PowerPoint Presentation. Available online at http://secowinetcourse.epfl.ch/previous/09/Bilogrevic.Igor/Final_Presentation.ppt. 19 January 2010.

[5] Braman, Sandra. *Privacy for Networked Computing, 1969-1979*. Internet, Politics, Policy 2010: An Impact Assessment. Conference 16-17 Septemeber 2010. Available online at http://microsites.oii.ox.ac.uk/ipp2010/system/files/IPP2010_Braman_Paper.pdf.

[6] Brown, Dan. *Techniques for Privacy and Authentication in Personal Communications Systems*. IEEE Personal Communications. August 1995. Page 6-10. Available at http://www.ece.msstate.edu/courses/ece8990/papers/bro95.pdf.

[7] Carlsen, Urf. *Optimal Privacy and Authentication on a Portable Communications System*. ACM SIGOPS Operating Systems Review, Volume 28, Issue 3. 1994. Page 16-23.

[8] Carnegie Mellon University, Software Engineering Institute, CERT Coordination Center. Dekker, Marcel, *Security of the Internet*, Froehlick / Kent Encyclopedia of Telecommunications, New York. Volume 15. 1997. Page 231-255. Available at http://www.cert.org/encyc_article/tocencyc.html.

[9] Cisco Systems Incorporated, "Information Security". Available online at http://www.cisco.com/web/about/ciscoitatwork/security/index.html. 2009.

[10] Couture, Erik. Information Security Reading Room, SANS Institute. *Wireless Mobile Security*. Available online at http://www.sans.org/reading_room/whitepapers/incident/wireless-mobile-security_33548. Accepted 3 December 2010.

[11] Curtin, Matt. *Introduction to Network Security*. March 1997. Reprinted with the permission of Kent Information Services, Inc. Available at http://www.interhack.net/pubs/network-security/.

[12] European Telecommunications Standards Institute (ETSI), GSM Standards. Available online at http://www.etsi.org/WebSite/technologies/gsm.aspx.

[13] European Telecommunications Standards Institution (ETSI), *GSM: Global System for Mobile Communications, Digital Cellular Telecommunications System (Phase 2+); Specification of Subscriber Identity Module – Mobile Equipment (SIM-ME) interface (GSM 11.11)*. December 1995.

[14] Hiramatsu, Tsuyoshi. *Protecting Telecommunications Privacy in Japan*. Communications of the ACM, Volume 36, Number 8. August 1993. Page 74-77.

[15] Information Security Reading Room, SANS Institute. *The GSM Standard (An Overview of its Security)*. Available online at http://www.sans.org/reading_room/whitepapers/telephone/gsm-standard-an-overview-security_317. Undated.

[16] Jansen, Wayne and Rick Ayers. National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. *Guidelines on Cell Phone Forensics*. Special Publication 800-101, Sponsored by the Department of Homeland Security. May 2007.

[17] Katz, James E. *Telecommunications and Computers: Whither Privacy Policy*. Society, Volume 25, Issue 1. 1987. Page 81-86.

[18] KaZam Technologies on behalf of Industry Canada. *The Canadian Wireless Industry: Analysis, Positioning and Capabilities 2006-2009*. January through March 2006. Available at http://www.ic.gc.ca/eic/site/ict-tic.nsf/eng/h_it07845.html.

[19] Kesdogan, Dogan, Hannes Federrath, Anha Jerichow and Andreas Pfitzmann. *Location Management Strategies: Increasing Privacy in Mobile Communication*.

[20] Kioskea.net Online Community. *Mobile Telephony*. Available online at http://en.kioskea.net/contents/telephonie-mobile/reseaux-mobiles.php3.

[21] Lee, C.-C., M. S. Hwang and W. P. Yang. *Extension of authentication protocol for GSM*. IEE Proc.-Communications, Volume 150, November 2. April 2003. Page 91-95.

[22] Lee, Chii-Hwa, Min-Shiang Hwang and Wei-Pang Yang. *Enhanced privacy and authentication for the global system for mobile communications*. Wireless Networks, Volume 5. 1999. Page 231-243.

[23] Lee, Laurie Thomas. *The USA Patriot Act and Telecommunications: Privacy Under Attack*, Rutgers Computer and Technology Law Journal, Volume 29. 2003. Page 371–403. Available at http://www.allbusiness.com/technology/telecommunications/618221-1.html.

[24] Peinado, Alberto. *Privacy and authentication protocol providing anonymous channels in GSM*. Computer Communications, Volume 24. 2004. Page 1709-1715.

[25] Pelkmans, Jacques. *The GSM standard: explaining a success story*. Journal of European Public Policy, Volume 8, Issue 3. 2001. Page 432-453.

[26] *Personal Information Protection and Electronic Documents Act*, 2000 Available online at http://laws.justice.gc.ca/en/P-8.6/?noCookie.

[27] Schwartz, Paul M. *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*. Hastings Law Journal, Volume 54. August 2003. Page 751-800.

[28] Shin, Minho, Justin Ma, Arunesh Mishra and William A. Arbaugh. *Wireless Network Security and Interworking*. Proceedings of the IEEE, Volume 94, Issue 2. February 2006. Page 455-466.
[29] Sydor-Estable, Nikola. Infomration and Communicnations Technologies Branch, Industry Canada. *Key Wireless Technologies and Developing Trends*. November 2006. Page 1-17.
[30] Wikipedia contributors. List of Canadian Mobile Phone Companies. Wikipedia, The Free Encyclopedia. August 30, 2010, 18:20 UTC. Available at: http://en.wikipedia.org/wiki/List_of_Canadian_mobile_phone_companies. Accessed September 1, 2010.
[31] Willig, Ing Andreas. Communications Networks Group, Hasso-PLattner-Institute, University of Potsdam. *The GSM Air Interface Fundamentals and Protocols*. 20 May 2003.
[32] Hamblen, Matt. *AT&T adds mobile services for business, government users*. Computer World. 20 July 2010. Available online at http://www.computerworld.com/s/article/9179425/AT_T_adds_mobile_services_for_business_government_users.